Märkuste tabel

Nr	Märkus	Märkusega arvestamine
	1. Kaitseministeerium kooskõlastas märkustega 17.02.2026 nr 5-9/26/2-3	
1.1.	Esmalt juhime tähelepanu, et läbi ettevõtete, mis on seotud Kaitseväe ja NATO võimetega, võib kaasneda mõju nii Eesti Kaitseväe kui ka liitlasüksuste või NATO ühistele operatsioonidele, mistõttu on oluline, et küberintsidentide info edastamise protsess oleks selge ja kiire ning saadud teave adekvaatne.	**Võetud teadmiseks**
1.2.	1. Eelnõu § 1 lõige 1 sätestab küberintsidentidest teavitamisel esmases teates esitatava teabe. Sätte kohaselt tuleb esmases teates esitada teave võimaluse korral, kuid ei täpsusta millal ei ole võimalik andmeid esitada ega ei sätesta, kas ja kuidas tuleb põhjendada info puudumist. Seletuskiri selgitab „võimaluse korral“ kasutamist, aga ei sätesta normis endas kohustust puudumist põhjendada. Info esitamata jätmine peab olema põhjendatud ja ajutine ning need alused peavad tulema selgelt õigusaktist. Määruses sätestamata jätmine võib anda kohustatud isikutele väga laia tõlgendusruumi. Palume eelnõu vastavalt täiendada.	**Selgitame** Riigi Infosüsteemi Ameti kommentaari 2.1. tõttu muudeti eelnõu § 1 lõike 1 sissejuhatavat lauset, mis täpsustab paremini, mida tähendab kommentaaris mainitud andmete esitamist „võimaluse korral“, tagamaks, et seletuskirjas kirjeldatud mõte oleks eelnõu tekstist paremini aru saada. Andmete puudumise põhjendamise aspekt kaetakse eelnõu § 1 lõikega 5.
1.3.	2. Juhime tähelepanu, et eelnõu ei viita kohaselt mõistete, nagu raskusaste, piiriülene mõju ega turvarikkemärk, definitsioonile. Mõistete definitsioonid on hajutatud teiste õigusaktide ja seletuskirja vahel, kuid õigusselguse mõttes tuleks kohaselt	**Selgitame** Mainitud mõisted ei ole õigusaktides defineeritud, mistõttu ei ole ka võimalik neile viidata eelnõuga ette nähtud määruses.

	viidata, millise õigusakti mõttes mõistet kasutatakse. Palume eelnõu vastavalt täiendada.	
1.4.	3. Seletuskirjakohaselt esitatakse vahearuanne Riigi Infosüsteemi Ameti taotlusel, kuid määrusest see ei nähtu. Lisaks ei nähtu eelnõust ka see, kas esitatakse üks või mitu vahearuannet. Palume eelnõu vastavalt täpsustada.	**Selgitame** Vastav nõue on ette nähtud küberturvalisuse seaduse § 8 lõikes 4^3. Ametil ei ole kohustust küsida vahearuannet, mistõttu ei ole ka selgitatud, kas neid tuleb esitada üks või mitu, kuna see sõltub konkreetse küberintsidendi asjaoludest. Teatav erisus on siis, kui lõppraportit käsitatakse vahearuandena (vt küberturvalisuse seaduse § 8 lõike 7 lauset 2), mille puhul on mitme sätte koosmõju tõttu ette näha, et vähemalt üks vahearuanne tuleb esitada.
1.5.	4. Kaitseministeeriumi hinnangul peaks asutus intsidendi korral analüüsima ja vajaduse korral rakendama süsteemseid muudatusi intsidendi kordumise vältimiseks. Palume kaaluda eelnõu täiendamist vastavalt.	**Selgitame** Vastav nõue on sisuliselt ette nähtud Vabariigi Valitsuse 09.12.2022 määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 6 punktiga 1 kui ka sama määruse § 5^1 ja seotud lisa punktiga 1.3. Sarnane nõue on ka ette nähtud Eesti infoturbestandardis, vt ettevõtlus- ja infotehnoloogiaministri 16.12.2022 määruse nr 101 „Eesti infoturbestandard“ lisa 1 punkti 10.1. ja selle alapunkte.
