Majandus- ja infotehnoloogiaministri määruse
„Küberintsidentide registri põhimäärus“ eelnõu
seletuskirja lisa

Märkuste tabel

	Märkus	**Märkusega arvestamine**
	Siseministeerium 15.02.2021 nr 1-7/18/5	
1.	Määruse §-s 7 sätestatud andmekoosseis on teoorias üsna põhjalik ja ulatuslik. Eelnõu § 6 on välja toodud registri ISKE turvaklass K1T1S2 ja turbeaste M. Siseministeeriumi hinnangul ei ole see turvatase piisav. Esiteks juhime tähelepanu, et koondina on see informatsioon väga tundlik ning seda on vaja proportsionaalsete meetmetega kaitsta. Teiseks on eelnõu § 8 loetletud andmeandjate hulgas on ka Siseministeerium ning tema hallatavad asutused ning riigisaladuse ja salastatud välisteabe seaduse (RSVS) § 10 lg 1 ja lg 9 koosmõjus võib antud asutuste poolt edastatud küberintsidente käsitlev teave ning selle kogumina hoidmine RSVS mõistes infrastruktuuri ja teabe riigisaladus, mida tuleb salastada kas konfidentsiaalsel või madalamal tasemel kuni 30 aastat. Kolmandaks kattuvad osaliselt eelnõu § 2 välja toodud registri eesmärgid ja eelnõu § 7 lg 2 loetletud registrisse kantavad andmed riigisaladuse ja salastatud välisteabe kaitse korra (RSVKK) § 8 lg 1 p 32 nimetatud Riigi Infosüsteemide Ameti (RIA) poolt kogutava teabega, milline salastatakse piiratud tasemel 10 aastaks. Riigisaladuse esinemisel tuleb registrile kohaldada RSVKK § 39 lg 2 p 3 ehk arvutite ja	**Antud selgitus** Küberturvalisuse seaduse (*KüTS*) jõustumisest (mai 2018) saadik ei kohaldata KüTS-i sätteid muu hulgas riigisaladuse ja salastatud välisteabe töötlemisele. Seega ei ole vajadus registri turvataset muuta. Kuna küberintsidentide registris ei kajastata riigisaladusega hõlmatud teavet, ei kohaldata ka registri pidamisele arvutite ja kohtvõrkude kaitse nõuete määrust (AKKN). Turvaklassi ja turbeastme muutmist ei ole vaja.

	kohtvõrkude kaitse nõuete määrust (AKKN).	
2.	Eelnevaga seoses palume RIA-l täiendavalt hinnata peetava registri eesmärki. Probleem tuleneb eelnõu seletuskirja §-st 12, milles selgitatakse, et registris kajastuvad ka mõjuta intsidendid ehk „õngitsuskirjad, mille ohvriks ei ole keegi langenud“. See selgitus ei haaku KüTS intsidendi definitsiooniga, mis on selgitatud ka seletuskirjas § 12 all. Ebaõnnestunud õngitsuskirjad, mida saabub nii avaliku- kui erasektori meiliaadressidele üleriigiliselt tuhandeid, siia sellisel kujul ei kvalifitseeru. Siseministeerium ei väida, et sellist infot ei oleks vajalik süstematiseerida, vaid peab vajalikuks see eelnõus ja seletuskirjas selgemalt eristada.	**Antud selgitus** RIA soosib ja ei piira küberintsidentidest teavitamist. Üksikjuhtumina mõjuta küberintsident annab aga kogumis teistega olulist teavet aktuaalsete trendide, vektorite ja sihtmärkide osas ehk on panuseks otseselt KüTS § 12 ülesannete täitmiseks ehk küberintsidendi ennetuse ja lahendamise koordineerimiseks. Õngitsuskirjad ja ka muud mõjuta küberintsidendid kantakse küberintsidentide registrisse samadel alustel teiste küberintsidentidega. Mõju puudumisel märgitakse nad koheselt lahendatuks. Teavet õngitsuskirjadest säilitatakse sarnaselt muule teabele 5 aastat alates selle küberintsidendi lahendatuks lugemisest.
3.	Eelnevast kahest märkusest lähtuvalt teeb Siseministeerium ettepaneku kajastada registris üksnes intsidentide arvestust, kaitstes seda seejuures rangemate ISKE nõuetega, kui K1T1S2. Selline lähenemine võimaldab kajastada intsidentide tundlikumat informatsiooni eraldi süsteemis, mis oleks kooskõlas ka riigisaladuse kaitse nõuetega, kui intsidendiga seotud haavatavus ja intsidendi koondanalüüs seda nõuavad. Juhul, kui RIA registri pidajana siiski soovib registris käsitleda oluliselt sisulisemat informatsiooni (nagu sätestatud eelnõu §-s 7, mh piiratud tasemel riigisaladust), peab register vastama ka AKKN nõuetele.	**Antud selgitus** Eelnõus tehtud muudatused vastavalt KüTS-i nõuetele ning registris ei kajastata riigisaladusega kaitstud teavet. Seega käesoleva registri kooskõla AKKN nõuetega ei ole vajalik. Riigisaladust puudutava töötlemine toimub selleks ettenähtud eraldi süsteemis.
	Eelnõu seletuskirjas on märgitud, et registri loomisega kulusid ei kaasne.	**Antud selgitus**

