Kaasamistabel Vabariigi Valitsuse otsuse juurde „Eesti seisukohad küberturvalisuse paketile" kohta

Nr	Märkus	Märkusega arvestamine
	1. Kliimaministeerium kooskõlastas märkustega 01.04.2026 e-kiri	
1.1	Nn. ENISA rolli laiendamist ja sertifitseerimist puudutav ettepanek (*COM(2026) 11 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT...):* Toetame ENISA rolli tugevdamist ja standardiseerimist, kuna küberrünnakud ei tunne valdkondade ega ka riigi piire ning ründevektorid on tihtipeale ka universaalsed (st sama rünnakutüübiga annab maha võtta nt energeetika ettevõtte, aga ka panku ning seda annab teha nii Eestis, aga ka mõnes muus riigis jne) ja seetõttu on oluline, et Euroopas käiakse selles osas ühte jalga – ühtne riskipilt, sarnased turvameetmed, intsidentidest teavitamine-info kiire jagamine; sertifitseeritud/turvalised seadmed/teenused, kuna enamik ise kohapeal tehnoloogiat ei tooda jne. Siiski on oluline, et turvalisus tagamine ei hakkaks omakorda takistama teenuse toimimist – st, et sertifitseerimine ei tooks omakorda kaasa teenuste/toodete-seadmete turutõrke ja selle asemel, et kaitsta tekitame olukorra, kus seadmed vananevad ja ei saa uute vastu välja vahetada, sest tarnejärjekorrad on ebaproportsionaalselt pikad või, et auditeid ei saa mõistlikus ajaraamis läbi viia (hetkel on 1x aastas kohustus), sest sertifitseerituid audiitoreid ei tule nii palju peale. Ehk, kokkuvõttes tuleb leida turvalisuse ja teenuse tagamise vaatest mõistlik tasakaal.	**Võtame teadmiseks**

1.2	Nn NIS2.0 muudatuste ettepanekut (*COM(2026) 13 - Directive Proposal for simplification measures and alignment with the Cybersecurity Act + COM(2026) 13 - Annex to the Directive Proposal for simplification measures and alignment with the Cybersecurity Act)*: Toetame, et selguse mõistes on täiendatud nii energeetika- kui ka transpordivaldkonnas NIS2.0 subjektide sõnastusi ja tehtud konkreetsed viited valdkondlikele EL õigusaktidele, mis võimaldab selgemini aru saada, millised teenuseosutajad on NIS2.0 alla hõlmatud ja millised mitte. Samuti toetame, et edaspidi on hõlmatud selgelt NIS2.0 direktiivi subjektidena ka kahese kasutuse/sõjalist liikuvust tagav taristu, mis oma sisult haakub juba täna transpordivaldkonnas tegutsevate teenuseosutajatega. Arvestades, et ettepaneku kohaselt võib Euroopa Komisjon välja töötada ka valdkondade põhiselt tehnilisi nõudeid, siis peame oluliseks, et need ei dubleeriks või läheks vastuollu juba seni väljatöötatud nõuetega (näiteks energeetika- või lennunduse valdkonnas on juba praegu olemas eraldi EL tasandil küberturvalisuse regulatsioon).	**Võetud teadmiseks**
	2. Majandus- ja Kommunikatsiooniministeerium kooskõlastas märkustega 06.03.2026 e-kiri	
2.1	Esitatud pakett sisaldab meetmeid, millega lihtsustatakse ELis tegutsevate ettevõtjate jaoks ELi küberturvalisuse eeskirjade ja riskijuhtimisnõuete täitmist. Muuhulgas on küberturvalisuse NIS2 direktiivi sihipäraste muudatuste eesmärk on suurendada õigusselgust, lihtsustatakse mikro- ja väikeettevõtjate ning väikeste keskmise turukapitalisatsiooniga ettevõtjate jaoks nõuete täitmist. Majandus- ja Kommunikatsiooniministeeriumi poolt toetame EL küberturvalisuse paketis muudatusi, mis lihtsustavad ELis	**Võetud teadmiseks** Vt seisukohta seletuskirja punktis 6.5.

	tegutsevate ettevõtjate jaoks ELi küberturvalisuse eeskirjade ja riskijuhtimisnõuete täitmist, tagades liidus jätkuva kõrge küberturvalisuse taseme. Toetame harmoneeritud EL küberturvalisuse sertifitseerimisraamistiku loomist, et edendada ja tõhustada EL sertifitseerimisskeemide loomist ja rakendamist. Seejuures peame oluliseks, et sertifitseerimine jääb ettevõtjatele valdavalt vabatahtlikuks ja et loodavad skeemid on kooskõlas rahvusvaheliste standarditega. Toetame ettepaneku lähenemist, mis edendab sertifitseerimise kasutamist vastavuskinnituse mehhanismina, lihtsustades nõnda ettevõtjatele nõuetele vastavuse tõendamist.	
2.2	Lisaks, Eesti seisukohtades ELi kosmosemääruse ja Euroopa kosmosemajanduse visiooni teatise kohta (mis kiideti heaks 19.02.2026 Vabariigi Valitsuse istungil) tõime välja, et toetame riskijuhtimisraamistiku loomist, mis hõlmaks küberturvalisust ja füüsilist turvalisust nii kosmoses asuva kui ka maapealse taristu puhul. Samuti rõhutasime seisukohtades, et kosmosevaldkonna kerksusnõuete puhul tuleb maksimaalselt ära kasutada olemasolevat küberturvalisuse õigusraamistikku, vajadusel seda täiendada ning mitte dubleerida olemasolevaid nõudeid. Märgime ära, et kosmosevaldkonna kerksusnõuded peavad arvestama Euroopa Kosmoseagentuuri ja ELi olemasolevate turvastandarditega ning toetama rahvusvahelise küberkoostöö ja infojagamise arendamist.	**Võetud teadmiseks**
	3. Rahandusministeerium kooskõlastas märkusteta 10.03.2026 e-kiri	
	4. Siseministeerium kooskõlastas märkustega 17.03.2026 kiri nr 5-1/5-4	
4.1	Tulenevalt Riigikantselei resolutsioonist 2-5/26-00267 edastab Siseministeerium arvamuse Justiits- ja Digiministeeriumi Euroopa Liidu (edaspidi EL) küberturvalisuse eelnõude paketi kohta: COM(2026) 11 ning COM(2026) 13. Ülevaate koostasid	**Võetud teadmiseks**

	Siseministeeriumi EL ja välissuhete osakond (info@siseministeerium.ee), sisejulgeoleku osakond ning digi- ja teabehaldusosakond. Politsei- ja Piirivalveamet ning Kaitsepolitseiamet olid kaasatud arvamuse kujundamisesse ning neilt täiendavaid märkusi ei laekunud.	
4.2	Siseministeerium toetab esitatud EL küberturvalisuse eelnõude paketti, kuna see aitab tugevdada Euroopa vastupanuvõimet kasvavatele küberohtudele ja lihtsustab ning ühtlustab olemasolevat küberturbenõuete ja sertifitseerimisskeemide süsteemi. Lisaks toob eelnõude pakett positiivse mõjuna kaasa ENISA rolli laiendamise, mille tulemusel on nendel suuremad volitused sertifitseerimise, riskihindamise ja liikmesriikide toetamise vallas. See omakorda aitab vähendada liikmesriikide halduskoormust, tugevdada nende olukorrateadlikust ning vähendada EL-i ülest tegevuste dubleerimist.	**Võetud teadmiseks**
4.3	Samas on ENISA mandaadi laiendamise osas mõned praktilised küsimused, mis vajaks arutelude käigus selgitamist. Nimelt kas ENISA mandaat muutub senisest märksa operatiivsemaks? Kui jah, siis see omakorda tõstatab küsimuse, kas ENISA-l kujuneb välja piisav institutsionaalne ja tehniline võimekus oma laienevaid ülesandeid tõhusalt täita.	**Võetud teadmiseks** Vt seisukohta seletuskirja punktis 6.2.
4.4	Samuti toetame ühtset küberturbe sertifitseerimise raamistikku, mis peaks lihtsustama ja ühtlustama nõudeid toodetele, teenustele ja tarneahelatele üle EL-i. Kuna IKT tarneahelad on keerukad ja paljude osapooltega, on ühtsetel alustel lähenemine kasulik liikmesriigile ja selle organisatsioonidele vähendamaks võimalikke riske.	**Võetud teadmiseks** Vt seisukohta seletuskirja punktis 6.5.
4.5	Lisaks vähendab eelnõude pakett NIS2 nõuete dubleerimist erinevatele määruste vahel (nt GDPR, DORA, CER AI määrus), mille tagajärjel samuti väheneb halduskoormus.	**Võetud teadmiseks**
	5. Sotsiaalministeerium kooskõlastas märkustega 19.03.2026 kommentaar EISis	

5.1	Hindame väga positiivseks EL-i ülese nõrkuste andmebaasi ja haldusteenuse loomist – see on kriitiline meditsiiniseadmete ja e-tervise tarkvara turvalisuse tagamiseks. Samuti toetame sertifitseerimise lihtsustamist, kuid on oluline silmas pidada, et mikro- ja väikeettevõtjate halduskoormus ei kasvaks.	**Võetud teadmiseks**
5.2	Eelnõu toob kaasa olulise rahalise mõju nii avalikule kui ka erasektorile: Järelevalve kulud: Liikmesriikide ametiasutuste järelevalvekuludeks prognoositakse kogu EL-is kuni 80 miljonit eurot viie aasta jooksul, Eestis tähendab see tõenäoliselt lisakulutusi mitte ainult RIA-le, vaid näiteks ka Tervise ja Heaolu Infosüsteemide Keskusele (TEHIK). Kas ja kuidas on plaanitud kulusid katta? Tuleb arvestada, et sõltumata tõenäolisest pikaajalisest säästust toob uute nõuete rakendamine alguses osapooltele kaasa kulusid sertifitseerimise ja auditite näol. Täiendavad kulutused kaasnevad kõrge riskiga tarneahelate asendamisega. Samuti võib see tekitada uusi raskusi kriitiliste süsteemide hooldamisel või hankimisel, kui puuduvad alternatiivid. Täiendav kulude kasv tuleb veel ilmselt IT-spetsialistide puudusest – vajadus uusi turvameetmeid ja sertifitseerimiskavasid õigeaegselt rakendada, tekitab suurenenud tööjõu vajaduse, mis mõjutab tööjõuturgu ja/või seab riski alla tähtaegse rakendamise.	**Selgitame** Praeguses etapis ei ole lõplikult võimalik ette teada ega näha, millises ulatuses tekib kulu. Kui neid peaks siiski tekkima, analüüsitakse neid riigieelarve planeerimise protsessis.
5.3	Soovitame ülemineku sujuvamaks kulgemiseks võimalusel tähtaegu pikendada.	**Arvestatud** Vt seisukohti seletuskirja punktides 6.8. ja 6.145.
5.4	Halduskoormus ja dubleerimine Oluline on silmas pidada, et uued meetmed ei dubleeriks juba kehtestatud määruseid ja nõudeid (NIS2 jt). ENISA rolli tugevdamine peab olema selgelt piiritletud, et see ei hakkaks kattuma (dubleerima) liikmesriikide enda pädevusega küberohtude ennetamisel ja reageerimisel.	**Arvestatud** Vt seisukohta seletuskirja punktis 6.2.