1.6.	5. Eelnõust jääb arusaamatuks, mis on lõppraporti sisuline väärtus ja kuidas on see seotud NIS2-st lähtuvalt pideva riskijuhtimisega. Seletuskiri küll üldjoontes selgitab, mida esitatakse, kuid selgusetuks jääb, kas ja kuidas saadud andmeid kasutatakse.	**Selgitame** Lõppraportitest esitatud sisu põhjal esitatakse iga kolme kuu tagant koondaruanne Euroopa Liidu Küberturvalisuse Ametile (vt küberturvalisuse seaduse § 12 lõiget 4^1), kes omakorda kasutab seda enda töös (vt nt küberturvalisuse 2. direktiivi artikli 23 lõiget 9). Samuti on Riigi Infosüsteemi Ametil võimalik lõppraportite sisu põhjal oma tööd planeerida ja tööd teha – vt nt ameti volitust ohuteadete edastamise osas küberturvalisuse seaduse § 12 lõikes 3.
1.7.	6. Seletuskirja kohaselt on eelnõu eesmärgiks luua teavitamise sisu ja kord, kuid eelnõu ei sätesta ühtegi konkreetset tähtaega esialgse aruande, vahearuande ega lõppraporti esitamiseks. Palume eelnõu vastavalt täiendada.	**Selgitame** Need tähtajad on sätestatud küberturvalisuse seaduse §-s 8, mille lõigete 1, 4^1, 4^2, 4^3 ja 7 kohaselt: • tuleb esmane teavitus teha viivitamata, kuid hiljemalt 24 tundi pärast teada saamist küberintsidendist,

		- millel on võrgu- ja infosüsteemi turvalisusele või teenuse toimepidevusele oluline mõju; - mille oluline mõju võrgu- ja infosüsteemi turvalisusele või teenuse toimepidevusele ei ole ilmne, kuid seda võib mõistlikult eeldada. • tuleb intsidenditeade edastada viivitamata, kuid hiljemalt 72 tundi pärast olulise mõjuga küberintsidendist teada saamist; usaldusteenuse osutajate puhul on maksimaalseks tähtajaks 24 tundi; • tuleb vahearuanne esitada enne lõppraportit, kui Riigi Infosüsteemi Amet vahearuannet seda taotleb; • tuleb lõppraport esitada ühe kuu jooksul alates intsidenditeate esitamisest arvates; kui olulise mõjuga küberintsident kestab, siis lõppraport on käsitatav vahearuandena, mille puhul esitatakse lõppraport ühe kuu jooksul pärast olulise mõjuga küberintsidendi lahendamist. Sama aspekt on lühidalt välja toodud eelnõu seletuskirjas, § 1 üldises selgituses.
	2. Riigi Infosüsteemi Ameti arvamus 09.02.2026 nr 1.1-20/26129	
2.1.	Teeme ettepaneku: 1) eelnõu § 1 saatelauses eemaldada sõnad „võimaluse korral“ ning lisada lause lõppu „kui see on teate esitamise hetkel teada“; Sõnapaar „võimaluse korral“ jätab avatuks põhjused, millises olukorras võib jääda teave esitamata. Seletuskirja põhjal on arusaadav, et silmas on peetud olukorda, kui teavet veel ei ole, kuid pakutud sõnastus on laiem. Vältimaks mitmeti tõlgendatavust teeme ettepaneku kohustust piiritlev tingimus selgelt saatelauses sõnastada.	**Arvestatud** Eelnõu § 1 lõike 1 sissejuhatav lause on muudetud.
2.2.	Teeme ettepaneku:	**Arvestatud** Eelnõu § 1 lõiget 1 on täiendatud uue punktiga 5.

	2) eelnõu § 1 lg 1 täiendada punktiga: „5) kontaktisik, kellega toimub edasine suhtlus seoses intsidendiga.“ Ettepaneku eesmärk on tagada suhtluse operatiivsus. Teavitusi ei tehta alati isiku poolt, kes peaks olema edasine kontaktisik. Vastava teabe esitamise kohustus tagaks kiirema kontakti intsidendiga tegeleva isikuga.	