	Siseministeerium näeb vajadust registri tervikliku eesmärgi täpsustamisega seoses täiendavalt üle hinnata ka kulud.	Registri asutamisega ei kaasne uue elektroonilise andmebaasi loomist vaid jätkatakse olemasoleva tehnilise lahendi kasutamist, mistõttu andmekogu asutamisega arendamise kulu ei teki.
4.	Eelnõu § 5 sätestab registri pidamise elektroonilisel kujul. Eelnõus ei ole ettenähtud, et loodav register oleks liidestatud infosüsteemide andmevahetuskihiga (edaspidi X-tee). Ka eelnõu seletuskirjas ei ole selgitatud, miks ei ole peetud vajalikuks, et loodav register oleks riigi infosüsteemi kuuluv andmekogu, st andmekogu, mis registreeritakse riigi infosüsteemi halduse infosüsteemis (RIHA) ning liidestatakse X-teega. Sellega seoses palub Siseministeerium selgitusi, miks ei ole X-teega liidestamist peetud vajalikuks.	**Antud selgitus** Register on mõeldud ametkondlikuks kasutamiseks ehk eelkõige RIA ülesannete täitmiseks. Tegemist on töövahendiga, mis lihtsustab RIA ülesannete täitmist, mistõttu selle X-teega liidestamine ei ole vajalik.
5.	Eelnõu § 10 sätestab andmetele juurdepääsu. Siseministeeriumi hinnangul ei ole õiguslikult üheselt selge, kas eelnõu § 10 võimaldab vastutaval töötlejal ehk RIA-l anda juurdepääse iseseisvalt. Siseministeeriumi haldusalas omavad kindlasti ligipääsuvajadust Politsei- ja Piirivalveameti Keskkriminaalpolitsei (PPA) ning Kaitsepolitseiamet (KAPO). PPA tegeleb intsidentide menetlemisega ning KAPO teeb järjepidevalt tööd Eesti riiklikku julgeolekut ohustavate küberrünnete tuvastamisel ja tõkestamisel. Sellest tulenevalt teeb Siseministeerium ettepaneku sätestada eelnõu §-s 10 konkreetsed asutused, kellele on juurdepääs õiguslikult tagatud või sõnastada asutuste ja isikute juurdepääs läbi seadusest tulenevate ülesannete täitmise pädevuse	**Arvestatud** Eelnõus sätestatud julgeolekuasutuste ja politseiasutuste õigus saada registris teavet päringute põhiselt, kui teave on vajalik nende ülesannete täitmiseks.