5.5	Lisaks märgime, et sätestatavad riskihindamise kriteeriumid ei tohiks omakorda veelgi pärssida innovatsiooni, milleks on juba niigi palju piiranguid ja regulatsioone.	**Võetud teadmiseks**
	6. Andmekaitse Inspektsiooni arvamus 06.03.2026 kiri nr 2.3-4/26/590-2	
6.1	1. Sertifitseerimine IKÜM ja CSA2 alusel CSA2 ettepaneku artikli 80 lõike 1 punkti w kohaselt on Euroopa küberturvalisuse sertifitseerimise skeemide sisu ülesandeks tagada isikuandmete töötlemise turvalisus. CSA2 alusel välja antav sertifikaat võib praktikas olla kasulik tõendusmaterjal, mis näitab, et organisatsiooni tehnilised turvameetmed võivad vastata ühtlasi isikuandmete kaitse nõuetele. Seda kinnitab ka CSA2 ettepaneku põhjenduspunkt 79, mille kohaselt peaks sertifitseerimisraamistik (ECCF) andma võimaluse tõendada vastavust erinevatele küber- ja andmeturbenõuetele ühe sertifitseerimismeetme kaudu, et vähendada koormust ja ühtlustada nõudeid. Põhjenduses rõhutatakse, et organisatsioonid seisavad korraga silmitsi mitmete regulatsioonide nõuete täitmisega ning seetõttu võib ühtne sertifikaat aidata lihtsustada mitme paralleelse regulatsiooni täitmist. Oluline on siiski rõhutada, et CSA2 sertifikaat ei asenda IKÜMi artikli 42 alusel antavat sertifikaati. CSA2 keskendub küberturbe nõuetele, IKÜM seevastu nõuab lisaks tehnilistele meetmetele ka õiguslike põhimõtete järgimist, sealhulgas läbipaistvust, andmete minimaalsust, eesmärgipärasust, andmesubjekti õiguste tagamist ning töötlemise õiguspärasust. Need jäävad CSA2 sertifikaadi ulatusest välja, kuna CSA2 sertifitseerimisskeem ei ole mõeldud hindama isikuandmete kaitset tervikuna. Teatav kattuvus võib esineda IKÜMi artiklis 32 sätestatud töötlemise turvalisuse nõuetega, kuid siinjuures tuleks panna tähele, et IKÜMi artikli 32 lõike 3 kohaselt võib	**Võetud teadmiseks**

	artikli 32 nõuetele vastavust tõendada artikli 42 alusel heakskiidetud sertifitseerimismehhanismi järgimisega.	
6.2	2. EAKNi ja CSIRT võrgustiku koostöö CSA2 artikli 68 lõike 1 kohaselt peab ENISA tegema koostööd EAKNiga. On positiivne, et selline koostöökohustus ENISA ja EAKNi vahel on CSA2 selgesõnaliselt ette nähtud. EAKN on varem oma valmidust kinnitanud 22. juuli 20241 kirjaga[1]. Küll aga on oluline märkida, et selline koostöö ei tähenda andmekaitseasutuste ja küberturbe intsidentidele lahendamise üksuste (Computer Security Incident Response Teams ehk edaspidi CSIRTid) vahelist süsteemset ja struktureeritud koostööd. EAKNi moodustavad riiklikud andmekaitseasutused, samal ajal kui CSIRTid on koondatud CSIRT võrgustikku (CSIRTs Network). CSIRT võrgustiku suhe ENISAga on reguleeritud NIS2 direktiivi artiklis 15. Kuigi mõlemate siseriiklike pädevate asutuste võrgustike koostöö ENISAga on kas juba ette nähtud või nähakse käesoleva ettepanekuga, ei ole ette nähtud koostöövormi EAKNi ja CSIRT võrgustiku enda vahele. Samal ajal on Euroopa Liidu õigusruumis sellised koostöövõimalused muude asutuste vahel juba ette nähtud, näiteks digiturgude määruse kõrgetasemeline töörühm (DMA HLG), kus osalevad nii EAKN kui ka Euroopa konkurentsivõrgustik. See näitab, et horisontaalne koostöö erinevate regulatiivsete asutuste vahel on võimalik. EAKN ja CSIRT võrgustiku koostööl oleks märkimisväärsed eelised. Esiteks võimaldaks see välja töötada ühiseid seisukohti olukordades, kus andmekaitse ja küberturbe kohustused põimuvad, näiteks küberturbeintsidentide ja isikuandmete	**Selgitame** ENISA pakub sekretariaadi rolli CNW-le ja CSA2-te on EAKNi ja ENISA koostöö sisse kirjutatud.

[1] EAKN vastus ENISA kirjale 22. juulil 2024. EDPB response to letter on collaboration with ENISA | European Data Protection Board

	rikkumiste teavitamiskohustuste ristumiskohtades. Ühtsed juhised vähendaksid õiguslikku killustatust ja annaksid ettevõtetele või organisatsioonidele selgemad ootused. Teiseks looks otsene koostöö kanali kiiremaks infovahetuseks olukordades, millel on samaaegselt nii küberturbe- kui ka andmekaitseline mõõde. CSIRTid tuvastavad sageli intsidente enne kui vastutavad töötlejad andmekaitseasutusi teavitavad, mistõttu otsekontakt parandaks oluliselt andmekaitseasutuste informeeritust ja reageerimisvõimet. Samuti oleks andmekaitseasutustel sellisel juhul võimalus anda CSIRTidele juhised olukordadeks, kus vastutavad töötlejad teavitavad küberrikkumistest küll CSIRTe, kuid hindavad rikkumise sellisele tasemele, et andmekaitseasutusi ei teavitata. Samas tuleb arvestada ka võimalike probleemidega. Andmekaitseasutused ja CSIRTid tegutsevad erinevate õiguslike volituste alusel, andmekaitseasutused rakendavad IKÜMi ja lähtuvad põhiõiguste kaitse loogikast, samal ajal kui CSIRTid tegutsevad küberturbe ja kriitiliste intsidentide lahendamise raamistikus. See tähendab, et riskitõlgendused ja konfidentsiaalsusnormid ei pruugi alati kattuda. CSIRTidel võib olla ligipääs tundlikule tehnilisele teabele, mida ei saa andmekaitseasutustega jagada, samas andmekaitseasutuste käsutuses võivad olla isikuandmed, mida CSIRTidel ei ole volitust töödelda. Selge õigusliku mehhanismita piirdub koostöö tõenäoliselt siseriiklike *ad hoc* kontaktidega, millel ei ole piisavalt kaalu, et tagada järjepidevust ja õigusselgust. Ühtlasi on selline koostöö vabatahtlik.	
6.3	3. ENISA andmetöötluse õiguslik alus intsidentidest teavitamisel CSA2 ettepanek näeb ette ENISA rolli märkimisväärset laiendamist, sealhulgas ülesannete tugevdamist EL-i	**Selgitame** Kui arvamus oli tehtud nn ühtse teavitusakna teemal, siis sellega seotud arutelud toimuvad nn digiomnibussi (ehk digivaldkonna

	küberturvalisuse poolel ja intsidentide teavitamise mehhanismide loomisel. Kavandatud ühtne intsidentidest teavitamise mehhanism tähendab, et ENISA hakkab toimima keskse infosõlmena, mille kaudu liiguvad ka isikuandmeid sisaldavad teated, mistõttu on vajalik selge ja konkreetne õiguslik alus isikuandmete töötlemiseks. Käesolev ettepanek ei sisalda sätteid, mis annaksid ENISA-le õiguse töödelda isikuandmeid nende uute ülesannete täitmiseks. Kuigi ettepanek viitab vajadusele arendada ühtne teavitussüsteem ja toetada liikmesriike koostöös, ei täpsusta see töötluse eesmärke ega andmekategooriaid ning seetõttu ei vasta see määruse (EL) 2018/1725 (edaspidi EUDPR) nõudele, mille kohaselt peab töötlemine tuginema selgele EL-i õiguslikule alusele, mis määratleb täpsed ülesanded ja vajaliku töötlemise ulatuse. ENISA andmetöötlust reguleerib EUDPR, mis seab Euroopa Liidu institutsioonidele IKÜM-iga sisuliselt samaväärsed põhimõtted. EUDPR sätestab raamistikud ja tingimused, millele peab töötlemine tuginema, samas kui õiguslik alus isikuandmete töötlemiseks peab tulenema mõnest muust EL-i õigusaktist, mis annab ENISA-le vastava ülesande ning kirjeldab töötluse vältimatut vajadust. Kuna CSA2 ettepanek õiguslikku alust ei sisalda, tekib olukord, kus ENISA-l võivad tulevikus olla ülesanded, mis sisuliselt eeldavad isikuandmete töötlemist, kuid mille töötlemiseks puudub õiguslik alus.	koondpaketi) ettepaneku[2] arutluse käigus. Seetõttu tuleb EUDPR nõuetele vastavusele tähelepanu juhtida tolles protsessis, mitte siinsete ettepanekutega seonduvalt.
6.4	4. Tarneahela turvalisus ja andmete edastamise piirangud kolmandatesse riikidesse CSA2 artikli 103 lõike 2 punkt b annab komisjonile võimaluse näha rakendusaktiga ette, et teatud üksused ei tohi küberturberiskide maandamiseks edastada andmeid	**Võetud teadmiseks**

[2] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52025PC0837

	kolmandatesse riikidesse ega kasutada sellist andmetöötlust, mida tehakse kolmandast riigist. Teisisõnu võimaldab see säte piirata olukordi, kus andmetele pääsetakse ligi või neid töödeldakse väljastpoolt Euroopa Liitu, kui sellega kaasneb oht liidu küberturvalisusele, kübervastupidavusele või usaldusele. Andmete kolmandasse riiki edastamise kohta on sätted ka IKÜMi V peatükis. CSA2 artikli 103 lõike 2 punkti b ja IKÜM V peatüki suhet tuleb mõista kumulatiivsena, mitte alternatiivsetena. Asjaolu, et CSA2 alusel võib komisjon kehtestada teatavatele üksustele keelu seoses andmete edastamisega kolmandatesse riikidesse või kolmandas riigis toimuva andmetöötlusega, ei tähenda, et IKÜM V peatükk muutuks kohaldamatuks. IKÜM V peatükk sätestab tingimused, mille esinemisel võib isikuandmete edastamine kolmandasse riiki olla lubatud, kuid see ei anna iseseisvat ega absoluutset õigust selliseid edastusi teha sõltumata muudest liidu õiguse nõuetest. CSA2 alusel kehtestatud keeld või piirang ei tähenda seda, et IKÜM V peatüki nõuded kaotaksid tähtsuse. Kui tegemist on isikuandmete edastamisega, tuleb paralleelselt hinnata ka vastavust IKÜM V peatükile, kuivõrd IKÜM V peatükk kaitseb isikuandmete edastamisel andmesubjektide õigusi ja tagab kaitsetaseme jätkumise pärast andmete liikumist kolmandasse riiki. Praktikas võib see tekitada õigusselguse probleeme, sest kolmanda riigi andmeedastuse lubatavus ei sõltu siis enam ainult IKÜM V peatükist, vaid potentsiaalselt ka CSA2 määrusest. Andmetöötleja jaoks ei pruugi olla läbipaistev, millal pelgalt IKÜMi järgimisest enam ei piisa. Seoses CSA2 artikli 103 lõike 2 punktiga b võiks määruses sisalduda täpsustus, et sätte kohaldamine ei piira IKÜM V peatüki kohaldamist, ning selgitus, et isikuandmete puhul tuleb mõlemat raamistikku hinnata paralleelselt.	

