Küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu seletuskiri

Sisukord

1. Sissejuhatus

1.1. Sisukokkuvõte

Tehnoloogia kiire areng, võrgu- ja infosüsteemide kasvav keerukus ning internetti ühendatud seadmete suurenev arv muudavad küberturvalisuse üha olulisemaks valdkonnaks. Nii COVID-19 kriisi ajal kui ka sellele järgnenud aastate geopoliitiliste sündmuste ning kriiside tõttu on Euroopa Liidus, sealhulgas Eestis, kasvanud nii küberrünnakute arv kui ka nende keerukus.

Olukorda arvestades on vaja saavutada ühtlaselt kõrgem küberturvalisuse tase Eestis, et tagada ning järk-järgult suurendada küberturvalisuse kõrget taset ka kogu Euroopa Liidus. Seetõttu võetakse eelnõukohase seadusega üle Euroopa Parlamendi ja nõukogu 14. detsembri 2022. a direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (edaspidi *NIS2-direktiiv*)[1]. NIS2-direktiiviga lahendatakse endise küberturvalisuse valdkonna direktiivi (Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148; edaspidi *direktiiv (EL) 2016/1148*) rakendamise kitsaskohti ning ühtlustatakse reegleid, kuidas hallata digitaalsete lahenduste järjest enama kasutuselevõtuga kaasnevaid küberohte. NIS2-direktiivi eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase kogu Euroopa Liidus, et parandada siseturu toimimist.

NIS2-direktiiv võetakse üle ennekõike küberturvalisuse seadusega, kuid muudatusi tehakse ka muudes seadustes: e-identimise ja e-tehingute usaldusteenuse seadus, Eesti Rahvusringhäälingu seadus, elektroonilise side seadus, hädaolukorra seadus, käibemaksuseadus, lennundusseadus, raudteeseadus, sadamaseadus ning tervishoiuteenuste korraldamise seadus. Neis tehtavad muudatused on paljuski tehnilised. Muudatusi tegemata ei ole võimalik NIS2-direktiivi üle võtta ega rakendada.

NIS2-direktiivi ülevõtmiseks ei ole vaja Eesti õigust palju muuta, kuna kehtiv küberturvalisuse seadus ja ka selle alusel kehtestatud määrused reguleerivadki suuremas osas NIS2-direktiivi küberturvalisuse nõudeid. Sellegipoolest on teemasid ja valdkondi, mis ei ole Eestis reguleeritud, ning just nendele seaduseelnõu keskendubki. NIS2-direktiiv võetakse üle minimaalsel võimalikul määral, arvestades riigi eripäraga. Seetõttu ei ole eelnõus muid uusi nõudeid, mis tekitaksid küberturvalisuse seaduse subjektidele uusi kohustusi.

Eelnõukohase seadusega tehtav peamine muudatus on küberturvalisuse seaduse kohaldamisalasse kuuluvate isikute (ennekõike juriidiliste isikute, kuid ei ole välistatud ka füüsilisest isikust

[1] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.EST&toc=OJ%3AL%3A2022%3A333%3ATOC

ettevõtjate) loetelu täiendamine. Küberturvalisuse seaduse nõudeid peavad järgima praegu umbes 3500 subjekti ning eelnõuga lisandub neile (esialgsel hinnangul) veel umbes 3000 (+/–10%) subjekti (üksust). Seaduse kohaldamisala täiendatakse ainult NIS2-direktiiviga ette nähtud subjektidega, et suurendada ühiskonna toimimise seisukohast vajalike organisatsioonide küberturvalisuse taset.

Mainitud loetellu lisatud uued subjektid peavad samuti hakkama tegelema küberturvalisuse tagamisega ehk rakendama turvameetmeid ning olulise mõjuga küberintsidendi korral teavitama sellest järelevalveasutust. Lisaks muutub turvameetmete rakendamise loogika – kui seniste nõuete kohaselt tuleb neid meetmeid üldjuhul erasektoris rakendada konkreetse teenuse (tegevuse) suhtes, siis NIS2-direktiiv näeb ette, et edaspidi tuleb neid meetmeid rakendada subjekti kogu organisatsiooni suhtes. Lisanduvatele subjektidele nähakse ette üleminekuaeg kolm aastat, mille jooksul tuleb viia oma tegevus küberturvalisuse seaduse turvameetmete kasutusele võtmise ja küberturvalisuse tagamise nõudega kooskõlla. Elutähtsa teenuse osutajate suhtes kohaldub erand – nemad lähtuvad kehtiva õiguse ehk hädaolukorra seaduse tõttu kuni viieaastasest tähtajast. Lisaks peavad subjektid teatama Riigi Infosüsteemi Ametile oma tegevuse andmed kolme kuu jooksul.

Uutele subjektidele kehtivate ja eelnõukohases seaduses sätestatud nõuete täitmisega tekkivaid kulusid on keeruline analüüsida. Majanduslik mõju igale subjektile on väga erinev ning seda ei ole praegu võimalik mõistlikult hinnata. Turvameetmete rakendamise rahaline kulu sõltub subjekti kasutatavate süsteemide hulgast ja keerukusest ning varem rakendatud turvameetmetest (subjekti vastutustundlikkusest oma IT-lahenduste kasutamisel või muudest nõuetest, näiteks isikuandmete töötlemiseks rakendatud tehnilistest ja korralduslikest meetmetest turvalisuse tagamiseks). Rakendamiseks vajaliku kulu majanduslik mõju subjektile sõltub omakorda selle kulu osakaalust subjekti eelarves, ennekõike IT-lahendustega seotud eelarves.

Eelnõukohase seadusega nähakse ette ka toetusmeede, millega oleks võimalik lisanduvaid või juba kehtivaid nõudeid täita. Toetusmeede on mõeldud nii KüTSi subjektidele kui ka muudele isikutele, kes soovivad küberturvalisuse seaduse nõudeid täita või oma küberturvalisust parandada. Lisaks loodavale toetusmeetmele on võimalik kasutada muid olemasolevaid toetusmeetmeid. Samuti on igaühel võimalik tutvuda suuniste, õpetuste ja juhenditega asjakohastel võrgulehtedel ning läbida tasuta kursusi (nt Digiriigi Akadeemia kaudu), mis aitavad igaühe küberturvalisust parandada. Lisaks on kavas luua uusi kursusi ja koolitusi.

Samuti luuakse küberturvalisuse seaduses õigusnormid, mis võimaldavad rakendada Euroopa Komisjoni 11. märtsi 2024. a delegeeritud määrust (EL) 2024/1366, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta (edaspidi *delegeeritud määrus (EL) 2024/1366*). Nende alusel määratakse Riigi Infosüsteemi Amet pädevaks asutuseks, mis vastutab talle delegeeritud määruses (EL) 2024/1366 sätestatud ülesannete täitmise eest. Kui Riigi Infosüsteemi Ametit pädevaks asutuseks ei määrataks, oleks see Eesti oludes automaatselt Konkurentsiamet, millel aga puudub küberturvalisuse valdkonnas kompetents delegeeritud määruses (EL) 2024/1366 sätestatud ülesannete täitmiseks. Arvestades Konkurentsiameti ja Riigi Infosüsteemi Ameti praegusi ülesandeid, ei oleks Konkurentsiametile pädeva asutuse ülesande andmine ka mõistlik. Eelnõus sätestatakse võimalus vajaduse korral edasi delegeerida delegeeritud määruse (EL) 2024/1366 artikli 39 lõikes 1, artikli 40 lõikes 4 ning artikli 41 lõigetes 1 ja 2 sätestatud ülesanded. Eelnõu koostamise ajal delegeerimise volitusnormi kasutamist ei arutatud, kuid selline võimalus on tulevikus.