6.	KüTS § 8 sätestab teenuse osutajate kohustuse teavitada Riigi Infosüsteemide Ametit intsidentidest. Sama paragrahvi lõige 8 annab õigusliku aluse kehtestada küberintsidentidest teavitamise kord ja raporti vorm. Siseministeeriumi hinnangul oleks asjakohane registri loomisel kaaluda ka ühise edastamise korra ja intsidendi vormi kehtestamist, et tagada intsidentide andmete ühetaolisus ja selgem struktuur.	**Võetud teadmiseks** Käesoleval ajal on teavitamise korra ja raporti vormi volitusnormi kohane määrusega sisustamata jätmine teadlik otsus. RIA jaoks on eelkõige oluline saada viivitamatult esmane teave küberintsidendist olenemata kanalist. Olulist teavet, küsib RIA juurde vastavalt vajadusele. Lisaks sellele märgime, et seoses Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2022/2555 ehk NIS2-ga on tolle direktiivi artikli 23 lõike 11 kohaselt Euroopa Komisjonil võimalik võtta vastu rakendusakte, et täpsustada NIS2-s reguleeritud rikkumisteadete edastamise teaveliiki, -vormingut ja esitamise korda. Seetõttu puudub ka hetkel otsene vajadus Eesti õiguses kommentaaris viidatud määrust sisustada.
	Eesti Infotehnoloogia ka Telekommunikatsiooni Liit 02.02.2021 nr 6.1-2/9-1	
7.	**Eelnõuga edasi liikumiseks tuleb meie hinnangul lahendada järgmised küsimused:** 1) Eelnõuga loodaval küberintsidentide registril (edaspidi: register) on oluline mõju kõigile isikutele ja asutustele, kelle edastatud andmeid seal hoidma plaanitakse hakata, mistõttu on äärmisel oluline tagada registris olevate andmete turvalisus ja konfidentsiaalsus. Eelnõus on hetkel selles osas mitmeid puudusi. Kindlasti tuleb silmas pidada, et kavandatud mahus andmete kokku koondamisega suureneb oht andmelekkeks, mistõttu on eriti tähtis vältida olukorda, kus Eesti	**Arvestatud** 1) Küberintsidentide registrit ei ühendata X-tee kaudu riigi infosüsteemi ning kandeid registrisse saab teha vaid vastutav töötleja; 2) Juurdepääsuõigusega isikud ja juurdepääsu eeldus on sätestatud eelnõus ja selgitatud seletuskirjas; 3) Riigisaladusega kaitstud teavet registrisse ei kanta. Küberintsidendist teavitanud teenuse osutaja saab eelkõige registriandmete põhjal loodavaid isikustamata analüüse ja ohuteateid. Samas toetab RIA soovi korral

	küberhaavatavused ründe tagajärjel avalikuks saavad. 2) Vajalik on saada selgus küsimuses, kas register on mõeldud töövahendiks Riigi Infosüsteemi Ametile (edaspidi: RIA) või saavad selles sisalduvatele andmetele juurdepääsu ka küberintsidentidest teavitavad teenuse osutajad. Igal juhul on vajalik oluliselt täpsemalt määratleda kasutajate õigustega seonduv. 3) Hetkel ei ole üheselt arusaadav, kas registrisse on mõeldud kanda ka riigisaladust puudutavad andmed. Kavandatavate turvanõuete tõttu tundub, et ei ole, aga samas vastavalt riigisaladuse ja salastatud välisteabe seaduse § 10 punktile 9 on küberturvalisuse järelevalvetoimingute käigus infosüsteemide kriitilise haavatavuse kohta kogutud teave teatud tingimustel piiratud tasemega riigisaladus.	teavitajat küberintsidendi lahendamisel. Ulatuslike küberintsidentide lahendamiseks on võimalik kaasata ka nn küberreservi, mis koosneb RIA-st, kuuest riigi IT-majast ning Kaitseliidu vabatahtlikest liikmetest.
8.	Registri eesmärgi mittevastavus volitusnormile 1.1. Eelnõu §-s 2 sätestatakse registri pidamise eesmärk, mis mõnevõrra erineb kõnealuse andmekogu asutamiseks ja pidamiseks ette antud volitunormist. Nimelt sedastab küberturvalisuse seaduse (KüTS) § 13 lõige 1 registri pidamiseks kaks eesmärki: a. ühelt poolt pidada küberintsidentide üle arvestust ning b. teisalt analüüsida küberintsidente nende lahendamiseks, ohuteadete edastamiseks ja järelevalvetoimingute tegemiseks. Erinevalt eelnõu §-s 2 sätestatust viidatud volitusnorm küberintsidentide tuvastamise tegevust ei hõlma. Hea õigusloome ja normitehnika eeskirja (RT I, 29.12.2011, 228, HÕNTE) § 53 kohaselt peab aga määruse eelnõu sisu olema kooskõlas seaduses sätestatud volitusnormi piiride, mõtte ja eesmärgiga ning määruse eelnõu ei tohi kitsendada ega laiendada volitava seaduse sätteid. Seejuures jääb meile	**Antud selgitus** Registrisse kogutakse teavet küberintsidendi kohta. Tagamaks, et kogutud teave oleks kättesaadav RIA ennetusega tegelevatele ametnikele nähakse eelnõuga ette ka õigus anda vaatlejana juurdepääs RIA ametnikele, kelle ametikoha järgne ülesanne on analüüsida küberintsidente, ohuteadete edastamine, sündmuste lahendamine või järelevalve. Küberintsidentide tuvastamine on esmalt oluline kõikidest järgnevateks tegevusteks, sh arvestuse pidamiseks, ohuteadete loomiseks ja edastamiseks ja lahendamise koordineerimiseks. Teiseks toetab register täiendavate küberintsidentide tuvastamist. Näiteks läbi selgunud ründevektorite või trendide, mis võimaldab RIA-l KüTS § 12 lõike 2 kohast Eesti internetiprotokolli aadressiruumis olevate ning Eesti maatunnusega seotud domeenide vaatlust