6.5	5. Lunavararünded Lunavararünnete avastamine, nende kohta teabe kogumine ja juhtumite kohta ülevaate loomine on küberturvalisuse seisukohalt oluline. Samas ei muuda see üleliigseks nõuet, et juhul kui kogutav või jagatav teave sisaldab isikuandmeid, peab selline andmetöötlus olema õiguspärane, eesmärgipärane ja piirduma vajalikuga. NIS2 määruse ettepaneku põhjenduspunktis 10 kasutatakse lunavararünnete juures väljendit "tundlik teave". Sellise mõiste kasutamine ei tähenda, et tegemist oleks IKÜM artikli 9 mõttes eriliigiliste isikuandmetega, vaid pigem osutab see sellise teabe tundlikkusele küberturbe ja konfidentsiaalsuse vaatest. Tegemist on olulise vaheteguriga, kuivõrd IKÜM artikli 9 mõttes tundliku teabe töötlemine on üldjuhul keelatud, väljaarvatud IKÜM artikkel 9 lõike 2 erandite kohaldumisel.	**Võetud teadmiseks** Vt seisukohta seletuskirja punktis 6.1.
	7. Riigi Infosüsteemi Ameti arvamus 06.04.2026 kiri nr 1.1-20/26281	
7.1	ENISA konverentsil väljendasid rakendajad üle Euroopa ootust töörahule, võimalusega enne järgmisi muudatusi mõistliku perioodi jooksul kehtestatud reegleid rakendada. Nõustume selle seisukohaga. Praegused muudatused seoses nt NIS2-ga ei adresseeri tõenäoliselt väga suurt osa praktikas ilmnenud või veel ilmnevaid probleeme, eriti arvestades, et paljude riikide poolt direktiivi ülevõtmine viibis, sh Eestil. Uued muudatused tähendaksid niigi põhjalikult muudetus küberturvalisuse raamistiku uuesti muutmist sisulistes aspektides. Muudatused, mis on planeeritud, näitavad selget ambitsiooni suurendada tsentraliseeritust ning vähenda liikmesriikide otsustuspädevust. Kuigi ühisturu mõistes on see ambitsioon arusaadav, ei ole see liikmesriikide ja nende erinevuste vaatest põhjendatud. Eestil on ühelt poolt väga arenenud digiriik ja teiselt poolt ka selge, meie vajadustele vastav, eripärasid, sh	**Võetud teadmiseks**

	väiksust ja turuosalisi arvestav küberturvalisuse tagamise süsteem. Kesksete meetmete ülimuslikkus liikmesriigi kehtestatud nõuete ees võib mõjutada negatiivselt saavutatud tasakaalu.	
7.2	ENISA rolli suurenemine 1. Nii CSA2 kui NIS2.2 ettepanekute oluline osa on ENISA rolli suurendamine. Selle juures on mitmed küsitavused ja murekohad. Eesmärk on suurem tsentraliseeritus, kuid pole selge selle tegelik kasutegur, samas tähendab see selgelt suuremaid kulusid. 2. Euroopa Komisjon on öelnud, et nende eesmärk ei ole teha ENISA-st CSIRTi, mis reageerib intsidentidele. On arusaadav, et ENISA roll CSIRT võrgustikus (edaspidi: CNW) on suurem kui ainult sekretariaadi oma. Sestap soovitame sõnastada ettepanekus ENISA rolli CNW-s palju täpsemalt ning ühes ääremärkusega, mis kirjeldab, mida tähendab, et ENISA on CNW liige ja milles seisnevad selle liikmelisusega kaasnevad õigused ja ülesanded. Tähelepanu tasub pöörata ka asjaolule, rahvusvahelised partnerid ei pruugi üheselt mõista, mida tähendab, et ENISA on CNW liige - võib jääda väärarusaam, et ENISA on üks Euroopa Liidu CSIRTidest, isegi kui CSA2 järgi ta seda ei ole.	**Võtame arvesse**
7.3	3. ENISA suurem roll tähendab ka suuremat ja intensiivsemat koostööd liikmesriikidega. CSA2 näeb ette NLO ja SNE-d, kuid tuleb arvestada, et spetsialistid CSIRT-is, järelevalves ja riskianalüütikud on erinevad inimesed - ei saa vaid ühe-kahe inimese peale üles ehitada kogu sisulist koostööd. Koostöö tugineb inimestel ja see tähendab lisaks kirjalikule suhtlusele ka reisikulusid - kuidas neid kaetakse. Tagajärjeks võib olla väiksemate riikide kõrvale jäämine ja marginaliseerumine.	**Võtame arvesse**

7.4	4. CSA2 ütleb, et ENISA hakkab komisjoni nõustama ja abistama ELi küberpoliitika ja väljatöötamisel (artikkel 4). Varem oli kirjas ainult "policies", nüüd ka "legislation". Ehk siis ENISA-l oleks suurem roll küberõiguse väljatöötamisel, samas artikkel 1 rõhutab jätkuvalt sõltumatust. Tekib küsimus, mida “assist” hõlmab ja kui suures mahus ning intensiivsusega hakkab ENISA õigusloomesse panustama. Selline mandaat muudab hägusaks piiri rakendusasutuse ja seadusandliku võimu vahel, andes kvaasi-seadusandlikud õigused. Samas ei ole ENISA-l samaväärset vastutust kui on seda Komisjonil. Samal ajal luuakse artikliga 10 senisest suurem operatiivse koostöö mandaat: koostöö toetamise asemel hakkab ENISA rohkem ise ka ülevaadetesse ja olukorra teadlikkuse panustama.	**Võetud teadmiseks** Vt seisukohta seletuskirja punktis 6.2.
7.5	5. Artikkel 11(1)(g) sätestab, et ENISA analüüsib ka lunavara meetodite, nõuete ja mõju trende. Mõistetav on vajadus piiriülese informatsiooni ja tervikvaate järgi, mis võimaldaks teha põhjendatud ning otstarbekaid poliitikaotsuseid. Teisalt juhime tähelepanu, et ENISA analüüsid on kõrge abstraktsustasandiga, ei sisalda tundlikku, kuid tihti olulist teavet ning valmivad pika ajaperioodi peale olles seega valmimise ajaks tihti teatud määral aegunud. Seega tasub sellise ülesande ettenägemisel arvestada eeltoodud piirangutega ning arvestada, et selline analüütika saab ennekõike informeerida kõrgema tasandi poliitikaotsuseid, kuid pole ilmselt suure kasuteguriga operatiivsele tasandile.	**Võetud teadmiseks** Vt seisukohta seletuskirja punktis 6.2.
7.6	6. Mitmes sättes on sisse toodud ja rõhutatud Europoli ja ENISA koostöö. Koostöö eeldab usaldust ja head infovahetust. Tuleb arvestada, et Europol ja CSIRT-id tegutsevad erineva loogika alusel. CSIRT-ide toimise eeldus on kiirus, konfidentsiaalsus ja neutraalsus, samas kui Europol lähtub uurimis- ja tõendamisraamistikest. Praktikas on näiteks	**Võetud teadmiseks**

	CSIRT-võrgustikus üleval probleem õiguspärase ligipääsu küsimusega, mille puhul pole Europol suutnud liikmesriikidele tõestada, kuidas nad saavutavad ligipääsu andmetele ilma küberturvalisuse põhimõtteid rikkumata. Seega on koostöö eelduseks selged piirid ja tagatised, mida praegune ettepanek ei adresseeri. See omakorda tähendab, et koostöö võib jääda vaid formaalseks.	
7.7	7. Artikkel 12 näeb ette varase hoiatuse (*early alerts*) süsteemi. Küsimus on, kas süsteem teatud määral ei dubleeri juba olevasolevaid teavitusskeeme (CNW-s, CERT-EU). Teiseks, arvestades, et ENISA tugineb kaudsele infole, on küsimus, kuidas tagatakse, et teavitused on piisavalt operatiivsed ja informatiivsed. Lisaks on osa teavitussüsteemist ka soovituste tegemine. Näeme siin teatavat ohukohta kui ENISA, kes ei seira EE küberruumi, teeb soovitusi meie ettevõtetele teadmata kõiki olulisi asjaolusid ja nimetatud soovitused ei ole kohandatud vastavatele oludele. Lisaks võib siin tekkida olukord, kus riiklik CSIRT jääb välja oluliselt infovahetusest ja kontaktist üksusega.	**Arvestatud** Vt seisukohta seletuskirja punktis 6.2.
7.8	8. Lisaks on neil ettepaneku kohaselt konkreetne roll (*shall assist*) ka lunavararünnetele vastamise osas (artikkel 13(3). Kuigi on toodud, et see toimub koostöös CSIRT-idega, jätab see ebamääraseks koostöö vahekorra ja jätab õhku küsimuse, kas ENISA hakkab nende eest või nendega paralleelset lunavara intsidentidele reageerima. See on laiem küsimus sellest, kas ENISA-l on liikmesriike toetav roll või hakkab ENISA-st saama/kujunema CSIRT. Kuigi Komisjon on seda eitanud, näitavad kõnealused mandaadilaiendused teistpidist suundumust. Konkreetsemalt näeme siin ohtu tungida CSIRTi ja riigi pädevuses. Säte viitab küll koostööle CSIRT-idega, kuid ei sisalda selget nõuet liikmesriigi nõusolekule, mida on kasutatud muudes sätetes.	**Arvestatud** Vt seisukohta seletuskirja punktis 6.2.

7.9	9. Artikkel 13(3) sätestab ka, et "*For that purpose, ENISA shall establish a helpdesk and in particular make use of the enhanced shared situational awareness of the cyber threat and incident landscape pursuant to Article 11(1), first subparagraph, points (a) and (g) of this Regulation."* Sellest võib järeldada, et ENISA hakkab pakkuma osaliselt SOC teenust. Sellega seoses tekib taas küsimus riikliku CSIRTi ja ENISA tegevuse kattuvusest või põrkumisest. Tekstist ei selgu, kuidas toimub koordinatsioon operatiivse toe pakkumisel ning kuidas toimub infovahetus. Tekib oht, et oluline informatsioon ei jõua seetõttu CSIRT-ini või, et üksus saab riiklikult ja ENISA tasandilt erinevaid suuniseid. Samuti on küsitav, millise kvaliteediga tuge saab ENISA tasandilt pakkuda, arvestades, et spetsiifiline teadmus oludest on siiski riiklikul tasandil.	**Arvestatud** Vt seisukohta seletuskirja punktis 6.2.
7.10	Euroopa küberturvalisuse sertifitseerimisraamistiku lihtsustamine 10. Sertifitseerimisraamistik näeb ette liikmesriikidele kohustuse aktsepteerida sertifikaate ilma õiguseta täiendavalt auditeerida. 11. Tuleb arvestada, et keskselt väljatöötatud sertifitseerimisskeem ei pruugi piisaval määral ajaga kaasas käia ning esitatavad nõuded on kompromiss erinevate lävendite vahel. Arvestades liikmesriikide siiski erinevat küberturvalisuse taset ei ole vastuvõetav ega mõistlik panna kohustust tingimusteta sellist sertifikaati aktsepteerida ning säilima peaks võimalus vajadusel täiendavalt auditeerida nõuetele vastavust. 12. Lisaks tuleb silmas pidada vastavushindamisasutuste (conformity assessment bodies, CAB) võimalikku erinevat praktikat, mis võib kaasa tuua kohtalluvuse valimist (f*orum shopping*) lähtuvalt soodsamaist praktikast. Kuigi on	**Selgitame** Ettepaneku artikli 88 kohaselt peavad riigid määrama riikliku(d) küberturvalisuse sertifitseerimise asutuse(d). Tollel asutusel on ettepaneku artikli 88 lõike 6 punktide b ja c kohaselt järgmised ülesanded: *b) nad teevad Euroopa küberturvalisuse sertifitseerimise kavade üle järelevalvet ja tagavad nende nõuete täitmise kooskõlas artikli 81 lõike 2 punktiga a eesmärgiga tagada IKT-toodete, -teenuste, -protsesside, hallatud turbeteenuste ja üksuste turvaoleku vastavus nende Euroopa küberturvalisuse sertifikaatide nõuetele, mis on väljastatud nende vastavatel territooriumidel, koostöös asjaomase turujärelevalve- või järelevalveasutusega, sh pädevate asutustega Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 või määruse (EL) 2024/2847 alusel;* *c) nad teevad nende vastaval territooriumil asutatud ning vastava Euroopa küberturvalisuse sertifitseerimise kava kohaselt vastavuse enesehindamist tegevate käesolevas määruses sätestatud IKT-*