Seaduseelnõuga kavandatavad muudatused on plaanis jõustada 2026. aasta 1. jaanuaril. See võimaldab ette valmistada ka eelnõuga seotud määruste kavandeid ja võtta need määrustena vastu.

1.2. Eelnõu ettevalmistajad

Eelnõu on koostanud Justiits- ja Digiministeeriumi riikliku küberturvalisuse talituse küberturvalisuse õigusnõunik Raavo Palu (raavo.palu@justdigi.ee) ja advokaadibüroo NOVE esindajad (Sten Tikerpe, Indrek Niklus, Kristiina Koll, Klen Teder) koostöös Riigi Infosüsteemi Ameti õigusosakonna õigusnõuniku Sander Pelisaare ning Küberturvalisuse Keskuse teenistujatega. Eelnõu ja seletuskirja on keeleliselt toimetanud Justiits- ja Digiministeeriumi õigusloome korralduse talituse toimetajad Merike Koppel (merike.koppel@justdigi.ee), Inge Mehide (inge.mehide@justdigi.ee) ja Aili Sandre (aili.sandre@justdigi.ee).

1.3. Märkused

Eelnõu on seotud muude menetluses olnud ja olevate eelnõudega.
NIS2-direktiiv avaldati ühises paketis teiste õigusaktidega:
1) Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1–79). Käsitleb muu hulgas liikmesriikide küberturvalisuse pädevate asutuste koostööd (edaspidi *DORA määrus*)[2];
2) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2556, millega muudetakse direktiive 2009/65/EÜ, 2009/138/EÜ, 2011/61/EL, 2013/36/EL, 2014/59/EL, 2014/65/EL, (EL) 2015/2366 ja (EL) 2016/2341 seoses finantssektori digitaalse tegevuskerksusega (seotud DORA määruse rakendamisega)[3];
3) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2557, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ (edaspidi *CER-direktiiv*)[4].
Nimetatud õigusaktid on mõneti seotud NIS2-direktiivi ja selle rakendamisega.

DORA määruse ja direktiivi arutelu Riigikogus oli seotud Finantsinspektsiooni seaduse ja teiste seaduste muutmise seadusega (eelnõu nr 422 SE). Sellega tagatakse finantssektori tegevust reguleeriva riigisisese õiguse kooskõla finantsasutustele kohalduvate Euroopa Liidu digitaalse tegevuskerksuse nõuetega. DORA määrusega luuakse erikord finantssektori mõningatele organisatsioonidele, mis NIS2-direktiivi põhiliste nõuete (riskijuhtimise meetmete rakendamise ning küberintsidentidest teavitamise nõue) asemel peavad järgima DORA määruse nõudeid. Eelnõuga nr 422 SE kavandatud muudatused avaldati Riigi Teatajas 11. oktoobril 2024 ning need jõustusid üldkorras (21.10.2024 jõustus kindlustustegevuse seaduse § 179 lg 1 p 2 muudatus). Ülejäänud muudatused jõustusid 17. jaanuaril 2025.

CER-direktiiv võeti üle hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seadusega (eelnõu nr 426 SE). Seos CER-direktiiviga tuleneb asjaolust, et asutus või isik, kes määratakse edaspidi elutähtsa teenuse osutajaks CER-direktiivi tähenduses, kuulub

[2] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0001.01.EST&toc=OJ%3AL%3A2022%3A333%3ATOC
[3] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0153.01.EST&toc=OJ%3AL%3A2022%3A333%3ATOC
[4] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0164.01.EST&toc=OJ%3AL%3A2022%3A333%3ATOC

automaatselt ka NIS2-direktiivi kohaldamisalasse. Sama põhimõte on kavas jätta kehtima ka tsiviilkriisi ja riigikaitse seaduse eelnõu kohaselt (eelnõude infosüsteemi toimik nr 21-0915, mis algatati Riigikogus 02.06.2025 tsiviilkriisi ja riigikaitse seaduse eelnõuna nr 668 SE[5]). Eelnõuga nr 426 SE kavandatud muudatused avaldati Riigi Teatajas 8. oktoobril 2024 ning need jõustusid 18. oktoobril 2024, sh mõned sätted (hädaolukorra seaduse täiendamine §-ga 91 ning § 53 täiendamine lõigetega 9–11) jõustusid üldises korras, kuid praktikas jõustusid need muude muudatustega samal kuupäeval.

Eelnõukohast seadust ei mõjuta (kuigi järgnevalt viidatud eelnõudes või väljatöötamiskavatsustes muudetakse ka neid seadusi, mida muudetakse eelnõukohase seadusega):
1. Riigikogus vastu võetud tervishoiuteenuste korraldamise seaduse, töötuskindlustuse seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse ning töövõimetoetuse seaduse muutmise seaduse eelnõu nr 604 SE;[6]
2. Riigikogus arutatav hädaolukorra seaduse ja teiste seaduste muutmise seaduse eelnõu nr 662 SEd;[7]
3. Riigikogus arutatav hädaolukorra seaduse ja teiste seaduste muutmise seaduse eelnõu nr 635 SEd;[8]
4. Regionaal- ja Põllumajandusministeeriumi ette valmistatud kohaliku omavalitsuse korralduse seaduse ja sellega seonduvate seaduste muutmise seadus (eelnõude infosüsteemi toimik 24-0006);[9]
5. Kliimaministeeriumi algatatud lennundusseaduse ja teiste seaduste muutmise seadus (eelnõude infosüsteemi toimik 25-0229).[10]

Majandus- ja Kommunikatsiooniministeeriumil on ettevalmistamisel kosmoseseadus (eelnõude infosüsteemi toimik 24-0963)[11], millega soovitakse teha muudatus küberturvalisuse seaduse (edaspidi *KüTS*) kehtiva versiooni § 3 lõikes 1, sh tekitada ristviited KüTSile, mida eelnõukohase seadusega soovitakse kaotada.

Sotsiaalministeeriumil on ettevalmistamisel inimgeeniuuringute seadus (eelnõude infosüsteemi toimik 25-0756),[12] milles tehakse ristviiteid KüTSile ning muudatusi ka kehtiva KüTSi sätetesse, mida samuti eelnõukohase seadusega muudetakse. Selle eelnõu eeldatav jõustumisaeg on 1. jaanuar 2026, kuid tuleb enne viia kõnesoleva eelnõuga vastavusse.