	selgusetuks, kuidas saab andmekogu pidamine küberintsidentide tuvastamist praktiliselt toetada. Ka see vajab täiendavat selgitamist, kuidas aitab register küberintsidente lahendada. Kui täna peab teenuse osutaja KüTS § 7 kohaselt rakendama meetmeid küberintsidentide ennetamiseks ja lahendamiseks, siis küberintsidentide register saab olema mõnes mõttes tagasivaade intsidentidele ning selleks ajaks on juba teenuse osutaja võtnud tarvitusele meetmed selliste juhtumite kordumise ennetamiseks. Seetõttu on raske aru saada registri väärtusest küberintsidentide lahendamise mõttes.	täpsemalt sihtida ja kavandada, tuvastades seega ka küberintsidente, millest aktiivselt teavitatud ei ole. Samuti on levivad trendid, ohuvektorid ja teave varasematest küberintsidentidest oluliseks sisendiks uute küberintsidentide lahendamise koordineerimiseks, st. lahendava isiku juhendamisel ja nõustamisel.
9.	Teeme ettepaneku kirjutada registri eesmärgi selgituseks paremini lahti, mida kogutud andmetega tehakse ning lisada ka, milline on analüüside tulemusest saadav võit andmete esitajale	**Seletuskirja täpsustatud** Andmete esitaja saab võimalusel ja põhjendatud juhul, ehk kui andmete esitaja on ise küberintsidendist mõjutatud subjekt ning RIA-l on asjakohast teavet, esmase tagasiside küberintsidendist teavitamise järgselt nõuannete ja soovituste näol, kuidas võimalusel küberintsidendi mõju vähendada, küberintsidenti lahendada või milliseid samme tuleks järgmisena kindlasti kaaluda või ette võtta. Samuti on kõikide andmete esitajate saadavaks kasuks kogumis tekkiva teabe pinnalt tehtud üldistatud analüüside tulemused ehk teavitused ja ohuteated, mis suunavad küberintsidente ennetama, mõjusid vähendavaid tegevusi ette võtma ja küberintsidendi toimumisel seda lahendama.
10.	Registri turvalisuse ebapiisav tase 2.1. Eelnõu ei võta arvesse seda, et vastavalt riigisaladuse ja salastatud välisteabe seaduse § 10 punktile 9 on RIA küberturvalisuse riskianalüüsid, seireteave	**Antud selgitus** RSVS § 10 punkt 9 teave on riigisaladus üksnes juhul, kui sellise teabe avalikuks