2.3.	Teeme ettepaneku: 3) eelnõu § 1 lõige (3) sõnastada järgmiselt: „Vahearuandes esitatakse vastavalt intsidendi kohta teatavaks saanud asjaoludele lõikes 1 nimetatud täiendatud teave ja asjakohasel juhul Riigi Infosüsteemi Ameti taotletud lisateave.“ Ettepaneku eesmärk on täpsemalt sätestada kohustus lõikes 1 nimetatud teavet täiendada. Praegune sõnastus võimaldab piirduda teabe üks-ühele uuesti esitamisega kui RIA eraldi täiendavalt lisainfot ei küsi. Seega tekiks olukord, kus RIA peab sellise üks-ühele teabe esitamise korral iga kord täiendavat infot juurde küsima, kuigi teabe esitaja võiks selle juba ise vahearuandes edasi anda.	**Arvestatud** Eelnõu § 1 lõike 3 sõnastust on muudetud, et ettepaneku olemus oleks paremini välja loetav.
2.4.	Teeme ettepaneku: 4) eelnõu § 1 lõiget 4 täiendada punktiga „1) intsidendi, sealhulgas selle tõsiduse ja mõju üksikasjalik kirjeldus“ ja sellest tulenevalt muuta järgmiste punktide numeratsiooni. Ettepaneku eesmärk on tagada, et lõppraport annaks sisulise ülevaate, mis võimaldab võtta vajalikke meetmeid ning tegeleda sisulise ja tulemusliku ennetustegevusega. Praegune sõnastus jääb üldsõnaliseks ega pane kohustust edastada piisavalt detailset infot. Seejuures ei välju ettepanek NIS2 direktiivi raamidest, vaid kasutab direktiivis endas kasutatud sõnastust.	**Arvestatud ja selgitatud** Esitatud kommentaariga soovitakse tagada, et sellega võetakse üle küberturvalisuse 2. direktiivi artikli 23 lõike 4 punkti d alapunkt i (*intsidendi, sealhulgas selle tõsiduse ja mõju üksikasjalik kirjeldus*). Eelnõus oli selle direktiivi sätte kui ka alapunkti iv (*kui see on kohaldatav, intsidendi piiriülene mõju*) puhul mõeldud, et see võetakse üle eelnõu § 1 lõike 4 punktiga 3, mille sõnastuseks oli kavandatud *küberintsidendi raskusaste ja mõju, sealhulgas asjakohasel juhul piiriülene mõju*. Siinse kommentaari tõttu muudeti eelnõu § 1 lõike 4 punkti 3 sõnastust, mitte ei tekitatud uut punkti. Direktiivi vastavas sättes oleva sõna „tõsidus“ asemel on kasutatud „raskusaste“ – seda on selgitatud eelnõu § 1 lõike 1 punkti 2 selgitustes.

	3. Eesti Haiglate Liidu arvamus 02.02.2026 nr 197-2B	
3.1.	Juhime tähelepanu, et eelnõu § 1 lõike 1 punktis 1 kasutatud mõiste "turvarikkemärk" (inglise keeles *indicator of compromise*) ei ole defineeritud ning selle tähendus on ebaselge. Teeme ettepaneku täpsustada § 1 lõike 1 punkti 1 sõnastust viisil, mis tagaks üheselt mõistetavuse ja selge arusaadavuse soovitavast sisust. Pakume välja järgmise sõnastuse: „1) teave olulise mõjuga küberintsidendi sisu ja toimumise põhjuse kohta, sealhulgas asjakohasel juhul teave küberintsidenti tuvastada võimaldavate märkide kohta;".	**Mittearvestatud** Turvarikkemärk on kasutatud küberturvalisuse seaduses (vt § 2 punkt 26 ja § 17^5 lõiget 1) ehk kõrgemalseisvas õigusaktis, mistõttu ei ole võimalik eelnõukohases määruses seda defineerida.