Riigikogus on arutlusel tsiviilkriisi ja riigikaitse seadus (eelnõu nr 668 SE),[13] mis teeb muu hulgas muudatusi eelnõukohase seadusega muudetavates seadustes ning tunnistab hädaolukorra seaduse kehtetuks. Selle eelnõu eeldatav jõustumisaeg on 1. juuli 2026 ehk pärast eelnõukohase seaduse jõustumist. Kuigi selle eelnõu § 75 lõike 4 punkt 3 ning lõige 5 arvestavad eelnõukohase seadusega

[5] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/679eeee7-62b9-4817-a660-745e6642a8d9/tsiviilkriisi-ja-riigikaitse-seadus/
[6] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1b263415-8c5b-47bc-b7f8-2699c47b186f/tervishoiuteenuste-korraldamise-seaduse-tootuskindlustuse-seaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seaduse-ning-toovoimetoetuse-seaduse-muutmise-seadus/
[7] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6ee13b43-f1c7-44ab-a3ee-abb51efa8134/hadaolukorra-seaduse-ja-teiste-seaduste-muutmise-seadus/
[8] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/854df69b-4a04-4ac2-bd27-5431ebcf44f8/hadaolukorra-seaduse-ja-teiste-seaduste-muutmise-seadus/
[9] https://eelnoud.valitsus.ee/main/mount/docList/345b8b87-0431-4aaa-ad59-6f0e7112fd8b
[10] https://eelnoud.valitsus.ee/main/mount/docList/d5d7ce18-2e1c-4a8d-85e2-ebf9bb75bf35
[11] https://eelnoud.valitsus.ee/main/mount/docList/c3ba07e8-ccf2-4159-ab17-dd7ecb1d9577
[12] https://eelnoud.valitsus.ee/main/mount/docList/7e9ad302-c1c7-4b83-99de-b439bf89bb6f
[13] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/679eeee7-62b9-4817-a660-745e6642a8d9/

tehtavaid muudatusi, tuleb selles teha järgmised muudatused:
- eelnõu § 213 (krediidiasutuste seaduse muutmine) punkti 6 sõnastus tuleks üle vaadata eelnõukohase KüTSi § 1 lõike 4 sõnastuse ning selle selgituste tõttu;
- eelnõu § 217 (KüTSi muutmine) punkti 1 tuleb muuta (sätestades, et eelnõukohase KüTSi viited hädaolukorra seadusele (vt eelnõu KüTSi § 3 lg 2 p-e 2 ja 7) tuleb muuta viideteks tsiviilkriisi ja riigikaitse seadusele) ning punkt 2 tuleb välja jätta eelnõukohase KüTSi § 3 lõike 2 punkti 7 tõttu. Samuti tuleb muuta eelnõukohase KüTSi § 4^1 lõike 4 esimest lauset ja § 28^1 lõike 4 esimest lauset (mõlema puhul asendada tekstiosa „hädaolukorra seaduse § 38 lõike 1^3 punktis 3“ tekstiosaga „tsiviilkriisi ja riigikaitse seaduse § 75 lõike 4 punktis 3“) ning eelnõukohase KüTSi § 17^4 lõike 4 esimest lauset (asendada tekstiosa „hädaolukorra seaduse § 37 lõike 5 alusel määratud asutuse“ tekstiosaga „tsiviilkriisi ja riigikaitse seaduse § 74 lõike 4 alusel määratud asutuse või ametiasutuse“).

Eelnõukohane seadus on seotud Euroopa Liidu õiguse rakendamisega: võetakse üle NIS2-direktiiv ning luuakse õigusnormid Euroopa Komisjoni delegeeritud määruse (EL) 2024/1366 rakendamiseks.

Eelnõukohane seadus on seotud 2025–2027 koalitsioonileppe riigikaitse ja julgeoleku valdkonna eesmärgiga „tagame Eesti digiühiskonna toimepidevuse nii, et teenused on küberturvaliselt kättesaadavad igas olukorras“ ning tõhusa asjaajamise valdkonna eesmärgiga „võtame Euroopa Liidu õiguse üle Eestile sobivaimal moel ja teeme Euroopas ettepanekud sobimatute normide muutmiseks, sealhulgas ettepanek lükata edasi kestlikkusaruandluse esitamine ja muuta need vabatahtlikuks“.[14] Eelnõu väljatöötamise alus on Vabariigi Valitsuse tegevusprogrammi 2023–2027 ELi direktiivide valdkonna all olev ülesanne „Eelnõu direktiivi (EL) 2022/2555 ülevõtmiseks (küberturvalisuse 2. direktiiv)“.

Eelnõukohase seadusega muudetakse järgmisi seadusi:
1) küberturvalisuse seadus (RT I, 21.06.2024, 15);
2) e-identimise ja e-tehingute usaldusteenuste seadus (RT I, 03.03.2023, 3);
3) Eesti Rahvusringhäälingu seadus (RT I, 08.10.2024, 2);
4) elektroonilise side seadus (RT I, 02.01.2025, 23);
5) hädaolukorra seadus (RT I, 22.05.2025, 4);
6) käibemaksuseadus (RT I, 02.01.2025, 13);
7) lennundusseadus (RT I, 04.12.2024, 12);
8) raudteeseadus (RT I, 08.10.2024, 16);
9) sadamaseadus (RT I, 17.04.2025, 37);
10) tervishoiuteenuste korraldamise seadus (RT I, 02.01.2025, 78).

Eelnõu seadusena vastuvõtmiseks on vajalik Riigikogu poolthäälte enamus. Käibemaksuseaduses tehtav muudatus on normitehniline (vt täpsemaid selgitusi allpool) ehk too muudatus ei ole seotud maksude kehtestamise ega muutmisega.

Vabariigi Valitsuse 22. detsembri 2011. a määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 1 lõike 2 punkt 2 ei nõua väljatöötamiskavatsust, kui eelnõu käsitleb Euroopa Liidu õiguse rakendamist ja kui eelnõu aluseks oleva Euroopa Liidu õigusakti eelnõu menetlemisel on

[14] https://valitsus.ee/valitsuse-eesmargid-ja-tegevused/valitsemise-alused/koalitsioonilepe-2025-2027

sisu poolest lähtutud sama paragrahvi lõikes 1 sätestatud nõuetest. Avalik konsultatsioon peeti[15] ning Eesti on avaldanud oma seisukohad (eelnõude infosüsteemi toimik 20-3668)[16] NIS2-direktiivi algatuse kohta. Eesti seisukohtade seletuskirjas (lk 1) leiti, et NIS2-direktiivi algatuse muudatustega Eestile kaasnevat mõju saab hinnata keskmiseks. Eelkõige kaasneb mõju kohaldamisala laienemise, nõuete karmistamise ning halduskoormuse suurenemise tõttu nii riigiasutustele kui ka ettevõtjatele. Seisukohtade seletuskirjas (lk 10) leiti, et ministeeriumid ja riigiametid peavad hakkama järgima NIS2-direktiivist tulenevaid kohustusi; samuti ka, et kuigi „Eesti riigiasutuste küberturvalisus ületab praegugi EL-i poolt sätestatud miinimumstandardit, siis hiljutised küberrünnakud riigiasutuste suunal näitavad, et täielikku kindlust küberrünnete vastu ei ole võimalik saavutada, kuid parem ülevaade infosüsteemidest aitab probleeme ära hoida. Üldiselt võib eeldada, et [NIS2-direktiivi] laienemine avalikule sektorile toob suurema kasuteguri kaasa nendele LRdele, kus konkreetseid meetmeid riigiasutuste küberturbele ette nähtud ei ole.“ Seisukohtade seletuskirjas (lk 11) leiti ka, et NIS2-direktiiv suurendab pädeva asutuse, st Riigi Infosüsteemi Ameti töökoormust koos pikemas perspektiivis vajadusega laiendada ameti koosseisu. Seisukohtade seletuskirjas (lk 12 ja 13) leiti, et teabevahetuse „suurenemine, tehnilise, operatiivse ja strateegilise koostöö tugevnemine ning poliitikate ühtlustamine aitavad LRdel paremini intsidentidega toime tulla. Kuna küberintsidentide ja -rünnakute arv on aegamööda suurenenud ning ettevõtete teadlikkus küberturvalisuse olulisest paranenud, võib eeldada, et küberturvalisusesse investeerivate ettevõtete arv on kasvamas ka ilma täiendava EL-i tasandi regulatsioonita. […] Üksustele tuleksid [NIS2-direktiivi] turvanõuete kohustustega olulised lisakulutused ning kulud kasvavad ka seoses intsidentidest teavitamise korra konkreetsemaks muutmisega (mis tõenäoliselt tõstab teavituste arvu). Samuti muutub [NIS2-direktiivi] põhjal trahvide ja karistuste kord, mis võivad nõudeid mitte täitvatele üksustele kaasa tuua mastaapsed trahvid. […] Peamine kulu ettevõtetele seondus turvanõrkuste hindamise ja analüüsimisega. Komisjon eeldab, et [NIS2-direktiiviga] kaasatud uutele sektoritele tõusevad IKT-alased kulutused 25%, samas kui juba direktiiviga kaetud sektoritele suurenevad IKT-kulutused ligikaudu 15%. […] [Riigi Infosüsteemi Ameti] hinnangul peaksid [NIS2-direktiivi] subjektid enda küberturbe direktiiviga kooskõlla viimiseks tegema mitmeid ühekordseid investeeringuid, millele lisanduksid püsikulud. Eesti puhul erinevad investeeringute ning püsikulude mahud sektoriti ning ettevõtte suurust arvestades. Väiksemad üksused, kes ostavad infoturbe ning IT-teenust sisse, teevad rohkem ühekordseid kulutusi, samas kui suured ettevõtted hoiavad palgal mitmeid (või vähemalt ühte) küberturbega seotud inimesi. Sama trendi jätkumist võib eeldada [NIS2-direktiivi] puhul, kus väiksemad üksused tellivad riskianalüüsid kolmandatelt osapooltelt“.