	ja järelevalvetoimingute käigus infosüsteemide kriitilise haavatavuse kohta kogutud teave niivõrd, kuivõrd need sisaldavad tehnilist teavet põhiseaduslike institutsioonide, valitsusasutuste, nende hallatavate asutuste, elutähtsa teenuse osutajate ning Eestis paiknevate ja Eesti poolt tagatava julgeolekuga rahvusvaheliste organisatsioonide infosüsteemide kriitilise haavatavuse kohta ja mille teatavaks saamine kõrvalistele isikutele tekitab turvaintsidendi tekke ohu nendes valdkondades, piiratud tasemega riigisaladus ja salastatakse kuni 10 aastaks. Sellest tulenevalt ei tohiks koguda kriitilise tähtsusega infot oluliste infosüsteemide haavatavuste ja turvameetmete kohta registrisse, mille turbeaste on M nagu näeb ette eelnõu § 6. See on ebapiisav tase nii oluliste andmete kaitseks. Juhime tähelepanu, et ka ISKE rakendusjuhend (8.00 p 1.1) sätestab, et ISKE ei ole mõeldud riigisaladust käitlevate infosüsteemide turbeks. Oleme seisukohal, et kui tegemist on ISKE S2 konfidentsiaalsustasemega andmekoguga (M), siis ei ole aktsepteeritav sellises andmekogus säilitada infosüsteemide loetelu, rakendatud kaitsemeetmeid ning logi- jms tõendeid intsidendi kohta, mis kirjeldavad võimalikke nõrkusi teenusepakkujate juures. Seega ei saa meie hinnangul registrile kohaldada turbeastet M, vaid register peab olema kõrgema turbeklassiga	tulek kahjustaks Eesti Vabariigi julgeolekut. Eelnõu arvestab KüTS-i nõudeid, sh ei sisalda registris olev teave riigisaladust.
11.	Kahtleme ka selles, kas eelnõu §-s 6 nimetatud K1 käideldavusklass on piisav, selleks et tagada võimalus registreerida küberintsident esimesel võimalusel, nagu KÜTS seda teenuse osutajatelt eeldab.	**Antud selgitus** Registri käideldavuse puudumisel on häiritud teataval määral analüüsi- ja ennetusosakonna töö, kelle töö (küberintsidentide ja pahavara leviku

		kohta raportite koostamine) põhiliseks sisendiks on küberintsidentide register. Samas ei mõjuta registri käideldavuse kadu oluliselt CERT-EE tööd seni, kuni säilib e-posti ja interneti teenus. Teenuse kvaliteet võib kannatada, kuid töö jätkub. Tegemist on asutuse sisemise tööriistaga, mis hõlbustab avaliku ülesande täitmist.
12.	Eelnõu § 10 sätestab andmetele juurdepääsu. § 10 lg 1 kohaselt määrab vastutav töötleja isikud, kellel on õigus töödelda registriandmeid töö- või teenistusülesannete täitmiseks. Eelnõu seletuskiri ei pööra piisava põhjalikkusega tähelepanu juurdepääsu tingimustele ja registris sisalduvate andmete kasutamisele. Seletuskirja lk 2 sedastatakse, et „registriandmed on mõeldud asutusesiseseks kasutamiseks lähtudes eelkõige avaliku teabe seaduse § 35 lõike 1 punktides 2 ning 9-12 sätestatud juurdepääsupiirangute alustest. Registriandmed võivad sisaldada teavet poolelioleva järelevalvemenetluse, turvasüsteemide või turvameetmete kirjelduse või tehnoloogiliste lahenduste kohta. Samuti võib registrisse kantud teave sisaldada isikuandmeid. Olenevalt küberintsidendi asjaoludest võib olla juurdepääsupiirangu seadmine põhjendatud ka muudel alustel kooskõlas avaliku teabe seadusega. Kuna tegemist on piiratud juurdepääsuga registriga, on juurdepääs registriandmetele teatud kindlatel kasutajate gruppidel, kellel on selleks seadusest või seaduse alusel antud õigusaktist tulenev õigus ja õigustatud huvi.” Viimane lause avab meie hinnangul selle registri väga laiale kasutajaskonnale. Eelnõu seletuskirja kohaselt (lk 3) määratakse nende isikute kasutajakonto õiguste klass ning reeglina saadakse lihtkasutaja õigused, kuid kindlatel	**Antud selgitus** KüTS § 13 lõike 2 kohaselt on küberintsidentide registris olev teave mõeldud asutusesiseseks kasutamiseks. Seega teavet kasutaval RIA ametnikul või töötajal peab teabe kasutamiseks olema teadmisvajadus. Teadmisvajadus tuleneb eelkõige isiku ametijuhendist või töölepingust või muust RIA sisemisest korrast, mis peab sisaldama viidet RIAle KüTSist tulenevate ülesandega seonduva töö- või teenistusülesande kohta, mille eelduseks on küberintsidentide registris oleva teabe kasutamine. Sellisel juhul peab vastutava töötleja ülesandeid täitev RIA struktuuriüksus või ametnik enne juurdepääsuõiguse andmist veenduma, et isikul on töö- või teenistusülesannetest tulenev teadmisvajadus. Isiku ülesannete muutumisel hinnatakse teabele juurdepääsu vajadus uuesti üle ning vajadusel registrile juurdepääs lõpetatakse. Detailsemalt reguleeritakse RIA sisene juurdepääsuõiguste andmise kord asutusesisese korra alusel. Asutuseväliste osapoolte poolt tehtud päringute osas vt ka eelmiste punktide selgitusi.