	ettenähtud mehhanism CAB-i tegevuse nõuetele vastamiseks (artikkel 94), on see selgelt ajakulukas protsess mis ei võimalda tagasi pöörata juba tehtud otsuseid. Ehk ettenähtud usaldus sertifikaatide vastu on suur, kui kontrollimehhanismid on kaudsed ja nõrgad. 13. Fundamentaalsemal tasemel võib sertifikaadi tingimusteta ja täiendava kontrollita aktsepteerimise kohustus olla vastuolus liikmesriikide pädevusega julgeoleku küsimustes. Küberturvalisusel on oluline koht riigi julgeolekus. Pandud kohustus välistab aga riigi võimaluse välistada mingeid tehnoloogiaid või teostada efektiivset kontrolli. Seega tõstatub küsimus, kas ettenähtud raamistik on kooskõlas Euroopa Liidu toimimise artikliga 4(2), eeskätt selle viimase lausega.	*toodete, -teenuste, -protsesside või hallatud turbeteenuste tootjate või pakkujate või sertifitseeritava turvaolekuga üksuste kohustuste täitmise üle järelevalvet ning tagavad nende kohustuste täitmise koostöös asjaomaste turujärelevalveasutustega;* Sama artikli lõike 7 punktide b, c ja e kohaselt on nendel asutustel vähemalt järgmised volitused: *b) uurida auditi vormis vastavushindamisasutusi, Euroopa küberturvalisuse sertifikaadi omanikke ja ELi vastavusdeklaratsiooni väljaandjaid, et kontrollida nende poolt käesolevas jaotises sätestatud nõuete järgimist;* *c) võtta asjakohaseid meetmeid vastavalt liikmesriigi õigusele tagamaks, et vastavushindamisasutused, Euroopa küberturvalisuse sertifikaadi omanikud ja ELi vastavusdeklaratsiooni väljaandjad järgivad käesoleva määruse ja Euroopa küberturvalisuse sertifitseerimise kava nõudeid;* *e) tunnistada liikmesriigi õiguse kohaselt kehtetuks Euroopa küberturvalisuse sertifikaadid, mille on välja andnud riiklikud küberturvalisuse sertifitseerimise asutused või vastavushindamisasutused kooskõlas artikli 85 lõikega 4, kui need sertifikaadid ei vasta käesolevale määrusele või Euroopa küberturvalisuse sertifitseerimise kavale;* Sama artikli lõike 8 kohaselt *[r]iiklikud küberturvalisuse sertifitseerimise asutused teevad omavahel ja komisjoniga koostööd, eelkõige vahetavad teavet, kogemusi ja häid tavasid seoses IKT-toodete, -teenuste ja -protsesside, hallatud turbeteenuste ja üksuste turvaoleku küberturvalisuse sertifitseerimisega ning küberturvalisust puudutavate tehniliste küsimustega.* Kehtiva küberturvalisuse määruse kontekstis on vastava ülesande täitja Tarbijakaitse ja Tehnilise Järelevalve Amet (vt küberturvalisuse seaduse § 13[1]).

		Lisaks vt ka küberturvalisuse 2. direktiivi muudatusega seotud seisukohta, mis on seotud direktiivi artikli 21 lõikega 5. Vt ka seisukohta seletuskirja punktis 6.13.
7.11	IKT tarneahela turvalisuse raamistik 14. Laias laastus IKT tarneahela turvalisuse raamistik (98-105) tegeleb mitte-tehniliste riskide maandamisega kõrge kriitilisusega sektorite tarneahelates ja meetmed kehtiksid NIS2 I ja II lisa üksustele. Artikkel 100 kohaselt saab määratleda kolmandaid riike küberturvalisuse vaatest riskiriigiks (designation of third countries posing cybersecurity concerns). Oluline on ka see, et sinna alla ei lähe ainult kolmandate riikide firmad, vaid ka firmad mis on kolmanda riigi kontrolli all või nt mille omanik on kolmanda riigi kodanik. 15. Üldiselt toetame riskiriikide määramise mehhanismi, sest see annab võimaluse vähendada kriitilises infrastruktuuris sõltuvust kõrge riskiga riikide tootjate tooteid. RIA vaatest pigem positiivne, et aktsepteeritakse, et tarneahela riskid on laiemad, kui kitsas mõistes tehnoloogilised.	**Arvestatud**
7.12	16. Ettepanek annab otsustuspädevuse kolmandate riikide määramiseks küberturvalisusele ohtu kujutavateks riikide hulka Komisjonile. Liikmesriigid küll panustavad läbi ohuhinnangu ja konsultatsioonide, kuid nende roll jääb selgelt nõuandvaks. Seejuures ei näe raamistik ette võimalusi ei leevendusteks ega ka liikmesriigi poolseks karmimaks lähenemiseks (kuigi art 98(3) näeb ette justkui vastava õiguse, on see allutatud ühisturu nõuetele). Juhime tähelepanu, et kuna otsustel on suure tõenäosusega lisaks mõjule julgeolekule ka oluline majanduslik mõju, on ka arvestatav risk protsessi politisserumisele, mis omakorda võib õõnestada selle usaldusväärsust.	**Arvestatud** Vt seisukohta seletuskirja punktis 6.8.

7.13	17. Artikkel 103 näeb ette, et komisjon võib rakendusaktiga ette näha seadmed ja komponendid, mille kasutamine on NIS2-s ettenähtud sektorites tegutsevatele ettevõtetele keelatud, ning anda neile üleminekuks tähtaja. Kui peab hakkama vahetama välja tooteid, siis millised on eeldatavalt need tähtajad ja kas sellele tuleb ka mingi täiendav EL-i tugi?	**Selgitame** Küberturvalisuse 2. määruse ettepaneku artikli 103 lõike 1 teine lause sedastab: "Kõnealustes rakendusaktides nähakse ette sobilikud üleminekuperioodid, mille vältel komisjon avaldab artiklis 104 osutatud suure riskiga tarnijate loetelud, ning täiendavad ajavahemikud asjaomaste IKT-komponentide ja IKT-komponente sisaldavate komponentide järkjärguliseks kasutusest kõrvaldamiseks." Vt seisukohti seletuskirja punktides 6.8. ja 6.14.
7.14	18. [Artikli] 99(1) kohaselt võib Komisjon või 3 liikmesriiki algatada, et NIS CG viiks läbi riskianalüüsi. Sätte alusel on silmas peetud süvitsi, põhjalikku riskihindamist, kuid samas on ajaraam vaid kuus kuud. RIA vaatest tekitab küsimusi NIS CG raames võimekus sellist hindamist läbi viia. Täna ei ole RIA panus NIS CG-sse FTE-de mõttes sellises mahus, et sisukalt sellisesse riskihindamisse panustada; küsitav on, kas teistegi riikide panus seda võimaldab. Seega eeldab selline raamistik riikide, sh Eesti suuremat panust NIS CG-sse. 19. Segaseks jääb protsessi n-ö omanik – kuigi NIS CG justkui viib seda läbi, on Komisjonil arvestatavad hoovad selle üle. Lisaks, riskihindamisel on oluline kaal kuna sellest sõltub hilisem kõrge-riskiga tootjate määratlemine, seega on liikmesriikide panusel väga oluline kaal, kuid kontroll protsessi üle on minimaalne (läbi NIS CG).	**Selgitame** Selles artiklis viidatud küberturvalisuse 2. direktiivi artikkel 22 ei määratle hetkel tähtaega, mis ajaks tuleb vastav riskianalüüs läbi viia.
7.15	NIS2 direktiivi ettepanekud 1. On tervitatav, et teatud üksuste kategooriaid täpsustatakse. Samas oleks hädavajalik, et täpsustataks mõisteid laiemalt. Näiteks järelevalve mõisted (ad hoc audit, targeted audit, and regulaar audit). Mõisted peaks olema kooskõlas ka standardiseeritud terminoloogiaga. Praegu kasutatav terminoloogia, mis pole ühegi turbevaldkonna terminoloogiaga	**Arvestatud**

	süstemaatiliselt kooskõlas. Sellegi korrastamine on täiesti välja jäänud teema ja probleemid aina progresseeruvad.	
7.16	2. Keskmise suurusega ettevõtte kategooria asendamine *Small mid-cap* kategooriaga a. Ettepanek ei võta laias laastus arvesse väiksemate riikide turuolukorda. Eestis kukuvad enamus ettevõtteid alla selle piiri. See omakorda tähendab, et enamus direktiivi lisas I toodud valdkondades tegutsevad ettevõtted jäävad üliolulise üksuse regulatsiooni alt välja ja seega ei ole kohustatud võtma ka vastavaid turvameetmeid ning nende üle järelevalve on võimalik teostada vaid *ex post* ehk kui midagi on juba juhtunud. b. Ettevõtete suuruste määratluse muutmine selleks, et skoopi vähendada, jätab tähelepanu alt aga välja ettevõtete mõju proportsionaalsuse ja sõltuvuse digitaalsest elemendist, võrgu- ja infosüsteemidest. See jookseb ka peamise kriitikana NIS2 kohta läbi teaduskirjandusest.	**Selgitame** Jah, selle tulemusena jääksid Eestis paljud direktiivi I lisas olevad ettevõtjad üliolulise üksuse regulatsiooni alt välja, sh muutuks ka nende üksuste suhtes järelevalve režiim rohkem reageerivaks. Samas see ei tähenda, et see muudab turvameetmete kohaldamise nõuet - kehtiva küberturvalisuse 2. direktiivi artiklis 21 pole hetkel sätestatud ning ettepanekuga seda artiklit ei muudeta viisil, et üliolulliste ja oluliste üksuste puhul toimuks erinev lähenemine turvameetmete (direktiivi sõnastuses "riskijuhtimismeetmete") kohaldamisele.
7.17	3. Artikliga 5 nähakse ette, et kui Komisjon on andnud rakendusmääruse art 21(5) alusel, kuulub kohaldamisele viimati nimetatu ning liikmesriigid ei või kehtestada täiendavaid nõudeid. Sellisele regulatsioonile oleme kindlasti vastu. Liikmesriikidel peab jääma võimalus kehtestada täiendavaid nõudeid, pidades silmas riigi eripära. Praegusel juhul oleks välistatud näiteks Eesti-spetsiifilised turvanõuded valdkonna üksustele, kellele on kehtestatud ka rakendusmäärus. Samuti kaasneb selle ettepanekuga kinni kirjutamise oht – olukorras, kus rakendusmäärus ei ole enam ajakohane, ei ole sellise regulatsiooni korral võimalik riigil kehtestada selle kategooria üksustele aja- ja asjakohasemaid nõudeid. Küsitav on aga komisjoni võime asjakohaseid tehnilisi, metodoloogilisi sektoripõhiseid nõudeid kehtestada piisava agiilsusega, et need oleksid ja jääksid asjakohaseks. Praegu on ühe rakendusakti sektorina välja toodud ka	**Arvestatud**

	pilvandmetöötlusteenuse osutajad ja andmekeskusteenuse osutajad – RIA hinnangul ei ole rakendusmäärus piisav, pidades silmas ka Eesti digiriigi eripärasid ja täiendavaid, riigispetsiifilisi nõudeid. Samas marginaliseerub E-ITS ja seeläbi ka muud kohalikud ettevõtluse algatused (Cybsis, Kordon, PlanPRO jne). Siin võiks jääda valdkondlike soovituslike standardite tasemele ja mitte üle reguleerida.	
7.18	4. Küberturvalisuse seisundi (cyber posture) sertifikaadi osas vt kommentaare ülalt seoses sertifitseerimisraamistikuga.	**Võetud teadmiseks**
7.19	5. Praegu ettenähtud ülevõtmisaeg 12 kuud on ilmselt liiga lühike periood, arvestades, et üleminek ja kohanemine seniste muutustega kestab veel pikalt.	**Arvestatud**
	8. Tarbijakaitse ja Tehnilise Järelevalve Ameti arvamus 31.06.2026 kiri nr 2-3/2026/0380	
8.1	Tarbijakaitse ja Tehnilise Järelevalve Amet (edaspidi TTJA) toetab küberturvalisuse paketis toodud eesmärke ja pakutud lahendusi eelkõige Euroopa Liidu Küberturvalisuse Ameti (edaspidi ka ENISA) mandaadi tugevdamisel ja küberturvalisuse sertifitseerimisraamistiku lihtsustamisel.	**Võetud teadmiseks**
8.2	1. Ettepaneku artikkel 2 Ettepaneku artiklis 2 on esitatud mitu uut definitsiooni, mis on seotud elektrooniliste sidevõrkude ja raadioside tehniliste aspektidega. Nende definitsioonide praktiline roll ettepaneku ülejäänud tekstis ei ole hetkel piisavalt selge, kuivõrd ettepanekus neid rohkem ei kasutata. Täiendavat selgitamist vajaks asjaolu, kas neid definitsioone on kavas kasutada edaspidi rakendusaktides (sealhulgas sertifitseerimisskeemides).	**Selgitame** Vastab tõele, et mujal ei ole neid definitsioone kasutatud, kuid paraku ei ole ka hetkel teada, kus ja millises kontekstis neid võidakse kasutada. Vt ka seisukohta seletuskirja punktis 6.1.
8.3	2. Ettepaneku artikkel 47 Ettepaneku artikkel 47 näeb vastavushindamise asutustele ette sertifikaatide väljastamisega seotud tasud, mis laekuvad ENISA eelarvesse. TTJA hinnangul suurendab selline lahendus	**Arvestatud** Vt seisukohta seletuskirja punktis 6.5.