Tuleb arvestada, et pärast nende seisukohtade koostamist tehti KüTSi ja selle alusel antud määrustesse täiendusi 2022. aastal, mis muu hulgas tegi turvameetmete nõuded samaväärseks NIS2-direktiivi nõuetega.

Kuna eelnõukohane seadus suurendab halduskoormust (KüTSi täiendatakse uute subjektidega, kes omakorda peavad KüTSi nõudeid täitma), siis halduskoormuse tasakaalustamine on kavas ette näha eelnõuga (eelnõude infosüsteemi toimik 25-0715),[17] millega muudetakse Vabariigi Valitsuse 9. detsembri 2022. a määrust nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ (RT I, 19.06.2024, 12). Nimetatud määruse muutmise eelnõu on seotud nii eelnõukohase seaduse kui ka

[15] https://eur-lex.europa.eu/legal-content/ET/HIS/?uri=uriserv:OJ.L_.2022.333.01.0080.01.EST; konkreetsemalt Euroopa Komisjoni ettepaneku rubriik, dokumendid nr 52020PC0823, 52020SC0345 ja 52020SC0344. Vt ka https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=celex:52020PC0823 ja https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Kuberturvalisus-vorgu-ja-infosusteemide-turvalisust-kasitlevate-ELi-oigusnormide-labivaatamine_et.

[16] https://eelnoud.valitsus.ee/main/mount/docList/5c847e1d-42e5-46f8-99d8-d21d144bca61

[17] https://eelnoud.valitsus.ee/main/mount/docList/7d3ea848-35b2-47d8-8eb8-fa2f735c3da6

selle lisades olevate määruste muutmisega, kuna on seotud samuti NIS2-direktiivi ülevõtmisega.

2. Seaduse eesmärk

Seadusega võetakse Eesti õigusesse üle NIS2-direktiiv ning sätestatakse delegeeritud määruse (EL) 2024/1366 artikli 4 lõike 1 alusel volitusnorm pädeva asutuse määramiseks. Pädevaks asutuseks saab Riigi Infosüsteemi Amet. Eelnõukohase seadusega on kavas sätestada ka Vabariigi Valitsusele võimalus vajaduse korral edasi delegeerida komisjoni delegeeritud määruse (EL) 2024/1366 artikli 39 lõikes 1, artikli 40 lõikes 4 ning artikli 41 lõigetes 1 ja 2 sätestatud ülesanded. Esimene küberturvalisuse direktiiv ehk direktiiv (EL) 2016/1148 sillutas paljudes liikmesriikides teed mõtteviisi olulisele muutusele, pani aluse institutsioonilise ja regulatiivse lähenemisviisi kujunemisele küberturvalisuse valdkonnas ning see on andnud märkimisväärseid tulemusi. Direktiivi ülevõtmisel otsustati, et Eesti õigusruumis on vaja eraldi õigusaktiga ehk KüTSiga sätestada riigisisesed meetmed ühiskondliku ja majandustegevuse säilitamise seisukohast oluliste võrgu- ja infosüsteemide turvalisuse tagamiseks. Nende hulka kuuluvad ka võrgu- ja infosüsteemid, mis on vajalikud riigi ja kohaliku omavalitsuse üksuste töö toimimiseks. Toona sätestati KüTSis direktiivi (EL) 2016/1148 kohased kohustused ja Riigi Infosüsteemi Ameti kui pädeva asutuse õigused teha järelevalvet ning koordineerida küberintsidentide ennetamist, tuvastamist ja lahendamist. Selle direktiivi rakendamisega pidi tugevnema ja ühtlustuma küberturbealane koostöö liikmesriikide vahel. Eesti jaoks on oluline, et küberturbe valdkonnas jagataks vastastikku rohkem kogemusi, oskusi, tehnoloogiaid ja teavet riiklikus küberruumis toimuva kohta.

Samas on direktiivi (EL) 2016/1148 rakendamise võimalused osutunud piiratuks. Ühiskonna digiüleminek (mida võimendas COVID-19 kriis) on ohumaastikku laiendanud ning toonud kaasa uusi probleeme, mis nõuavad kohandatud ja uuenduslikke lahendusi. Küberrünnete arv kasvab endiselt, need on üha keerukamad ning pärinevad paljudest eri allikatest nii Euroopa Liidus kui ka mujal. Ühiskonna võrgu- ja infosüsteemidest suureneva sõltuvuse taustal areneb tehnoloogia kiiresti, võrgu- ja infosüsteemide suurenev keerukus ning internetti ühendatud väga erinevate seadmete kasvav arv ning küberruumis tegutsevate erineva motivatsiooni ja oskustasemega toimijate kasvav hulk muudab küberturvalisuse tagamise üha tähtsamaks ülesandeks. Tegutseb ju ka küberruumis selliseid isikuid, kes tunnevad Eesti digitaristu ja -teenuste vastu huvi seetõttu, et Eesti toetab Ukrainat. Muudatused ohukeskkonnas tingivad vajaduse tagada senisest parem olukorrateadlikkus ja tagada ohtude ennetamine, väljaselgitamine ja tõrjumine ka juhul, kui võrgu- ja infosüsteemi omanik või valdaja vajalikku hoolsust tahtlikult või teadmatusest ei ilmuta.