	isikutel on ka eeliskasutaja õigused. Seletuskirjast ei nähtu, mida need õigused endast kujutavad. Oleme seisukohal, et kui register hakkab sisaldama sedavõrd tundlikku informatsiooni nii kaitsemeetmete kui intsidentide olemuse üle, on vaja täpsemalt aru saada, mida nende andmetega tehakse ja kes neile ligi saab. Keeruline on nõustuda, et „vastutav töötleja määrab isikud“. Teeme ettepaneku need põhimääruse tasemel kirja panna koos õigusliku alusega („volitatud töötlejad“) ning lahti mõtestada, mida tähendab õigustatud huvi. Eelnõu praegune sõnastus annab õigustatud huvi piiritlemise osas väga laia tõlgendamisruumi, mis ei ole lubatav, kuna registris olevad andmed on tundlikud ja ka riigisaladusena käsitletavad. Seega tuleb eelnõus väga selgelt ära defineerida, kas ja mis juhtudel üldse väljastpoolt RIA-t keegi sellele süsteemile ligi saab. Meie ettepanek on lisada eelnõusse ammendav loetelu nendest isikutest ja kui peale nende veel keegi soovib registris olevale infole ligi pääseda, siis saab seda teha vaid RIA kaudu. Soovitame seejuures võtta näiteks teiste olemasolevate andmekogude põhimäärused, kus on andmekoosseisu, juurdepääsude ja tehtavate (registri)toimingute kirjeldamiseks kasutatud vastavasisulisi peatükke.	
13.	Juhime tähelepanu ka sellele, et eelnõust ja selle seletuskirjast jääb selgusetuks, kas vastutaval töötlejal on lubatud esitada päringuid ka teistele riigi või kohaliku omavalitsuse andmekogudele ja saada neist andmeid või siis edastada registri andmeid teistesse andmekogudesse (ehk siis andmete ristkasutuse lubatavus).	**Antud selgitus** Registrit ei ühendata X-teega. Register ei tee päringuid teistesse andmekogudesse ning ei anna teavet teistele andmekogudele. Registri kande algatab vastutav töötleja edastatud teabe alusel.