	sertifitseerimise kogukulu ning kandub lõppastmes edasi tarbijahindadesse. Ettenähtud tasude süsteem võib pidurdada Euroopa küberturvalisuse sertifitseerimise arengut, eelkõige nendes liikmesriikides (nagu Eesti), kus vastavushindamise asutuste turg on alles kujunemisjärgus. Seetõttu palume täiendavalt hinnata, kas kavandatud tasude süsteem on praeguses arengufaasis proportsionaalne ja kas see toetab regulatsiooni eesmärke	
8.4	3. Ettepaneku artikkel 74 Ettepaneku artikkel 74 kohustab ENISA-t valmistama pärast komisjoni vastava taotluse saamist sertifitseerimisskeemi ette 12 kuu jooksul. Leiame, et kõikide sertifitseerimisskeemide puhul ei pruugi see tähtaeg olla realistlik. Arvestades vajadust koguda arvamusi huvirühmadelt ja Euroopa küberturvalisuse sertifitseerimisrühmalt (ECCG) võib sertifitseerimisskeemi valmistamine nõuda põhjendatult pikemat aega. TTJA hinnangul tuleks kaaluda tähtaja põhjendatud juhtudel pikendamise võimalust.	**Võetud teadmiseks** Vt seisukohti seletuskirja punktides 6.7 ja 6.8.
8.5	4. Ettepaneku IV jaotis Peame vajalikuks selgitada, mida täpsemalt hõlmab ettepaneku IV jaotises sätestatud IKT tarneahela turvalisuse regulatsioon. Eelkõige vajab selgitamist, kas kohaldamisala hõlmab ka IKT kasutajaseadmeid või üksnes võrguseadmeid ja nende komponente. TTJA hinnangul peaks kolmandatest riikidest pärinevate IKT kasutajaseadmete puhul üldjuhul piisama sellest, et need vastavad küberkerksuse määruse (EL) 2024/2847 nõuetele.	**Selgitame** Küberkerksuse määrus käsitleb tehnilisi riske ja küberturvalisuse 2. määrus keskendub mittetehnilistele riskidele ehk siis need täiendavad üksteist. Toode võib täita ära kõik küberkerksuse määruse tehnilised nõuded, kuid siiski langeda riskiriigi nimekirja, kuna CSA2 käsitleb mittetehnilisi riske.
	9. Eesti Maaülikooli arvamus 12.03.2026 kiri nr 5.1-14/1406-1	
9.1	Eesti Maaülikool (edaspidi: ülikool) toetab Euroopa Liidu küberturvalisuse paketi üldisi eesmärke tugevdada ELi kübervastupidavust, vähendada liikmesriikide vahelist	**Võetud teadmiseks**

	killustatust ning parandada IKT-tarneahela turvalisust. Peame oluliseks, et regulatsioonide rakendamisel järgitaks proportsionaalsuse põhimõtet ning välditaks dubleerivat halduskoormust, mis ei suurenda sisuliselt turvalisust, kuid tekitab märkimisväärseid lisakulusid.	
9.2	Ülikool taotleb ISO/IEC 27001 (edaspidi: ISO 27001) sertifikaati eesmärgiga kehtestada rahvusvaheliselt tunnustatud ja riskipõhine infoturbe juhtimissüsteem. ISO 27001 rakendamine tuleneb nii kehtivast küberturvalisuse seadusest kui ka ülikooli rahvusvahelisest tegevusmudelist, mis eeldab võrreldavat ja usaldusväärset turberaamistikku rahvusvaheliste partnerite ees. Sertifitseerimine toimub täielikult ülikooli oma vahenditest ning ülikool ei ole saanud kasutada eraldi riiklikke toetusmeetmeid. Samuti ei ole riigisisene E-ITS raamistik rahvusvahelise ülikooli kontekstis täiel määral rakendatav. ISO 27001 ja NIS2 põhinevad samadel alustel: riskijuhtimine, juhtkonna vastutus, tarneahela turvalisus, intsidentide haldus ja pidev parendamine. Seetõttu peab ISO 27001 sertifitseeritud infoturbe juhtimissüsteemi käsitlema NIS2 nõuete täitmise alusraamistikuna. Kui ISO 27001 sertifikaati NIS2 rakendamisel ei arvestata, tekib olukord, kus ülikool peab looma paralleelsed protsessid, dubleeriva aruandluse ja täiendavad auditimehhanismid, mis oleks ebamõistlikult kulukas ning vastuolus halduskoormuse vähendamise eesmärgiga.	**Võetud teadmiseks ja selgitame** Küberturvalisuse 2. direktiivi põhjendus 79 sedastab, et võrgu- ja infosüsteemide turvalisuse tagamisega seotud riskijuhtimismeetmed peavad käsitlema erinevaid aspekte “kooskõlas Euroopa ja rahvusvaheliselt tunnustatud standarditega, näiteks ISO/IEC 27000 seeria standarditega”. Ka direktiivi artikli 21 lõike 5 alusel vastu võetud komisjoni rakendusmääruse (EL) 2024/2690 põhjenduses 3 on märgitud “Tulenevalt direktiivi (EL) 2022/2555 artikli 21 lõike 5 kolmandast lõigust põhinevad käesoleva määruse lisas esitatud küberturvalisuse riskijuhtimismeetmete tehnilised ja metoodilised nõuded Euroopa ja rahvusvahelistel standarditel, nagu ISO/IEC 27001, ISO/IEC 27002 ja ETSI EN 319401, ja tehnilistel nõuetel, nagu CEN/TS 18026:2024, mis puudutavad võrgu- ja infosüsteemide turvalisust.”. Too rakendusmäärus kohaldub ennekõike valitud üksustele (kes on rohkem seotud piiriüleste digivaldkonna teenustega). Eeltoodu ilmestab, et direktiivi artikliga 21 ette nähtud nõuete täitmise osas on võimalik rakendada ISO/IEC 27001 standardit ning taoline võimalus on ette nähtud ka Eestis teatud üksuste korral.[3]
9.3	Toetame ENISA rolli tugevdamist koordineeriva ja juhendava institutsioonina, EL-ülese sertifitseerimisraamistiku ühtlustamist ning IKT-tarneahela riskide süsteemset ja riskipõhist käsitlemist, kuna need meetmed suurendavad õigusselgust, vähendavad liikmesriikide vahelist killustatust	**Arvestatud**

[3] https://www.riigiteataja.ee/akt/127092025002, vt § 3 lõikeid 2 ja 2[1].

	ning aitavad kaasa turvalisemate ja usaldusväärsemate digilahenduste laialdasemale kasutuselevõtule. Samas on praktilise rakendatavuse seisukohalt oluline tagada selge üleminekuperiood olemasolevatele teenuslepingutele, eriti pilveteenuste osas, rakendada teadus- ja haridusasutuste suhtes selgelt proportsionaalsuse põhimõtet ning arvestada järelevalves ja vastavuse hindamisel ISO 27001 sertifitseeritud organisatsioonide küpsustaset, vältides dubleerivat sertifitseerimist olukorras, kus riskijuhtimine on juba tõendatult toimiv.	
9.4	Eesti-spetsiifiliste aspektidena juhime tähelepanu, et rahvusvahelise ülikoolina teeme tihedat koostööd kolmandate riikide partneritega, kasutame rahvusvahelisi teadustaristuid ning globaalset pilveinfrastruktuuri. Liiga jäik või formaalne tarneahela piirangute rakendamine võib kahjustada teaduskoostööd ning tuua kaasa märkimisväärseid aja- ja finantskulusid. Eestis puuduvad praegu sihitud toetusmeetmed, mis aitaksid kõrgkoolidel katta sertifitseerimise ja ülemineku kulusid. Seetõttu on eriti oluline, et juba rakendatud ja rahvusvaheliselt tunnustatud ISO 27001 sertifitseerimist arvestataks NIS2 rakendamisel sisulise vastavuse tõendina. Toetame küberturvalisuse paketi eesmärke ning vajadust tugevdada ELi vastupanuvõimet, kuid rõhutame, et ISO 27001 sertifitseeritud infoturbe juhtimissüsteemi mittearvestamine NIS2 rakendamisel tooks kaasa ebaproportsionaalse topeltkoormuse ega aitaks sisuliselt kaasa küberturvalisuse taseme tõstmisele. Palume Eesti seisukohtade kujundamisel arvestada rahvusvaheliste ülikoolide eripära, proportsionaalsuse põhimõtet ning standardite ja regulatiivsete nõuete sisulist kooskõla.	**Selgitame** Vt ka kommentaari 9.2 vastust.
9.5	Samuti palume ministeeriumil algatada arutelu riikliku toe või paindlike rakendusmehhanismide võimalikkuse üle teadus- ja	**Võetud teadmiseks**

	haridusasutustele, sealhulgas üleminekutoetuse või rahvusvaheliste projektide erimenetluse osas, et regulatsioon võimaldaks riskipõhist otsustamist automaatsete keeldude asemel, lubaks põhjendatud juhtudel kasutada kolmandate riikide teenuseid juhul, kui riskid on nõuetekohaselt hinnatud ja maandatud, ning näeks ette mõistliku üleminekuperioodi olemasolevatele lepingutele, vältimaks kohest ja kulukat migratsiooni. Kui ülikool suudab ISO 27001 raamistikus tõendada riskide süstemaatilist hindamist ja kontrolli, ei peaks regulatsioon automaatselt nõudma teenuse lõpetamist ega dubleerivat sertifitseerimist. Tegemist on proportsionaalsuse ja halduskoormuse vähendamise küsimusega, mis on kooskõlas ka paketi üldiste eesmärkidega.	
	10. Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu arvamus 31.03.2026 kiri nr 6.1-2/58	
10.1	ITL-i üldised seisukohad 1) Küberturvalisus on väga oluline valdkond ja selle regulatsioon on tervikuna selgelt vajalik. Kuna küberturvalisuse määrusega ei ole saavutatud soovitud eesmärke, siis toetame selle ülevaatamist ja muutmist. 2) Teeme ettepaneku võtta Euroopa Liidu (EL) küberturvalisuse paketi suuremaks eesmärgiks regulatsioonide päriselt lihtsustamine, sealhulgas kattumiste ja dubleerimiste vähendamine NIS2, finantssektori digitaalse tegevuskerksuse määruse (DORA), küberkerksuse määruse (CRA) ja muude asjakohaste raamistike vahel. See võimaldaks ettevõtetel ja asutustel suunata ressursid vastavuse tagamise ja tõendamise asemel meetmete rakendamisele, mis praktikas aitavad luua suuremat turvalisust. Kehtivad küberturvalisust ja digiteemasid reguleerivad õigusaktid on keerulised ja mahukad ning seepärast on neid rakendavatel organisatsioonidel raske mõista, millised on kõige olulisemad meetmed, mis tagaksid nende	**Võetud teadmiseks**