Direktiivi (EL) 2016/1148 toimivuse hindamisega tuvastati järgmised probleemid: Euroopa Liidus tegutsevate ettevõtjate kübervastupidavusvõime madal tase; vastupidavusvõime ebaühtlane tase liikmesriikide ja sektorite tasandil ning ühise olukorrateadlikkuse madal tase ja ühistegevuse puudulikkus kriisidele reageerimisel.[18] Seetõttu oli sama mõjuhinnangu kohaselt direktiivi (EL) 2016/1148 läbivaatamisel kolm üldeesmärki:

1. Suurendada Euroopa Liidus kõigis asjaomastes sektorites tegutsevate ettevõtjate (ulatusliku kogumi) kübervastupidavusvõimet, kehtestades eeskirjad, millega tagatakse, et kõik siseturul tegutsevad avaliku ja erasektori üksused, kes täidavad majanduse ja ühiskonna kui terviku jaoks olulisi ülesandeid, peavad võtma asjakohaseid küberturvalisuse meetmeid.

2. Vähendada vastupidavusvõime taseme ebaühtlust siseturul direktiiviga [(EL) 2016/1148] juba

[18] Euroopa Komisjoni talituste töödokument mõju hindamise aruande kommenteeritud kokkuvõte; lisatud dokumendile: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148. A osa: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020SC0344.

hõlmatud sektorites, ühtlustades täiendavalt 1) tegelikku kohaldamisala, 2) turvanõudeid ja intsidentidest teatamise nõudeid, 3) riiklikku järelevalvet ja täitmise tagamist reguleerivaid sätteid ning 4) liikmesriikide pädevate asutuste suutlikkust.
3. Tõsta ühise olukorrateadlikkuse taset ning suurendada ühist valmisolekut ja reageerimissuutlikkust, võttes meetmeid usalduse suurendamiseks pädevate asutuste vahel, jagades rohkem teavet ning kehtestades eeskirjad ja menetluskorra ulatuslike intsidentide või kriisi korral tegutsemiseks.
NIS2-direktiivi algatuse[19] 7. lisas (finantsselgitus – ametid) on punkti 1.5 (ettepaneku/algatuse põhjendused) alapunktides 1.5.1–1.5.3 selgitatud NIS2-direktiivi koostamise vajadust nii:
1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused, sealhulgas algatuse rakendamise täpne ajakava
Muutmisettepaneku eesmärk on suurendada Euroopa Liidus kõigis asjaomastes sektorites tegutsevate ettevõtjate kübervastupidavusvõimet, vähendada siseturul vastupanuvõime taseme ebaühtlust [direktiivi (EL) 2016/1148] kohaldamisalasse juba hõlmatud sektorites ning suurendada ühist olukorrateadlikkust, ühist valmisolekut ja ühist reageerimissuutlikkust. See tugineb sellele, mis on viimase nelja aasta jooksul direktiivi (EL) 2016/1148 kohaldamisel juba saavutatud.
1.5.2. ELi meetme lisaväärtus (see võib tuleneda eri teguritest, nagu kooskõlastamisest saadav kasu, õiguskindlus, suurem tõhusus või vastastikune täiendavus). Käesoleva punkti kohaldamisel tähendab „ELi meetme lisaväärtus" väärtust, mis tuleneb liidu sekkumisest ja lisandub väärtusele, mille liikmesriigid oleksid üksi tegutsedes loonud.
Kübervastupidavusvõime ei saa olla kogu liidus ühtlaselt tõhus, kui seda käsitletakse eri lähenemisviise rakendades ja riiklikult või piirkondlikult kapseldudes. Küberturvalisuse direktiiviga [(EL) 2016/1148] püüti seda puudust kõrvaldada, kehtestades võrgu- ja infosüsteemide turvalisuse raamistiku riiklikul ja liidu tasandil. Küberturvalisuse direktiivi [(EL) 2016/1148] esimese korrapärase läbivaatamise tulemusena juhiti siiski tähelepanu mitmetele olemuslikele puudustele, mille tõttu on liikmesriikide suutlikkus, kavandamine ja kaitse tase oluliselt erinev. See takistab ka ettevõtjatele võrdsete võimaluste tagamist siseturul.
ELi sekkumine suuremas ulatuses, kui küberturvalisuse direktiivi praegused meetmed ette näevad, on põhjendatav peamiselt järgmisega: i) probleemi piiriülene olemus; ii) ELi meetmete potentsiaal edendada ja hõlbustada tõhusat riiklikku poliitikat; iii) kooskõlastatud ja koostööl põhinevate küberturvalisuse alaste poliitikameetmete panus andmekaitse ja eraelu puutumatuse tõhusasse kaitsesse.
Seega on mainitud eesmärke parem saavutada ELi tasandi meetmetega kui et liikmesriikide üksinda tegutsemisega.
1.5.3. Samalaadsetest kogemustest saadud õppetunnid
Küberturvalisuse direktiiv [(EL) 2016/1148] on esimene horisontaalne siseturu õigusvahend, mille eesmärk on parandada liidu võrkude ja süsteemide vastupanuvõimet küberturvalisuse riskide suhtes. Alates selle jõustumisest 2016. aastal on see juba aidanud märkimisväärselt tõsta küberturvalisuse üldist taset liikmesriikides. Direktiivi toimimise ja kohaldamise läbivaatamise tulemusena on siiski osutatud mitmele puudusele, mida tuleb muudetud õigusaktiga käsitleda peale ajakohasemate meetmete vajaduse küsimuse, mis tuleneb üha suurenevast digiteerimisest.

Sellest johtuvalt võeti vastu NIS2-direktiiv, mille eesmärk on saavutada küberturvalisuse ühtlaselt kõrge tase kogu Euroopa Liidus, et parandada siseturu toimimist. Selle eesmärgi saavutamiseks on

[19] Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020PC0823.

NIS2-direktiivis sätestatud:
a) liikmesriikide kohustus võtta vastu riiklikud küberturvalisuse strateegiad ning määrata või asutada pädevad asutused, ulatuslike küberintsidentide ja kriisi ohjamise asutused, küberturbe ühtsed kontaktpunktid ja küberintsidentide käsitlemise üksused („CSIRTid“);
b) NIS2-direktiivi I või II lisas osutatud üksuste ning CER-direktiivi kohaldamisalasse kuuluvate üksuste küberturvalisuse riskijuhtimismeetmed ja teatamiskohustus;
c) küberturvalisuse teabe vahetamisega seotud reeglid ja kohustused;
d) järelevalve ja täitmise tagamisega seotud kohustused liikmesriikidele.
Seetõttu kannab eelnõukohane seadus sama eelkirjeldatud eesmärki ehk saavutada küberturvalisuse ühtlaselt kõrge tase, et sel viisil suurendada küberturvalisuse taset kogu Euroopa Liidus. Selleks lisanduvadki KüTSi kohaldamisalasse NIS2-direktiiviga ette nähtud üksused, et suurendada ühiskonna toimimise seisukohast üliloluliste üksuste ja oluliste üksuste ning domeeninimede registreerimise teenuse osutajate küberturvalisuse taset. Sel teel parandatakse ka Eesti ettevõtjate ja majanduse konkurentsivõimet.