	4. Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu arvamus 03.02.2026 nr 6.1-2/6-1	
4.1.	Eelnõuga võetakse üle NIS2-direktiivi artikkel 23 lõige 4 osas, mida ei reguleerita küberturvalisuse seadusega ega muude õigusaktidega. Konkreetsemalt sätestatakse eelnõuga, milline on küberintsidendist teavitamisel esitatavate teadete sisu. Eelnõus toodud andmekoosseisude osas meil kommentaare ja ettepanekuid ei ole.	**Võetud teadmiseks**
4.2.	Eelnõu seletuskirjas viidatakse küberturvalisuse seaduse § 8 lõikele 8^1, mis tekitab eelnõu puhul seose NIS2-direktiivi artikli 23 lõike 11 alusel antud Euroopa Komisjoni rakendusaktiga. Samas on see kirjas ainult seletuskirjas ja hüpoteetilise tuleviku võimalusena (seletuskiri lk 2: „Kui sedasorti rakendusakt vastu võetakse, lähtuvad…"). Reaalsuses on vähemalt üks rakendusakt sellel alusel juba Euroopa Komisjoni poolt vastu võetud: Komisjoni rakendusmäärus (EL) 2024/2690, 17. oktoober 2024, millega kehtestatakse seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate,	**Selgitame** Määruse eelnõu seletuskirjas on selgitatud küberturvalisuse seaduse § 8 lõike 8^1 olemust ehk kui komisjoni teeb rakendusakti, mis sisustab „küberintsidendi, sealhulgas olulise mõjuga küberintsidendi kohta esitatava teate või raporti vormi ja selle esitamise korra, lähtutakse nimetatud rakendusaktis sätestatud nõuetest". Komisjoni rakendusmäärus (EL) 2024/2690 on tõesti vastu võetud küberturvalisuse 2. direktiivi artikli 23 lõike 11 alusel, kuid too rakendusakt sisaldab volitusnormi aluseks oleva artikliga seonduvalt ainult need „juhud, mille korral tuleks intsidendi pidada oluliseks küberturvalisuse 2. direktiivi artikli 23 lõike 3 tähenduses" (vt artikli 23 lõike 11 teist lõiget). See rakendusmäärus ei sätesta vastavat vormi

	turbetarnijate ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite, sotsiaalvõrguteenuse platvormide ja usaldusteenuse pakkujatega direktiivi (EL) 2022/2555 kohaldamise eeskirjad, mis puudutavad küberturvalisuse riskijuhtimismeetmete tehnilisi ja metoodilisi nõudeid ja selliste juhtude täpsemat kindlaksmääramist, mille korral peetakse intsidenti oluliseks. Seetõttu teeme ettepaneku eelnõus viidata konkreetselt rakendusmäärusele (EL) 2024/2690 ning lahtiselt ka tulevastele rakendusaktidele. Vastasel juhul jääb eelnõu subjektidele segaseks, kas seda rakendusmäärust ei pea järgima või veel ei pea järgima, kuna küberturvalisuse seaduse muudatuste üleminekuaeg on 3 aastat. Nimetatud rakendusmääruses on sätestatud olulised täpsustavad tingimused. Eelnõu rakendajatele oleks õigusselguse huvides vajalik sellele määrusele viidata ning seletuskirjas rohkem selgitada erinevate õigusaktide omavahelist seost ja vahekorda.	ega täpsusta küberintsidendist, sh olulise mõjuga küberintsidendist teate või raporti esitamise korda (vt artikli 23 lõike 11 esimest lõiget). See siiski ei tähenda, et rakendusmäärust (EL) 2024/2690 ei tule järgida nendel üksustel, kes on selles nimetatud. Eeltoodu tõttu on seletuskiri üle vaadatud ja täiendatud.
4.3.	Kindlasti vajab muutmist eelnõu jõustumisaeg, kuna see on juba minevikus.	**Arvestatud**
4.4.	Lisaks juhime tähelepanu, et eelnõu seletuskiri viitab küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõule 739 SE, mis oli eelnõu kooskõlastamisele saatmise ajaks juba Riigikogu poolt vastu võetud ja Riigi Teatajas avaldatud ning jõustunud. Seega oleks õigem öelda, et eelnõu on seotud 01.01.26 jõustunud küberturvalisuse ja teiste seaduste muutmise seadusega ning rääkida juba tehtud, mitte tulevastest muudatustest.	**Arvestatud**
	5. Eesti Kaubandus-Tööstuskoja arvamus 03.02.2026 nr 4/28	
5.1.	Eelnõu seletuskirja lk-l 2 on kirjas, et „*739 SE kohaselt lisandub küberturvalisuse seadusesse ka § 8 lõige 8[1], mis tekitab kavandatava määruse puhul seose NIS2-direktiivi artikli 23 lõike*	Vt Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu kommentaari 4.2. vastust.