	turvalisuse. Kuna regulatsioonid on mahukad, siis ruumi lihtsustamiseks ja ühtlustamiseks neis jagub. 3) Uute täiendavate riskihaldusemeetmete kaalumisel ja kehtestamisel tuleb lähtuda sellest, et kõik kohuslased erinevates riikides oleks võimelised neid täitma. Nende regulatsioonide eesmärgiks tagada EL-i kõigis liikmesriikides turvalisuse ühtlaselt (harmoneeritult) kõrge tase. Kui ettevõtted tegutsevad mitmes riigis, siis tuleb praegu praktikas tegelda tegeliku turvalisuse tagamise asemel erinevate riikide regulatsioonide erisuste tuvastamise ning nendega kohandumisega. Seega tuleb regulatsioonide läbivaatamisel ja uuendamisel lähtuda minimaalsuse printsiibist ning sellest, et need ei tekitaks rakendamisel ülemäärast ressursikulu ega tekitaks ainult läbi erinevate nõuete täitmise kinnitamise eksitavat tunnet tegelikust turvalisusest. 4) Küberturvalisuse regulatsioone kehtestades ja muutes on oluline arvestada suuremat eesmärki milleks on õiguskindluse- ja selguse tagamine ning osapooltele aja andmine regulatsioonide sisuliseks rakendamiseks. Hetkel oleme olukorras, kus viimastel aastatel on vastu võetud mitmeid mahukad regulatsioone, mida juba on asutud muutma. Leiame, et oluline on lasta juba kehtestatud regulatsioonidel piisava ajaperioodi jooksul toimida. Seejärel teha nende mõjude ja tulemuste kohta analüüs mille järelduste põhjal saab otsustada muutmise vajalikkuse üle. Heitlik õigusruum kus toimuvad pidevad muudatused ja uute kohustuste kehtestamine nõuab nii era kui avalikult sektorilt ebavajalikke investeeringuid ja protseduuride muutmist. Tuleb jätta rohkem ruumi riskipõhiseks tegutsemiseks kuna see loob pidevalt muutuvas olukorras võimaluse paindlikult riske hallata mitte käituda nõuete, mis tegelikult põhinevad mineviku intsidentidel, järgi.	
10.2	ITL-i seisukohad CSA2 ettepaneku kohta:	**Selgitame**

	1. ENISA mandaadi uuendamine, uute ülesannete ja pädevuste lisamine ITL-ina tegime CSA ülevaatamise käigus ettepaneku, et ENISA-le ei määrataks uusi täiendavaid rolle, mis ei ole kooskõlas tema seniste võimekustega. Uute ülesannete lisamise asemel soovitasime ENISA-l keskenduda oma põhiülesannetele ja vältida liigset laienemist kõrvalteemadele, mis võivad takistada tõhusat tegutsemist põhivaldkondades ja nende arendamist. Konkreetsemalt leidsime, et ENISA peaks keskenduma EL-i küberturvalisuse valdkonna õigusaktide, nagu küberturvalisuse 2. direktiiv (NIS2), finantssektori digitaalse tegevuskerksuse määruse (DORA) ja küberkerksuse määruse (CRA) rakendamist abistavate tehniliste spetsifikatsioonide ning juhiste väljatöötamisele. CSA2 ettepanekuga ENISA rolli ei kitsendata, vaid reformitakse ja antakse uusi tegevusvaldkondi, näiteks seoses tarneahela turvalisuse ja oskustega. Seega on oht ENISA tegevuse fookuste veel suuremale hajumisele.	Vt seisukohta seletuskirja punktis 6.2.
10.3	ENISA kui üks teavituspunkt Kordame Euroopa Komisjoni avaldatud digivaldkonna lihtsustamispaketile ehk digiomnibussile ITL-i poolt 19.12.2025 esitatud tagasisides sisaldunud seisukohta mille kohaselt toetame erinevate intsidentide raporteerimiseks ühise keskkonna loomist. Novembris 2025 avaldatud nn digiomnibussi ettepanekus pakkus Euroopa Komisjon välja ühise teavitamiskanali loomise, et sama intsidendi puhul ei tuleks mitmes kohas ning mitu korda teavitada. Selline üks teavitamiskanal on kindlasti tervitatav, eriti piiriüleselt tegutsevate ettevõtete jaoks ning me toetame seda.	**Võetud teadmiseks ja selgitame** Siinsete eelnõude puhul sama Eesti seisukohta ei koostata, kuna see on juba koostatud[4] digiomnibussi eelnõude raames, mida on siinses protsessi võimalik taaskasutada.

[4] https://eelnoud.valitsus.ee/main/mount/docList/a4bbca3f-8cca-4bcb-af5b-6d6e15dbb143

	Hetkel peab mitmes Euroopa Liidu riigis tegutsev küberturvalisuse erinevate regulatsioonide alla langev ettevõte tegema teavitust kohalikele CERT-idele eraldi ja erinevatel dokumendi vormidel. Sealjuures tekib täiendav oluline ressursikulu ettevõttele iga riigi CERT-iga eraldi suhtlemisel, kui teavituse kohta tuleb lisaküsimusi. Ettevõtte jaoks läheb seega kaotsi intsidendi lahendamiseks vajalik aeg ning muud ressursid, kuna tuleb suhelda mitme asutusega teavituse teemal. Seetõttu toetame ülesandeid, mis ENISA-le antakse CSA2 ettepaneku artikliga 15. Seoses ühtse teavituskanaliga lisame, et lihtsustamise eesmärki silmas pidades tuleb olla ambitsioonikam ning ühtlustada ka teavitamise aegasid, vorme jm EL-i küberturvalisuse õigusaktides, kuna see hoiab kokku mitmes riigis tegutsevate ettevõtete ressursse.	
10.4	2. Sertifitseerimisskeeme puudutava regulatsiooni laiendamine ITL on järjepidevalt toetanud vabatahtlikke standardeid ja sertifitseerimist. CSA2 ettepanek võimaldab kehtestada kohustuslikke standardeid (art 71 lg 3). CSA2 ettepaneku kohaselt saaks tulevikus sertifitseerimisskeeme kasutada ettevõtte tegevuse nõuetele vastavuse tõendamiseks ja vastavuseelduse saamiseks asjakohastele ELi õigusaktidele. Kuivõrd see ei ole kohustus, siis leiame, et kohustusliku sertifitseerimise sätestamine ei ole vajalik. Iga õigusakti kohuslane saab tellida endale välise sõltumatu hinnangu, millega tõendatakse vastavust õigusaktidele. Täiendava sertifikaadi andmine ei tõsta vastavust tõendanud ettevõtte tegevuse kvaliteeti, küll aga suurendab bürokraatiat ja võib tõsta turule sisenemise barjääre.	**Selgitame** Vt seisukohta seletuskirja punktis 6.5.

	Lisaks võiks uus skeem hakata mõjutama ISO 27001, E-ITS või muude juba kehtivate ja tunnustatud sertifitseerimise skeeme. Seega pole mõistetav, et kui tekib uus sertifitseerimisskeem, mis on erinev vastavuse tõendamisest juba kehtivatele standarditele, siis milliste kriteeriumite põhjal peaks ettevõte otsustama, millise skeemi alusel sertifitseerimist teha. Samas küberkerksuse õigusakti (CRA) vaates on vaja selgust ja kaetust sertifitseerimisskeemidega, mis on täna veel puudu. Omaette küsimus on see kuidas tagatakse sertifitseerimisskeemide kirjeldused ja koolitused sertifitseerimisprotsessi läbiviijatele nii, et liikmesriigid oleksid CRA rakendamisega ajagraafikus. Kokkuvõtteks jääb meile arusaamatuks, miks soovitakse lisada CSA2 nõue uue sertifikaadi järele.	
10.5	3. Üldine raamistik turvalise IKT tarneahela jaoks CSA2 artiklitega 98 jj antakse Euroopa Komisjonile õigus kehtestada meetmeid, et tagada info-ja kommunikatsioonitehnoloogia (IKT) tarneahela turvalisus. Meile jääb väljapakutava regulatsiooni eesmärk arusaamatuks, kuna olemasolevad EL-i küberturvalisuse õigusaktid juba tagavad piisava juhendmaterjali ja tehniliste standardite olemasolu. Näiteks peavad ettevõtted ja asutused NIS2 täitmiseks viima läbi riskide hindamise ning sealhulgas tuleb hinnata ka tarneahela riske. Lähtudes hinnangu tulemustest tuleb rakendada vastavaid meetmeid. Tarneahela riskide hindamise üksikasjalikul reguleerimisel võib juhtuda, et see kaotab kiiresti oma ajakohasuse. Nimelt koostatakse regulatsioon olemasolevate tarneahelate näidete põhjal. Samas on iga uus tarneahel uut tüüpi juhtum ja seda ei ole võimalik ette kirjeldada. Kui organisatsioon(id) rakendavad riskipõhisuse põhimõtteid sisuliselt, mitte formaalselt	**Võetud teadmiseks** Olemasolevad EL-i küberturvalisuse õigusaktid pakuvad juba ulatuslikku juhendmaterjali ja tehnilisi standardeid. CSA2 lisandväärtus seisneb aga eelkõige mittetehniliste riskide käsitlemises valdkonnas, mida ELi tasandil on seni käsitletud suhteliselt piiratud ulatuses. Euroopa Liidu tasandil on kavas kehtestada miinimumnõuded, jättes liikmesriikidele võimaluse kehtestada siseriiklikult täiendavaid või rangemaid meetmeid.

	olemasolevate regulatsioonide alusel, ei ole vajadust täiendava regulatsiooni järele. Täiendavast regulatsioonist palju olulisem on tagada juba kehtivate regulatsioonide rakendamist abistava materjali ajakohasus ja praktiline tugi kohustatud subjektidele.	
10.6	4. Tarneahela turvalisuse erinormid elektroonilise side sektorile CSA2 ettepaneku artiklitega 110 ja 111 kehtestatakse elektroonilise side võrkude osas keeld kasutada suure riskiga tarnijaid ning see jõustuks hiljemalt 36 kuu pärast suure riskiga tarnijate nimekirja avaldamist. Põhimõttelisel tasandil on mõistetav keeld riikliku julgeoleku kaalutlustel kasutada kõrge riskiga tarnijaid elektroonilise side võrkude tuumiksüsteemides. Siiski on oluline arvestada, et tarneahela turvalisuse (kõrge riski määratlemine) EL-i tasandile tõstmine ning ettepanekus välja pakutud lühikesed üleminekutähtajad (36 kuud) tekitavad Euroopa ettevõtetele kindlasti olulisi riske. Näiteks seoses tarneahelate erinevate ülesehitustega, teostatavuse ja investeeringute mõistlikkusega. Samuti eeldab kõrge riskiga riikide nimekirjade kujundamine EL-i tasandil poliitilist konsensust, mis võib olla erinevate liikmesriikide vahel raskesti saavutatav. ITL-i ettepanekud ja küsimused artiklite 110 ja 111 osas on järgmised: 1) Teeme ettepaneku antud sätete rakendumise üleminekuaega pikendada ja siduda üleminekuaeg olemasolevate seadmete elueaga. Märgime, et CSA2 ettepanekus sisalduv väga lühike tähtaeg võib kaasa tuua tarneraskused ja tellimuste koondumise vähestele tarnijatele. Samuti suurendab see ettevõtete kulusid hüppeliselt (sh uued hanked, integratsioon, teenuse	**Selgitame** Vt seisukohta seletuskirja punktis 6.8.