Võrreldes direktiiviga (EL) 2016/1148 on NIS2-direktiiviga tehtud muudatused esmapilgul justkui uued ja nõuded täpsemad võrreldes varasematega. Allpool esitatakse NIS2-direktiivi nõuded, mis eelnõukohase seadusega üle võetakse ja millest KüTSi subjekt (üksus) peab lähtuma või mida arvestama:
a) artiklid 3 ja 27 – teavita ja vajaduse korral uuenda oma infot: *üksusel tuleb esitada pädevale asutusele (Riigi Infosüsteemi Amet) teatav info oma organisatsiooni kohta (nt nimi, kontaktandmed jne), sh hoida seda infot ajakohasena;*
b) artikkel 26 – esindaja määramine: *selles artiklis on nimetatud teatavad üksused (eelnõus digitaalse teenuse osutajad), kes peavad nimetama oma esindaja, kui nende tegevuskoht ei ole Euroopa Liidus või nad ei ole seal asutatud, kuid pakuvad Euroopa Liidus oma teenuseid;*
c) artikkel 20 – juhtorgani ehk KüTSi kontekstis juhatuse liikmete kohustused: *juhatuse liikmed (juhatuse puudumisel juhatuse liikmetega sarnasel positsioonil olevad isikud) kiidavad heaks küberturvalisuse riskijuhtimismeetmed, jälgivad nende rakendamist ning neid võidakse võtta vastutusele teatavate nõuete rikkumise eest (eelnõu järgi ühinguõiguses sätestatud vastutuse, mitte väärteo korras);*
d) artikkel 20 – juhtorgani ehk KüTSi kontekstis juhatuse liikmete koolitused: *juhtorganite liikmed ehk KüTSi kontekstis juhatuse liikmed (juhatuse puudumisel juhatuse liikmetega sarnasel positsioonil olevad isikud) on kohustatud läbima korrapäraselt koolitusi*);
e) artikkel 21 – üksus võtab kasutusele riskijuhtimismeetmed: *tegemist on üksuse küberturvalisuse kaitse ja sellega seotud meetmete kasutusele võtmisega ehk KüTSi kontekstis turvameetmete rakendamisega;*
f) artikkel 23 – küberintsidentidest teavitamine: *üksused teavitavad järelevalveasutust (üldreeglina Riigi Infosüsteemi Ametit) ning asjakohasel juhul ka oma teenuse kasutajaid kõikidest olulise mõjuga küberintsidentidest;*
g) artikkel 24 – Euroopa küberturvalisuse sertifitseerimise kavade kasutamine: *liikmesriik ehk Eesti võib nõuda üksuselt riskijuhtimismeetmetega seotud nõuetele vastavuse tõendamiseks teatavate IKT-toodete, IKT-teenuste ja IKT-protsesside kasutamist; eelnõuga seda volitust ei sätestata, kuid sarnane volitus nende kohustuslikus korras kasutamiseks on ka Euroopa Komisjonil, kes saab seda teha delegeeritud õigusaktide alusel. Kui komisjon taolise delegeeritud õigusakti kehtestab, siis nõude järgimine tuleb delegeeritud õigusaktist, mitte KüTSist;*
h) artikkel 28 – domeeninimede registreerimisandmete andmebaas: *artikkel sätestab, kuidas toimetavad tippdomeeninimede registrid ja tippdomeenide domeeninimede registreerimise teenuste osutajad, sh mis infot nad ise koguvad;*

i) artikkel 29 – küberturvalisusalase teabe vahetamise kokkulepped: *üksused ja muud asjaosalised võivad vabatahtlikult vahetada asjakohast küberturvalisuse alast teavet, sõlmides selleks asjakohased kokkulepped; kui NIS2-direktiivi subjekt osaleb sellises kokkuleppes, siis tuleb selles osalemisest ja sellest väljumisest teavitada Riigi Infosüsteemi Ametit;*
j) artiklid 31–33, mis sätestavad järelevalve tegija õigused ja kasutatavad meetmed;
k) artikkel 34 – haldustrahvid: *see artikkel sätestab haldustrahvide määramise üldtingimused, kui rikutakse artikli 21 või 23 nõudeid; haldustrahvide piirsuurused sõltuvad sellest, kas tegemist on elutähtsa üksuse (eelnõus üliolulise üksuse) või olulise üksusega; eelnõukohases seaduses võetakse haldustrahvide sätted üle väärteomenetluse sätetena;*
l) artikkel 34 – sunniraha: *samas artiklis on ka säte, et liikmesriigid võivad ette näha õiguse määrata sunniraha, mille eesmärk on sundida üksust direktiivi rikkumist lõpetama; NIS2-direktiiv sunniraha suurust ega selle kindlakstegemise nõudeid ette ei näe.*

Eesti on KüTSi täiendanud ka 2022. aastal.[20] Toona tehtud muudatustel oli lõpptulemusena neli eesmärki, millest seletuskirjas nimetatakse üks peamistest – ajakohastada KüTSi, et oleks võimalik kehtestada Eesti infoturbestandard ja muud ajakohastatud võrgu- ja infosüsteemide küberturvalisuse nõuded, et suurendada süsteemide küberturvalisust, kuid ka teenuseosutajate vastupanuvõimet süsteeme ähvardavatele ohtudele. Muudatusega sooviti saavutada olukord, mis võimaldaks ühtsetel põhimõtetel paindlikult ja rakendajatele arusaadavalt rakendada tänapäevastele vajadustele vastavat turvameetmete süsteemi avalike ülesannete täitmiseks või oluliste teenuste osutamiseks loodud äriprotsessides. Toona leiti, et infoturbe rakendamata jätmine ei ole tolle aja küberturbe olukorras KüTSi subjektide võrgu- ja infosüsteemide puhul aktsepteeritav. Eesti infoturbestandardi loomisega sooviti olukorda muuta, tõstes andmeid töötleva võrgu- ja infosüsteemi asemel turvameetmete rakendamise fookusesse olulist, sh avalikku ülesannet täitva organisatsiooni, mille eesmärk on pakkuda avalikke teenuseid ja tugiteenuseid. Eesti infoturbestandard koostati, arvestades rahvusvahelisi standardeid ning teiste riikide standardseid nõudeid – tegemist on nõuete kogumiga, mis on kooskõlas Saksa päritolu IT-Grundschutzi ja rahvusvahelise standardiga ISO/IEC 27001.[21] Viimati nimetatud standard võeti eeskujuks ka NIS2-direktiivi artikli 21 riskijuhtimismeetmetega seotud nõuete sõnastamisel.

Kui arvestada ka asjaoluga, et direktiiv (EL) 2016/1148 võeti üle laiemalt, kui selle miinimumnõuded ette nägid, lihtsustab 2022. aastal Eesti infoturbestandardi ja selle järgimise kohustuse kehtestamine NIS2-direktiivi ülevõtmist Eesti õigusesse, kuna NIS2-direktiivi peamised nõuded on kehtivas õiguses juba sätestatud. Pigem täpsustatakse olemasolevas õiguses olevaid sätteid ning kehtestatakse mõned uued normid. Konkreetsemalt tehakse eelnõukohase seadusega järgmised peamised muudatused:

- täiendatakse KüTSi subjektide nimekirja (*säilitatakse kehtiva KüTSi subjektid ning lisanduvad ennekõike need üksused, mille näeb ette NIS2-direktiiv*;
- sätestatakse, milliseid andmeid peab KüTSi subjekt pädevale asutusele enda kohta esitama (*nt nimi, registrikood, kontaktandmed jne*);
- sätestatakse KüTSi tasandil nõuded turvameetmete (riskijuhtimismeetmete) rakendamiseks (*eelnõuga sätestatakse KüTSis üldpõhimõtted, mida teenuseosutaja peab arvestama turvameetmete rakendamisel; konkreetsed NIS2-direktiivi artiklis 21 ette nähtud turvameetmed kehtestatakse KüTSi § 7 lõike 5 alusel kehtestatava määruse muudatustega;*