	11 alusel antud Euroopa Komisjoni rakendusaktiga. Selles rakendusaktis kehtestatakse nõuded küberintsidendi, sealhulgas olulise mõjuga küberintsidendi kohta esitatava teate või raporti korrale ja vormile. Kui sedasorti rakendusakt vastu võetakse, lähtuvad rakendusaktis nimetatud teenuseosutajad selles rakendusaktis kehtestatud nõuetest. Ülejäänud küberturvalisuse seaduse 739 SE kohased teenuseosutajad järgivad kavandatavat määrust“. Juhime tähelepanu, et Euroopa Komisjoni rakendusmäärus (EL) 2024/2690 on juba vastu võetud. Oluline on, et ka eelnõus viidatakse konkreetselt rakendusmäärusele (EL) 2024/2690 ning lahtiselt ka tulevastele rakendusaktidele, sest viite puudumine tekitab ettevõtjates segadust, kas nad peavad järgima EL-i määrust, Eesti määrust või mõlemat korraga. Lisaks on oluline, et ka seletuskirjas oleks selgelt ja lihtsalt aru saada nende õigusaktide omavahelist seost.	
	6. Eesti Linnade ja Valdade Liidu kooskõlastus 02.02.2026 nr 2-3/27-2	
6.1.	**1.** Eelnõu §1 lg1 p1 kasutab mõistet „turvarikkemärk“, mis on NIS2-direktiivi art. 23 lg. 4 punktis b kasutatava mõiste rikkeindikaator teisendus. Mõiste „turvarikkemärk“ on eelnõu seletuskirjas lahti kirjutatud - see on rikkumisele viitav asjaolu (igasugune tunnus, mis viitab rikkumise toimumisele). Teeme ettepaneku uue segadust tekitava sõna asemel kasutada eelnõu tekstis mõiste lahtiseletust. Praegu: 1) teave olulise mõjuga küberintsidendi sisu ja põhjuse kohta, sealhulgas asjakohasel juhul teave turvarikkemärgi kohta koos selgitusega, kas olulise mõjuga küberintsidendi eeldatavaks põhjuseks on ebaseaduslik või pahatahtlik tegevus; Ettepanek: 1) teave olulise mõjuga küberintsidendi sisu ja põhjuse kohta, sealhulgas asjakohasel juhul teave rikkumisele viitavate asjaolude	**Mittearvestatud** Turvarikkemärk on kasutatud küberturvalisuse seaduses (vt § 2 punkt 26 ja § 17^5 lõiget 1) ehk kõrgemalseisvas õigusaktis, mistõttu ei ole võimalik eelnõukohases määruses seda defineerida.

	kohta koos selgitusega, kas olulise mõjuga küberintsidendi eeldatavaks põhjuseks on ebaseaduslik või pahatahtlik tegevus;	
6.2.	**2.** Rõhutame, et kohalike omavalitsuste jaoks on oluline, et Riigi Infosüsteemi Amet (RIA) tagab selged ja lihtsad juhised teavitamise kohta. Seletuskiri (p 5) sõnastab, et RIA peab üle vaatama nii enda võrgulehel kui ka ettenähtud veebikeskkonnas olevad vormid, et need vastaksid määrusega kindlaks määratud teadete sisule, kuid ei mainita juhiseid, kasutusjuhendeid, selgitavaid materjale ega koolitusi ega rõhutata, et juhised oleksid lihtsad, selged, piisavalt arusaadavad. Palume seletuskirja vastavalt täiendada.	**Arvestatud**
	7. Eesti Perearstide Seltsi arvamus 03.02.2026 kiri	
7.1.	Eesti Perearstide Selts toetab nelja erineva teavitusvormi vältimist ning põhimõttelist suunda, et dubleerimise asemel võiks olla võimalik juba esitatud infot täpsustada ja täiendada. Hindame ning palume rõhutada paindlikkust esmase teate esitamisel, kuna selles etapis peaks prioriteet olema teabe esitamise operatiivsus, mitte detailsus ja analüüs. Seda peaksid arvestama ka vormid ning teabe menetlejad, võttes muuhulgas arvesse NIS2-st tulenevaid varajase hoiatuse eesmärke. Vormil või juhises võiks olla olemas ka indikatsioon, et varases etapis on aktsepteeritav vastata "hindamisel / info puudub". Varases etapis detailse teabe esitamise nõue vähendaks esmaste teavituste operatiivsust ning ei pruugiks olla otstarbekas ressursikasutus ajal, mil fookus on intsidendi lahendamisel ja/või teenuse taastamisel. Palume eelnõu § 1 lg 1 osas seletuskirjas selgemalt välja tuua, et esmase teavituse etapis ei eeldata informatsiooni detailsust ega juurpõhjuse tasemel analüüsi, vaid piisab teadaoleva esmase info edastamisest.	**Arvestatud** Siin vt Riigi Infosüsteemi Ameti kommentaari 2.1. ja selle vastust. Lisaks täiendati eelnõud § 1 lõikega 5.