	katkestustega seotud tegevused seadmete ümbervahetamisel jms). 2) Kuivõrd sideettevõtjad on hankinud seadmed ajal, mil nende kasutus oli lubatud ja on neid kasutanud õiguspäraselt, tekib küsimus ka enne nende tegeliku eluea lõppu väljavahetamisega seotud kulude hüvitamisest. Seda teemat ei ole CSA2 ettepanekus üldse käsitletud. 3) Lisaks tekitab küsimusi kõrge riskiga tarnija määramine. Kuivõrd selle nimekirja koostab CSA2 ettepaneku kohaselt Euroopa Komisjon koos liikmesriikidega lähtudes julgeolekukaalutlustest, ei hakka selle otsuse tagamaad olema läbipaistvad ettevõtjatele. Seetõttu jääb ettevõtjatele seadmeid hankides ebakindlus, millistele kriteeriumitele vastavalt täpselt võidakse Euroopa Komisjoni poolt mõni tarnija tulevikus lubamatuks või kõrgema riskiga tarnijaks lugeda. Seetõttu on ka eriti oluline, et üleminekuperiood oleks piisavalt pikk või alternatiivselt oleks sätestatud kompensatsioonimehhanism ja ettevõtjad saaksid teabe tarnija staatuse muutumisest võimalikult varakult. 4) Kahjuks on jätkuvalt ka väga palju lahtisi küsimusi, sest ei ole teada, mida täpselt hõlmavad komisjoni rakendusaktid. Lisaks on artikli 110 lõigete 4 ja 5 sõnastuse kohaselt Euroopa Komisjonil õigus, mitte kohustus vastu võtta rakendusakte, mis tekitab väga ebakindla olukorra. Samuti tekib küsimus, mis saab Euroopa Liidu 5G küberturvalisuse tööriistakastist (Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures), mis võeti vastu 2020. aastal liikmesriikide küberturvalisuse asutuste koostöö raames ning mille aluseks on Euroopa Komisjoni soovitus (EL) 2019/534 5G-võrkude küberturvalisuse kohta. 5) Lisaks tekkis praktilisi küsimusi. Kui keeld kohaldub komponentidele, siis kas hooldus ja tugiteenused on sama	

	tootja poolt siiski lubatud? Või kui tehakse tarkvarauuendusi nt juba kõrge riskiga tootja kasutuses olevale tarkvaral, kas see oleks lubatud?	
10.7	ITL-i seisukohad NIS2 muutmise ettepaneku kohta: 1. Subjektide nimekirja täpsustamine ja täiendamine ITL toetab, et täpsustakse NIS2 subjektide nimekirja. Mitmed subjektide kategooriad on kehtivas NIS2-s sõnastatud segaselt ja direktiivi ülevõtmisel on osutunud üheks raskemaks küsimuseks mõista, kes on NIS2 kohuslased. Kahjuks näeb NIS2 muutmise ettepaneku artikkel 1 punkt 1 ette vaid uute subjektide lisamise NIS2 artiklisse 2. Teeme ettepaneku, et artikkel 2 vaadatakse tervikuna üle ja täpsustatakse sisuliselt vastavalt liikmesriikide poolt esitatud küsimustele. Teeme ettepaneku viia NIS2 sisse muudatus, mis kohustab pädevat asutust teavitama ise kohuslasi, et nad on NIS2 kohuslased või pädeva asutuse poolt tehtud eelhinnangu kohaselt nad võivad osutuda NIS 2 kohuslasteks. Hetkel on selle osas liikmesriikides suur segadus ja erinev praktika, kuna paljud NIS2 kohuslased ei oska ennast määratleda subjektina ja seega ei rakenda ka vajalikke riskihalduse meetmeid. Leiame, et EL-is peaks subjektide määramine olema ühetaoline ning ettevõtted ja asutused ei peaks ise end subjektina üles andma.	**Selgitame** Osaliselt arvestatud – vt seisukohta seletuskirja punktis 6.1. Nende üksuste puhul, mis on seotud nn suuruse kriteeriumiga ehk kellele kohaldub komisjoni soovitus 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta, ei pruugi pädevatel asutustel olla piisavalt algandmeid ja andmeid, et teada konkreetse üksuse puhul tema seoseid selle soovituse kohaste partnerettevõtjate ja sidusettevõtjatega. Teave nendest seostest (sh nende ulatusest) on ennekõike teada konkreetsel üksusel, mitte pädeval asutusel. Seetõttu on kaheldav, kuivõrd on pädeval asutusel avalike andmete (nt üksuse majandusaasta aruannete ja tema võrgulehel olevate muude ülevaadete ja andmete) põhjal konkreetse üksuse asemel kindlaks teha, kas nn suuruse kriteeriumid (töötajate arvud ja/või finantsnäitajaid) on täidetud.
10.8	2. Üksuste subjektsuse lävendi tõstmine NIS2 muutmise ettepanekuga tõstetakse ülioluliste üksuste subjektsuse lävend keskmise suurusega ettevõtetelt (kuni 250 töötajat ja aastakäive kuni 50 miljonit eurot või bilansimaht kuni 43 miljonit eurot vastavalt Euroopa Komisjoni soovitusele (2003/361/EÜ) väikese keskmise turukapitalisatsiooniga ettevõteteni (kuni 750 töötajat ja aastakäive kuni 150 miljonit eurot või bilansimaht kuni 129 miljonit eurot vastavalt Euroopa	**Arvestatud** Vt seisukohta seletuskirja punktis 6.10.

	Komisjoni soovitusele (EL) 2025/1099). See tähendaks praktikas NIS2 mõttes ülioluliste üksuste arvu vähenemist. ITL-ina toetame seda muudatust.	
10.9	3. Täiendavate siseriiklike küberturvalisuse riskihalduse meetmete kehtestamise keeld Toetame NIS2 muutmise ettepaneku artikkel 1 punktiga 7 tehtavat muudatust (NIS2 art 21 lg 5 muutmine), mille kohaselt ei või liikmesriigid kehtestada täiendavaid nõudeid, kui Euroopa Komisjon on kehtestanud küberturvalisuse riskijuhtimismeetmed NIS2 art 21 lg 5 alusel. Hetkel kehtib Eestis kõigile küberturvalisuse seaduse subjektidele kohustus rakendada sõltuvalt suurusest kas esmaseid turvanõudeid või kohalikku E-ITS standardit, millega loetakse võrdsustatuks ka ISO 27001 sertifikaat. See tähendab, et NIS2 art 21 lg 5 alusel kehtestatud rakendusmääruse (EL) 2024/2690 subjektiks olevad digiteenuse osutajad peavad Eestis täitma lisaks kohalikke riskihalduse meetmeid (KüTS-i alusel kehtestatud turvameetmed). See tähendab topeltkoormust, erisuste otsimist ja nõuete võrdlemist. See omakorda viib suurema halduskoormuseni ja võimalik, et ka paralleelsete nõuete rakendamiseni. Piiriüleselt tegutsevate digiteenuste osutajate jaoks tähendab see riigikohaseid erisusi. Juhime tähelepanu, et osa rakendusakte on veel välja andmata, mistõttu ei ole selge, kas nendes sisalduvad nõuded oleksid leebemad või rangemad nendest, mida Eesti hetkel või tulevikus plaanib rakendada. Lisaks ei ole ka Komisjonile sätestatud tähtaega, millal vastavad rakendusaktid peaksid jõustuma. Teeme ettepaneku sätestada NIS2-s ka rakendusaktide vastuvõtmise tähtajad, et tagada õigusselgus.	**Jäetud arvestamata ja selgitame** Vt seisukohti seletuskirja punktides 6.13. ja 6.14.
10.10	4. Lunavara rünnakute andmete kogumine Hetkel kehtib NIS2 üle võtnud küberturvalisuse seaduse alusel kohustus teavitada küberintsidentidest. Leiame, et kehtivas	**Arvestatud osaliselt** Vt seisukohta seletuskirja punktis 6.16.

	regulatsioonis sisalduv kohustus katab ära ka lunavara rünnakud. NIS2 muutmise ettepanekus sisalduva eraldi lunavara rünnakuid (kui ainult ühte rünnaku viisi paljudest) puudutava regulatsiooni (NIS2 ettepaneku art 1 punkt 8) lisamine eraldiseisvalt ei muudaks olukorda. Seega tekkis küsimus, miks soovitakse lunavaraga seotud rünnakute eraldi regulatsiooni lisada. Kas hetkel kehtiv regulatsioon ei kata ära seda küberintsidendi osa? Samuti jääb ebaselgeks, millal (*upon request*) ja millises mahus andmeid täpselt soovitakse. Kui eraldi lunavara rünnakuid käsitlev regulatsioon jääb alles, siis teeme ettepaneku see põhjalikumalt lahti kirjutada. Näiteks võib makseandmete avaldamine kaasa tuua ettevõtjatele sanktsioonidega seotud riske, kui olid sunnitud siiski mingis olukorras lunaraha maksma isikutele, kes on seotud sanktsioneeritud jurisdiktsiooniga. Seetõttu oleks vajalik selge *safe harbour* klausel ettevõtjatele vastavate teavituste tegemisel.	
10.11	NIS2 muutmise ettepaneku kohta toome täiendava olulise teemana välja DORA rakendamise IKT teenuse osutajatele. Täname Justiits- ja Digiministeeriumit, et arvestasite Euroopa Komisjoni digiomnibussi määruse ettepanekule Eesti seisukohti koostades ITL-i ettepanekut lahendada küsimus NIS2 ja DORA paralleelsetest kohustustest IKT teenuse osutajatele. Teeme ettepaneku korrata seda seisukohta ka küberpaketile Eesti poolt tagasisidet andes. See teema on vaja lahendada, et vähendada ettevõtete halduskoormust ja lihtsustada regulatsioone. Kehtivate õigusaktide kohaselt on DORA subjektid vabastatud NIS2 täitmisest, kuid NIS2 subjektid, kes osutavad teenuseid DORA subjektidele, peavad DORA subjektide nõudel vastama	**Võetud teadmiseks ja selgitame** Siinsete eelnõude puhul sama Eesti seisukohta ei koostata, kuna see on juba koostatud[5] digiomnibussi eelnõude raames, mida on siinses protsessi võimalik taaskasutada.

[5] https://eelnoud.valitsus.ee/main/mount/docList/a4bbca3f-8cca-4bcb-af5b-6d6e15dbb143

	ka DORA-le. See tekitab NIS2 subjektidest IKT teenuse osutajatele, kes soovivad oma teenuseid osutada ka finantssektori asutustele, väga suurt halduskoormust. Seetõttu on ITL-i ettepanek muuta nii NIS2-te kui ka DORA-t selliselt, et NIS2 direktiivi kohuslased, kes osutavad finantssektori asututele IKT teenuseid, ei pea tõendama eraldi DORA-le vastavust, vaid need turvanõuded tunnistatakse samaväärseteks, kui nad vastavad NIS2 alusel kehtestatud nõuetele.	
10.12	Ettepanek võtta NIS2 artikkel 3 lõikes 4 sisalduvast loetelust, millist teavet peavad teenuse osutajad esitama, välja punkti f ehk IP-vahemikud. Me ei saanud ju Eestis NIS2 üle võttes tegelikult selgeks, milliseid IP-vahemikke mõeldakse. Nüüd aga tahetakse artikkel 27 lõikes 3 lühendada oluliselt seda teabe edastamise kohustust - 3 kuult 2 nädalani.	**Osaliselt arvestatud** Vt seisukohti seletuskirja punktides 6.1. ja 6.11.
	11. Eesti Kaubandus-Tööstuskoja arvamus 31.03.2026 kiri nr 4/68	
11.1	1. Regulatsioonide lihtsustamine ja koostoime Kaubanduskoja hinnangul on kriitilise tähtsusega, et küberturvalisuse paketi keskmes oleks tegelik regulatiivne lihtsustamine. Ettevõtted tegutsevad juba täna mitme paralleelse raamistikuga (nt NIS2, DORA, CRA), mille nõuded osaliselt kattuvad ning tekitavad märkimisväärset halduskoormust. Nagu ka ettepanekus on märgitud, on üheks eesmärgiks vähendada regulatiivset killustatust ja lihtsustada nõuete täitmist. Kaubanduskoda toetab seda eesmärki, kuid rõhutab, et praktikas peab see tähendama dubleerivate nõuete vähendamist, ühtlustatud aruandlust ja protsesse ning selget prioriseerimist, millised meetmed on tegeliku turvalisuse seisukohalt kõige olulisemad.	**Võetud teadmiseks**