[20] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus/
[21] Eesti infoturbestandardi rakendusjuhend, peatükid 1 ja 3, sh vt viimases olevat joonist nr 3 – kättesaadav: https://eits.ria.ee/et/abimaterjalid/rakendusjuhend.

nende turvameetmete kui nõuete põhisisu on näiteks täidetud Eesti infoturbestandardi nõuete täitmisega või selle alternatiivi ehk rahvusvahelise standardi ISO/IEC 27001 nõuete täitmisega);
- täpsustatakse küberintsidendist teatamise nõudeid (*täpsustatakse seaduse tasandil esitatavate teadete intervalli, sisu ja intsidendi lahendamisega seotud korraldust*);
- kaotatakse direktiivil (EL) 2016/1148 põhinev üksuste liigitus (olulise teenuse operaator ja digitaalse teenuse osutaja (*viimast terminit kasutatakse küll ka eelnõus, kuid seda uues, NIS2-direktiivile vastavas tähenduses*) ning luuakse uute kategooriatena ühiskonna toimimise seisukohast üliolulised üksused ja olulised üksused (*nende erinevus on järelevalve tegemises ja võimalike trahvide ülemmääras*);
- sätestatakse selgelt, kellega tuleb ja võib teavet vahetada või koostööd teha (*koostöö tegemine pädevate asutuste vahel, üle riigipiiride ja vabatahtlikus vormis; näiteks piiriülese küberintsidendi või küberkriisi korral*);
- määratakse pädevad asutused, kellele on sätestatud ülesanded NIS2-direktiivi või delegeeritud määruse (EL) 2024/1366 kohaselt (*üldiselt on tegemist valitsusasutustega, kes juba praegu tegelevad samade ülesannetega*);
- määratakse selgemalt KüTSi subjekti juhatuse liikmete roll ja ülesanded (*põhilisemad nõuded on juba kehtestatud, kuid nüüd sätestatakse need seaduse tasandil; samuti kehtestatakse juhatuse liikmetele kohustus osaleda küberturvalisuse koolitustel*);
- täpsustatakse järelevalve- ja täitemeetmeid, mida KüTSi subjekti suhtes on võimalik kasutada (*järelevalveasutusel on juba praegu peaaegu samad volitused, kuid mõned volitused lisanduvad NIS2-direktiivi järgi*);
- ühtlustatakse trahvide suurused (*eeskuju võetud isikuandmete kaitse valdkonna trahvidest*);
- sätestatakse võimalus osaleda riikidevahelises küberturvalisuse taseme hindamises (*tegemist on vabatahtliku ülesandega*).

Suurimad muudatused on KüTSi subjektide nimekirja täiendamine ja üleminek võrgu- ja infosüsteemide pidamisele suunatud nõuetelt üksustele ehk seaduse kohaldamisalasse kuuluvatele isikutele ja asutustele tervikuna suunatud nõuetele, mis toob kaasa seniste nõuete laienemise ka olemasolevatele subjektidele (ennekõike erasektoris). Avalikule kooskõlastusele saadetud eelnõu seletuskirjas oli iga subjekti kategooria juures ka Riigi Infosüsteemi Ameti esialgne hinnang, kui palju üksusi selliste subjektide määratlusele vastab, sh kui paljud neist kuuluvad KüTSi kohaldamisalasse. Eelnõu kohta saadetud tagasiside tõttu on eelnõu koostajad korrigeerinud lisanduvate üksuste arvu suuremaks, kuid edaspidi ei ole konkreetse subjekti kategooria juurde lisatud hinnangut, kui palju üksusi määratlusele vastab ning kui paljud neist kuuluvad ka KüTSi kohaldamisalasse. Üldistatult saab kokku võtta, et olemasolevaid subjekte on umbes 3500 ning uusi subjekte lisandub umbes 3000 (+/- 10%) ehk kokku on umbes 6500 subjekti, kellele KüTSi nõuded hakkavad kohalduma. Nende arvude puhul tuleb arvestada ka asjaoluga, et teatud hulk subjekte vastab samal ajal mitmele tunnusele. Näiteks on ühe üksuse puhul tegemist nii keskvalitsuse avaliku halduse üksusega kui ka avaliku teabe seaduse tähenduses andmekogu vastutava töötlejaga või volitatud töötlejaga; või on näiteks tegemist elutähtsa teenuse osutajaga ning samal ajal ka üldkasutatava elektroonilise side võrgu teenuse osutajaga; või on tegemist vee-ettevõtjaga, kes samal ajal tegutseb ka reovee valdkonnas. Eelnõu kohaldamisalast on välja jäetud mikro- ja väikeettevõtjad Euroopa Komisjoni 6. mai 2003. aasta soovituse 2003/361/EÜ (mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta, ELT L 124. 20.05.2003, lk 36) tähenduses, välja arvatud elektroonilise side võrgu teenuse osutajad või üldkasutatava elektroonilise side teenuse osutajad, usaldusteenuse osutajad, tippdomeenide domeeninimede registrid, domeeninimede süsteemi teenuse osutajad, domeeninimede registreerimise teenuse

osutajad, elutähtsa teenuse osutajad ja avaliku halduse üksused ning mõned muud üksused, näiteks mõne teenuse ainupakkujad liikmesriigis. Nimetatud üksused on KüTSi kohaldamisalas, kuna see on ette nähtud NIS2-direktiiviga. Seetõttu lisanduvate üksuste lõplik arv selgub siis, kui üksused on täitnud teavitamiskohustuse ning selle käigus esitatud andmete põhjal on Riigi Infosüsteemi Amet koostanud üksuste nimekirja.

Eelnõu sõnastamisel lähtuti NIS2-direktiiviga ette antud liikmesriigi kaalutlusõigusest mingi õigusnorm sõnastada ning kehtestada. Seetõttu on eelnõus ennekõike piirdutud ainult sellega, mida NIS2-direktiiv kitsamas tähenduses ette on näinud, ehk n-ö üldnõuetega. Nagu eespool mainitud, on osa eelnõu muudatustest kas täpsustused (seal, kus on juba vajalikud nõuded Eesti õiguses olemas, et viia need NIS2-direktiiviga kooskõlla) või NIS2-direktiivi miinimumnõuete ülevõtmine (osas, kus on seadus vaja ühtlustada Euroopa Liidu õigusega). NIS2-direktiiv võetakse üle minimaalsel võimalikul määral, arvestades riigi eripära. Seetõttu ei ole eelnõus endas muid uusi nõudeid, mis tekitaksid teenuseosutajatele uusi kohustusi.

NIS2-direktiivi ülevõtmise tähtaega arvestades ei ole seaduseelnõuga võimalik teha kogu küberturvalisuse valdkonna normide laiapõhjalist revisjoni, mistõttu käsitleb eelnõu üksnes NIS2-direktiivi ülevõtmise ja delegeeritud määrusega (EL) 2024/1366 seotut. Revisjoni tegemiseks tullakse välja eraldi väljatöötamiskavatsusega.