7.2.	§ 1 lõikes 3 sätestatud lisateabe küsimise võimaluse juures palume sisse tuua mõistlikkuse ja proportsionaalsuse põhimõtted	**Selgitame**

	või muu piirangu, mis välistaks nö lõputu andmete juurdeküsimise võimaluse.	Neid põhimõtteid ei ole võimalik sätestada eelnõukohases määruses, kuna see ei oleks kooskõlas määruse andmise volitusnormiga (vt küberturvalisuse seaduse § 8 lõiget 8). Seda enam, et mainitud põhimõtted on ette nähtud haldusmenetluse seaduse § 3 lõikes 2. Lisaks on siin asjakohane sama seaduse §-id 4 (kaalutlusõigus), 5 (vormivabadus ja eesmärgipärasus) kui ka 6 (uurimispõhimõte). Need nõuded kohalduvad ka mainitud lisateabe küsimisele. Seletuskirjas on kommenteeritava sätte selgitust täiendatud.
	8. Eesti Põllumajandus-Kaubanduskoja arvamus 02.02.2026 nr 15/1-4	
8.1.	Kuigi peame küberturvalisuse tagamist oluliseks ning mõistame vajadust saada asjakohast teavet toimunud intsidentide kohta, soovime juhtida tähelepanu mitmele probleemile, mis puudutavad eelnõus sätestatud teavituskohustuse ulatust ja selgust. Esiteks jääb eelnõust ebaselgeks, millistele konkreetsetele kriteeriumidele vastavat intsidenti tuleb käsitada „olulise küberintsidendina“. Määratlus on liiga üldine ega võimalda ettevõtjatel ja asutustel piisava kindlusega hinnata, millisel juhul teavitamiskohustus tekib. Selline ebaselgus võib praktikas viia kas ületeavitamiseni või vastupidi – tahtmatute rikkumisteni.	**Selgitame** Esitatud kommentaar ei ole seotud määrusekohase eelnõuga ja seda ei saa sätestada kommenteeritava määrusega, kui arvestada määruse volitusnormi (vt küberturvalisuse seaduse § 8 lõiget 8). Pealegi on kommentaari sisu tegelikkuses reguleeritud seaduse tasandil. Küberturvalisuse seaduse § 8 lõige 1 sätestab, et teenuseosutaja, välja arvatud julgeolekuasutus, esitab Riigi Infosüsteemi Ametile esmase teate viivitamata, kuid hiljemalt 24 tundi pärast teada saamist küberintsidendist: 1) millel on võrgu- ja infosüsteemi turvalisusele või teenuse toimepidevusele oluline mõju; 2) mille oluline mõju võrgu- ja infosüsteemi turvalisusele või teenuse toimepidevusele ei ole ilmne, kuid seda võib mõistlikult eeldada. Sama paragrahvi lõige 2 täpsustab, millal on tegemist olulise mõjuga küberintsidendiga. Tolle lõike punktis 6 on viidatud Euroopa Komisjoni rakendusaktile, mille all mõeldakse komisjoni rakendusmäärust (EL) 2024/2690.