11.2	2. Sertifitseerimine Küberturvalisuse määruse ettepanek sätestab Euroopa küberjulgeoleku sertifitseerimise raamistiku ning artikkel 71 lg 3 ütleb, et Euroopa küberjulgeoleku sertifitseerimine on vabatahtlik, kui liidu või liikmesriigi õigusaktides ei ole sätestatud teisiti. Toetame põhimõtet, et sertifitseerimine jääb vabatahtlikuks, kuna see võimaldab ettevõtetel valida oma tegevuse iseloomust ja riskitasemest lähtuvad sobivaimad lahendused. Samas tekitab küsimusi, miks on sellised sätted määrusesse lisatud olukorras, kus sertifitseerimine ei ole kohustuslik. On oht, et praktikas kujuneb vabatahtlik sertifitseerimine kaudselt kohustuslikuks läbi teiste õigusaktide, hangete või turuosaliste ootuste, mis võib omakorda suurendada ettevõtete haldus- ja finantskoormust. Seetõttu peab Kaubanduskoda oluliseks, et sertifitseerimise roll ja eesmärk oleksid selgelt põhjendatud ning et välditaks olukorda, kus vabatahtlikest mehhanismidest kujunevad siiski kohustuslikud nõuded ilma vastava mõjuanalüüsita.	**Võetud teadmiseks** Vt seisukohta seletuskirja punktis 6.5.
11.3	3. Subjektide nimekiri Kaubanduskoda toetab NIS2 direktiivi puhul ettepanekut tõsta oluliste üksuste subjektsuse lävend keskmise suurusega ettevõtetelt väikeste keskmise turukapitalisatsiooniga ettevõteteni (kuni 750 töötajat ja aastakäive kuni 150 miljonit eurot) (artikkel 1 p 2). See vähendab nii ettevõtete halduskoormust kui ka pädevate asutuste järelevalvekoormust. Lisaks oleme seisukohal, et NIS2 direktiivi muudatusettepanekutega tuleks ka täpsustada direktiivi subjektide nimekirja. Paljud kategooriad on kehtivas NIS2-s sõnastatud ebaselgelt ning direktiivi ülevõtmisel on see põhjustanud tõlgendamisraskusi, sest ei ole selge, millistele ettevõtetele kohalduvad NIS2 direktiivi nõuded ja millistele	**Selgitame** Vt kommentaaride 6.1 ja 10.7 vastuseid

	mitte. Seetõttu teeme ettepaneku vaadata üle tervikuna direktiivi subjektide nimekiri ning täpsustada seda vastavalt liikmesriikide poolt tõstatatud küsimustele. See aitaks vältida olukorda, kus ettevõtetel on jätkuvalt keeruline hinnata oma kuulumist NIS2 kohaldamisalasse. Samuti teeb Kaubanduskoda ettepaneku täiendada direktiivi sättega, mis kohustab liikmesriigi pädevat asutust teavitama ettevõtteid nende kuulumisest NIS2 reguleerimisalasse. Praegu on liikmesriikide praktika subjektide määramisel erinev, mistõttu oleks vajalik kehtestada ühtne lähenemine ka direktiivi tasandil. Kui ettevõtja peab ise oma subjektsust hindama, paneb see talle ebamõistliku koormuse. Leiame, et subjektide määramine peaks olema kogu EL-is ühtne ja selge ning see kohustus peaks lasuma riiklikul järelevalveasutusel, kellel on terviklik ülevaade turuosalistest.	
11.4	4. Liikmesriikide täiendavate nõuete keeld Kaubanduskoda toetab ettepanekut, mille kohaselt ei või liikmesriigid kehtestada täiendavaid tehnilisi, metoodilisi ega sektoripõhiseid nõudeid, kui Euroopa Komisjon on need juba NIS2 artikli 21 lõike 5 alusel rakendusaktidega kehtestanud (artikkel 1 p 7). See on oluline samm ühtse siseturu toimimiseks ning on eriti oluline piiriülese tegevusega ettevõtete jaoks, et vähendada nende halduskoormust.	**Jäetud arvestamata ja selgitame** Vt seisukohti seletuskirja punktides 6.13. ja 6.14.
	12. Eesti Tööandjate Keskliidu arvamus Kiri nr 1-3/59-1	
12.1	Eesti Tööandjate Keskliit toetab Euroopa Liidu eesmärki tugevdada liidu küberturvalisust ning suurendada digitaalse majanduse ja avalike teenuste vastupanuvõimet. Küberturvalisus on ettevõtluse ja ühiskonna toimimise seisukohalt kriitilise tähtsusega ning tõhus regulatiivne raamistik on vajalik.	**Võetud teadmiseks**

	Samas rõhutame, et küberturvalisuse regulatsioonide edasine arendamine peab olema proportsionaalne, õigusselge ja praktiliselt rakendatav, vältides topeltkoormust ning regulatiivset killustatust, mis ei paranda sisulist turvalisust, kuid suurendab märkimisväärselt haldus- ja kulukoormust. Oluline on arvestada Eesti organisatsioonide investeerimisvõimekusega ja arendusressursi võimalustega (nt küberturbe spetsialistide ja IT arendajate piisavus).	
12.2	1. Regulatiivne raamistik ja üldpõhimõtted Peame vajalikuks, et ELi küberturvalisuse raamistik lähtuks järgmistest põhimõtetest: 1) Regulatsioonide lihtsustamine ja kattuvuste vähendamine NIS2, DORA, CRA ja CSA2 vahel, et ettevõtted ja asutused ei oleks sunnitud täitma paralleelseid või sisuliselt kattuvaid nõudeid. 2) Õigusselgus ja regulatiivne stabiilsus – ettevõtjatele tuleb anda piisav aeg regulatsioonide rakendamiseks ning hoiduda olukorrast, kus värskelt kehtestatud reegleid hakatakse enne mõjude hindamist uuesti muutma. 3) Riskipõhine ja vähima vajaliku sekkumise printsiibile tuginev lähenemine, mis arvestab organisatsioonide tegelikku riskiprofiili, suurust ja tegevusvaldkonda. 4) Ühtne siseturg, kus piiriüleselt tegutsevad ettevõtted ei pea kohanema liikmesriikide erinevate tõlgenduste ja lisatingimustega.	**Selgitame** 1) nõustume põhimõttega, sh vt digiomnibussi eelnõude raames koostatud[6] seisukohti 1.1.1, 1.1.4, 1.3.1 ja 1.3.4 , mida on siinses protsessi võimalik taaskasutada. 2) Vt seisukohti seletuskirja punktides 6.8.ja 6.14. 3) võetud teadmiseks 4) võetud teadmiseks
12.3	2. Sertifitseerimine ja vastavuse tõendamine Eesti Tööandjate Keskliit on seisukohal, et küberturvalisuse sertifitseerimine peab jääma vabatahtlikuks. Täiendavate sertifitseerimisskeemide loomine ei tohi viia de facto	**Selgitame** Vt seisukohta seletuskirja punktis 6.5. ISO/IEC 27001 osas vt kommentaari 9.2 vastust.

[6] https://eelnoud.valitsus.ee/main/mount/docList/a4bbca3f-8cca-4bcb-af5b-6d6e15dbb143

	kohustuslikkuse tekkeni ega suurendada bürokraatiat ilma sisulist turvalisust parandamata. Rahvusvaheliselt tunnustatud standardeid, eeskätt ISO/IEC 27001, tuleb käsitleda sisulise vastavuse alusena NIS2 ja teiste küberõigusaktide rakendamisel. Vastavuse tõendamine ei tohiks nõuda paralleelsete auditite, protsesside ja aruandlussüsteemide loomist olukorras, kus riskijuhtimine on juba tõendatult toimiv. Eriti oluline on see rahvusvaheliselt tegutsevate organisatsioonide, sh teadus- ja haridusasutuste ning piiriüleste teenusepakkujate puhul.	
12.4	3. ENISA roll ja ülesanded Toetame ELi tasandil küberturvalisuse koordineerimist, kuid rõhutame, et: 1) ENISA roll ei tohi liigselt laieneda viisil, mis hajutab agentuuri fookust või dubleerib liikmesriikide pädevate asutuste, standardiorganisatsioonide ja turuosaliste tegevust. 2) Prioriteet peab olema kehtivate õigusaktide rakendamist toetava praktilise juhendmaterjali ja tehniliste suuniste arendamine. 3) Uute ülesannete lisamisel tuleb hinnata nende tegelikku lisandväärtust ning mõju halduskoormusele.	**Arvestatud** Vt seisukohta seletuskirja punktis 6.2.
12.5	4. Intsidentide teavitamine ja menetluste ühtlustamine Toetame ühtse ELi-ülese intsidentide teavitamise kanali loomist, kuna see aitab vähendada dubleerivat raporteerimist ja ressursikulu, eriti piiriüleste ettevõtete puhul. Samas rõhutame, et: 1) teavitamise tähtajad, vormid ja protseduurid tuleb ühtlustada kõigis asjakohastes ELi küberturvalisuse õigusaktides;	**Võetud teadmiseks ja selgitame** Siinsete eelnõude puhul sama Eesti seisukohta ei koostata, kuna see on juba koostatud[7] digiomnibussi eelnõude raames, mida on siinses protsessi võimalik taaskasutada.

[7] https://eelnoud.valitsus.ee/main/mount/docList/a4bbca3f-8cca-4bcb-af5b-6d6e15dbb143

	2) eesmärk peab olema ettevõtjate koormuse vähendamine kriisiolukorras, mitte uute formaalsete kohustuste lisamine.	
12.6	5. IKT tarneahela turvalisus ja kõrge riskiga tarnijad Mõistame vajadust käsitleda IKT tarneahelas ka mitte tehnilisi riske, kuid peame oluliseks, et: 1) võimalikud piirangud või keelud põhineksid läbipaistvatel, selgelt määratletud kriteeriumitel; 2) üleminekuperioodid oleksid piisavalt pikad ning seotud olemasolevate seadmete elutsükli ja amortisatsiooniga; 3) arvesse võetaks ettevõtjate õiguspärast ootust olukorras, kus seadmed on hangitud ajal, mil nende kasutamine oli lubatud; 4) rakendusaktide sisu ja ajakava oleksid varakult teada, vältimaks pikaajalist ebakindlust investeerimisotsustes. Ilma nende eeldusteta võivad tarneahelapiirangud kaasa tuua ebaproportsionaalse halduskoormuse ja turuhäired, mis ei ole kooskõlas määruse eesmärgiga.	**Arvestatud** Vt seisukohti seletuskirja punktides 6.8.ja 6.14.
12.7	6. NIS2 muudatused Toetame NIS2 muudatusi, mis: 1) täpsustavad subjektide ringi ja vähendavad ebaselgust kohuslaste määratlemisel; 2) tõstavad subjektsuse lävendeid, vähendades ebaproportsionaalset koormust; 3) keelavad täiendavate siseriiklike küberturvanõuete kehtestamise, kui ELi tasandil on riskijuhtimismeetmed juba kehtestatud. Peame eriti oluliseks lahendada NIS2 ja DORA paralleelsed kohustused IKT teenuse osutajatele, et vältida topeltregulatsiooni ja vastuolulisi nõudeid.	**Selgitame** **1 ja 2** - võetud teadmiseks, sh vt seisukoha punkti 6.1; **3 –** vt seisukoha punkti 6.13. **DORA määruse osas – s**iinsete eelnõude puhul sama Eesti seisukohta ei koostata, kuna see on juba koostatud[8] digiomnibussi eelnõude raames, mida on siinses protsessi võimalik taaskasutada.

[8] https://eelnoud.valitsus.ee/main/mount/docList/a4bbca3f-8cca-4bcb-af5b-6d6e15dbb143

12.8	Kokkuvõttes Eesti Tööandjate Keskliit toetab küberturvalisuse tugevdamist Euroopa Liidus, kuid rõhutab, et selle eelduseks on lihtsam, sidusam ja sisuliselt riskipõhine regulatiivne raamistik. Küberturvalisus paraneb eelkõige läbi toimiva riskijuhtimise ja tehnoloogia, mitte halduskoormuse kasvatamise.	**Võetud teadmiseks**

Kaitseväe arvamus oli tunnistatud avaliku teabe seaduse § 35 lõike 2 punkti 1 alusel juurdepääsupiiranguga teabeks, mistõttu seda ei esitata siinses seletuskirjas.