14.	Eelnõu § 12 reguleerib registrisse kantud andmete säilitamise tähtaegasid ja normi sõnastuse kohaselt säilitatakse neid kas viis aastat alates intsidendi lahendamisest või siis viis aastat alates intsidendi registreerimisest, kui intsidendil pole mõju. Mõlemal juhul on andmete säilitamise 5-aastase tähtaja kulgema hakkamine seotud eeltingimusega, et intsident on "ilma mõjuta". Viimase puhul on oluline aga juhtida tähelepanu küberintsidendi legaalmõistele, mis on avatud KüTS § 2 punktis 3 ning mille kohaselt on küberintsident süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust. Ehkki võib vaid oletada, et eelnõu koostajad on "ilma mõjuta intsidendi" puhul silmas pidanud sündmust, mis võib KüTS-i tähenduses süsteemi turvalisust ohustada ja millega ei kaasne ebasoodne tagajärg, siis olukorras, kus eelnõu toob küberintsidendi määratlemiseks sisse täiendava termini, võib see määruse rakendamisel põhjustada lubamatut ebaselgust. Seega teeme ettepaneku "ilma mõjuta intsidendi" mõiste kas eelnõust välja jätta või siis alternatiivselt see määruse tähenduses siiski määratleda. Selguse huvides on hea, kui kirjutatakse selgelt ka lahti, milliste kriteeriumite põhjal fikseeritakse see, et küberintsident on mõjuga.	**Arvestatud** Eelnõu ja seletuskirja muudetud. Säilitamisele nähakse ette 5 aastane tähtaeg, sõltumata küberintsidendi mõjust. Säilitamise tähtaega arvestatakse küberintsidendi lahendatuks lugemisest, seejuures märgitakse mõjuta küberintsident lahendatuks küberintsidendi osas kande tegemisel.
15.	Terminite osas väärib märkimist veel "logi". Elektroonilise side seaduse § 113 lg 5 määratleb logifaili nimetades, et see sisaldab toimingu aega, liiki, objekti ja numbrit. Teeme ettepaneku logi sarnaselt terminiga "mõjuta intsident" määruse eelnõus avada või alternatiivselt loetleda ammendavalt andmed, mida logi määruse mõttes sisaldab. Vastasel juhul jääb akt andmete töötlemise seisukohast mitmeti	**Arvestatud sisuliselt** Eelnõus ettenähtud millist teavet küberintsidentide registri toimingute kohta kogutakse. Teavet hoitakse 1 aasta.

	tõlgendatavaks nii normi adressaatidele kui ka määruse rakendajatele.	
16.	Eelnõus on § 12 mõistetavus andmete säilitustähtaja kulgema hakkamise osas problemaatiline, sest selles sisalduvad alternatiivsed koosseisud. Näiteks võib ühe küberintsidendi kohta saadav/loodav teave (mis usutavasti registris registreeritakse, kui tegemist pole riigisaladuseks kvalifitseeruva teabega) hõlmata sündmuse nii algusaega kui ka selle lahendamist, milleks kuluvat aega pole aga võimalik ette teada ja määratleda. Samuti nähakse säilitustähtaja osas ette erisus sõltuvalt sellest, kas küberintsident on mõjuga või ilma mõjuta, aga arvestama peab ka seda, et mõju olemasolu saab hinnata mingil ajahetkel, mis ei pruugi ühtida küberintsidendist teatamise ajaga	**Arvestatud** Säilitamise tähtajad ühtlustatud. Säilitamisetähtaega arvestatakse küberintsidendi lahendatuks lugemisest. (vt. ka eelmiste punktide selgitusi)
17.	Lisaks ei selgu eelnõu seletuskirjast, millele on eelnõu ettevalmistajad andmete ja logi säilitustähtaegade määramisel tuginenud. Seejuures tuleb veel arvestada, et küberintsidendi kohta käiv andmestik võib sageli sisaldada muu hulgas ka isikuandmeid (sh ka nt intsidendist teavitaja andmeid, kes ei ole KüTS mõttes teenuse osutaja) ning mida pikem on selliste andmete säilitamise aeg, seda ulatuslikum on riive inimese eraelule. Seega tuleb eelnõu seletuskirjas andmete säilitamise 5-aastase tähtaja relevantsust ja proportsionaalsust kindlasti põhjalikumalt käsitleda.	**Arvestatud ja seletuskirja täiendatud**
18.	Mõjud. Leiame, et eelnõu seletuskirjast on puudu piisav mõjude analüüs. Nimelt sisaldub seletuskirjas lk 5 napp viide, et „Ebasoovitavate mõjude risk: väike, kuna negatiivset mõju andmete esitamisega ei kaasne.“ ITL-i jaoks on üllatav niivõrd lihtsustatud lähenemine. Elutähtsa teenuse	**Antud selgitus** Ettevõtjate kohustus esitada teavet tuleneb seadusest ja selle mõjusid on hinnatud seaduseelnõu menetluse raames, mistõttu selle uuesti esitamine käesoleva eelnõu juures ei ole vajalik.

	osutajate, riigi ja teiste ettevõtete ja asutuste tundlike andmete taolise kogumina hoidmine on juba risk iseenesest ja see tuleb vähemalt seletuskirja tasemel piisava põhjalikkusega teadvustada.	