8.2.	Teiseks tekitab küsimusi eelnõus ette nähtud mitmekordne teavitamiskohustus ühe ja sama intsidendi kohta. Ei ole arusaadav, miks on vajalik esitada sama intsidendi puhul mitu eraldiseisvat teadet eri etappides, eriti olukorras, kus intsidendi sisu ja mõju ei pruugi vahepeal sisuliselt muutuda. Selline	**Selgitame** Mitmeastmeline teavitus on ette nähtud küberturvalisuse 2. direktiivi artikli 23 lõikes 4. Selles on ette nähtud „varajase hoiatuse“, „intsidenditeate“, „vahearuande“ ja „lõpparuande“ (küberturvalisuse seaduses vastavalt „esmane teavitus“, „intsidenditeade“,

	lähenemine suurendab põhjendamatult halduskoormust ega toeta küberturvalisuse tõhusat juhtimist. Leiame, et ühekordne, sisuline ja hästi struktureeritud teavitus oleks piisav ning eesmärgipärasem. Samuti peaks lõpparuande koostamine ja intsidendi põhjalikum analüüs olema selgelt määratletud Riigi Infosüsteemi Ameti vastutusalasse kuuluvaks, mitte täiendavaks kohustuseks teavitajale. Kokkuvõtvalt peame vajalikuks teavituskohustuse selgemat määratlemist ning selle mahu vähendamist, et vältida põhjendamatut bürokraatiat ja tagada regulatsiooni praktiline ning proportsionaalne rakendatavus.	„vahearuanne“ ja „lõppraport“) esitamise nõuded kui ka nende esitamise tähtajad. Need nõuded võetigi üle sama käsitlusega nagu on direktiivis ette nähtud. Jah, esimese seaduseelnõu kavandis (avaldati 09.12.2024) oli ette nähtud, et nn intsidenditeade tehakse 24 tunni jooksul ja see sisaldab samu andmeid, mis on eelnõukohase määrusega ette nähtud, st sellisel juhul ei oleks eristatud esmast teavitust ja intsidenditeadet, vaid need oleksid ühe etapina koos. Samuti oli soov ette näha vahearuande esitamise nõue kui ka säilitada (lõpp)raporti esitamise nõue. Seepeale tuli seaduseelnõule tagasiside, et see lähenemine ei arvesta direktiivis ette nähtud käsitlust ega ole sellega kooskõlas. Seetõttu muudetigi seaduseelnõud viisil, mis on nüüd sätestatud küberturvalisuse seaduse §-s 8. Küberturvalisuse seaduse § 8 lõikes 7 ette nähtud lõppraporti koostamine ei saa olla Riigi Infosüsteemi Ameti ülesanne, vaid see on ennekõike teenuseosutaja ülesanne. Selle käigus peab teenuseosutaja hindama, mis läks valesti ja mida võeti ette, et küberintsident ära lahendada, sh mida võeti ette, et sama või sarnane küberintsident ei korduks konkreetse teenuseosutaja juures. Vt siin ka Kaitseministeeriumi kommentaari 1.5. ja sellega seotud vastust.
	9. Eesti Vee-ettevõtete Liidu arvamus 03.02.2026 nr 2-2/202	
9.1.	Määruse eelnõu kohaselt on jõustumine kavandatud alates 01. veebruarist 2026. Eelnõu seletuskirjas on märgitud, et jõustumisaja puhul on lähtutud kuupäevast, mis võimaldab eelnõu kooskõlastada ning Riigi Infosüsteemi Ametil asjakohased vormid üle vaadata. Meie hinnangul ei vasta see tegelikkusele, kuna määruse eelnõu kooskõlastamise aeg lõpeb alles 03.02.2026. Sellest lähtuvalt teeme ettepaneku, et määruse jõustumise aeg määratakse hea õigusloome ja normitehnika eeskirja § 62 lg-s 1 sätestatu alusel, mille kohaselt jõustumisnormiga sätestatakse määruse või selle sätte jõustumine haldusmenetluse seaduse § 93 lõikes 2	**Arvestatud**

	ettenähtud kolmepäevasest tähtajast hilisemal tähtpäeval, kui seadus ei näe ette varasemat jõustumisaega. Jõustumisnormis jõustumisaja sätestamisel arvestatakse § 14 lõikes 2 sätestatud asjaolusid ja määruse avaldamiseks Riigi Teataja seaduse § 9 lõikes 6 ettenähtud seitsmetööpäevast tähtaega.	

Riigikantselei, Haridus- ja Teadusministeerium, Kultuuriministeerium, Rahandusministeerium ja Sotsiaalministeerium kooskõlastasid märkusteta. Andmekaitse Inspektsioonil ja Eesti Arstide Liidul täiendavad ettepanekud puudusid. Kaitseväe arvamus oli tunnistatud avaliku teabe seaduse § 35 lõike 2 punkti 1 alusel juurdepääsupiiranguga teabeks, mistõttu seda ei esitata siinses seletuskirjas.
Eelnõu, seletuskiri ja märkuste tabel edastati 25.02.2026. a kooskõlastajatele ja märkuste esitajatele e-kirja teel.