Ülevaade NIS2-direktiivi sätetest

- I peatükk: üldsätted (artiklid 1–6) – reguleerimisese; kohaldamisala; üliolulised ja olulised üksused; valdkondlikud liidu õigusaktid; minimaalne ühtlustamine; mõisted.
- II peatükk: koordineeritud küberturvalisuse raamistikud (artiklid 7–13) – riiklik küberturvalisuse strateegia; pädevad asutused ja ühtsed kontaktpunktid; riiklikud küberkriiside ohjamise raamistikud; küberintsidentide käsitlemise üksused (CSIRTid); CSIRTidele esitatavad nõuded, nende tehniline võimekus ja ülesanded – turvahaavatavuse koordineeritud avalikustamine ja Euroopa turvahaavatavuste andmebaas; koostöö liikmesriigi tasandil.
- III peatükk: koostöö liidu ja rahvusvahelisel tasandil (artiklid 14–19) – koostöörühm; CSIRTide võrgustik; Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik (EU-CyCLONe); rahvusvaheline koostöö; aruanne küberturvalisuse olukorra kohta liidus; vastastikune hindamine.
- IV peatükk: küberturvalisusega seotud riskijuhtimismeetmed ja teatamiskohustus (artiklid 20–25) – juhtimine; küberturvalisuse riskijuhtimismeetmed; liidu tasandi kriitilise tähtsusega tarneahelate koordineeritud turberiski hindamine; [küberintsidendist] teatamiskohustus; Euroopa küberturvalisuse sertifitseerimise kavade kasutamine; standardimine.
- V peatükk: jurisdiktsioon ja registreerimine (artiklid 26–28) – jurisdiktsioon ja territoriaalsus; üksuste register; domeeninimede registreerimisandmete andmebaas.
- VI peatükk: teabevahetus (artiklid 29 ja 30) – küberturvalisuse alase teabevahetuse kokkulepped; vabatahtlik teavitamine asjakohasest teabest.
- VII peatükk: järelevalve ja täitmise tagamine (artiklid 31–37) – järelevalve ja täitmise tagamise üldised aspektid; järelevalve- ja täitemeetmed seoses üliolulistе üksustega; järelevalve- ja täitemeetmed seoses oluliste üksustega; üliolulistele ja olulistele üksustele haldustrahvide määramise üldtingimused; isikuandmete väärkasutamisega seotud rikkumised; karistused; vastastikune abi.
- VIII peatükk: delegeeritud õigusaktid ja rakendusaktid (artiklid 38 ja 39) – delegeeritud

volituste rakendamine; komiteemenetlus.
- IX peatükk: lõppsätted (artiklid 40–46) – läbivaatamine; ülevõtmine; määruse (EL) nr 910/2014 muutmine; direktiivi (EL) 2018/1972 muutmine; kehtetuks tunnistamine; jõustumine; adressaadid.
- Lisad: I lisa (kriitilise tähtsusega sektorid); II lisa (muud kriitilise tähtsusega sektorid); III lisa (vastavustabel).

NIS2-direktiivi ülevõtmisega seotud vastavustabel on esitatud seletuskirja lisas 1.

3. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb 11 paragrahvist. Eelnõu § 1 sisaldab küberturvalisuse seaduse muudatusi ning ülejäänud paragrahvid on seotud valdkondlike õigusaktide muutmisega, et võtta üle NIS2-direktiiv ning rakendada Euroopa Komisjoni delegeeritud määrust (EL) 2024/1366.

3.1. Eelnõu sisu analüüs

§ 1. Küberturvalisuse seaduse muudatused

Eelnõu §-s 1 nähakse ette küberturvalisuse seaduse (KüTS) muudatused:

KüTSi § 1 lõike 1 muudatusega viiakse seaduse reguleerimisala kooskõlla NIS2-direktiiviga. Kui kehtiv KüTS sätestab „ühiskonna toimimise seisukohast oluliste, sealhulgas avaliku sektori võrgu- ja infosüsteemide pidamise nõuded, vastutuse ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused“, siis NIS2-direktiivi ülevõtmise järel jääks selle reguleerimisala kehtivas sõnastuses kitsaks.

Tõenäoliselt kõige olulisema aspektina ei ole NIS2-direktiivi fookus erinevalt varasemast Euroopa Liidu tasandil ühtlustatud (ja ka KüTSis kajastatud) regulatiivsest lähenemisest seatud mitte üksnes ühiskonna toimimise seisukohast oluliste *võrgu ja infosüsteemide pidamise* nõuetele (ja sellele järgnevale), vaid selle kohaldamisalasse kuuluvad kõik NIS2-direktiivi järgi üliolulised või olulised üksuseks kvalifitseeruvad isikud, sh I ja II lisades loetletud üksused (isikud ja asutused) ning domeeninime registreerimise teenuse osutajad organisatsiooni kui tervikuna, mitte üksnes n-ö kriitilise teenusega seoses. Teisisõnu nõuab NIS2-direktiiv, erinevalt oma eelkäijast ehk NIS-direktiivist, et riskijuhtimismeetmeid rakendataks kõigi asjaomase üksuse tegevuste ja teenuste suhtes, mitte üksnes konkreetsete teenuste või infovarade suhtes.[22] Lisaks täiendatakse reguleerimisala nii, et seaduses oleks võimalik esitada reguleerimisala ulatuses normid, mis puudutavad i) küberintsidentide käsitlemise aluseid ja nõudeid turvahaavatavuse ja küberohtudega tegelemiseks; ii) ulatusliku küberintsidendi ja kriisi ennetamist ning lahendamist; iii) küberturvalisuse valdkonnas toimuva koostöö, teabevahetuse ja vastastikuse hindamise nõudeid; ja iv) küberturvalisuse valdkonna pädevate asutuste nimetamist või nende määramise nõudeid (see hõlmab lisaks eelnõu tulemusel määratud asutustele ka KüTSi kehtiva redaktsiooni §-des 5^1 ja 13^1 sätestatud asutusi).

KüTSi § 1 lõiget 2 täiendatakse punktiga 3, jättes seaduse kohaldamisalast välja Eesti Vabariigi diplomaatilised ja konsulaaresindused ning nende võrgu- ja infosüsteemid tingimusel, et:

a) mainitud võrgu- ja infosüsteemid asuvad esinduse ruumides; või

b) selliseid süsteeme käitatakse kolmanda riigi kasutajate jaoks.

Täiendus tehakse NIS2-direktiivi põhjenduse 8 viimase lause alusel, mille kohaselt *[k]äesolevat direktiivi ei kohaldata liikmesriikide diplomaatiliste ja konsulaaresinduste suhtes kolmandates riikides ega nende võrgu- ja infosüsteemide suhtes, kui sellised süsteemid asuvad esinduse*

[22] Vt selle kohta näiteks komisjoni teatis „Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta“, (2023/C 328/02), p 7.

ruumides või kui neid käitatakse kolmanda riigi kasutajate jaoks. Nende kohaldamisalast väljajätmine on seotud üksnes kolmandate riikidega ja sellistes riikides asuvate kasutajatega ehk kohaldamisalast ei ole välja jäetud Eesti Vabariigi diplomaatilised ja konsulaaresindused, mis asuvad Euroopa Liidu territooriumil ega nende sellised süsteemid, mida käitatakse Euroopa Liidu kasutajate jaoks. Selliste süsteemide kaitse vajadus tuleneb NIS2-direktiivi põhieesmärgist ehk vajadusest tagada siseturul võtmetähtsusega üksuste ja nende osutatavate teenuste ühtlane, järjepidev ja riskipõhine kaitse.

KüTSi lisatava § 1 lõike 2[1] eesmärk on võtta üle NIS2-direktiivi artikli 2 lõige 9. Kõnealune lõige ja selles viidatud lõiked on sõnastatud järgmiselt.
7. [NIS2-direktiivi] ei kohaldata avaliku halduse üksuste suhtes, mis tegutsevad riigi julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamise, uurimise, avastamise ja nende eest vastutusele võtmise valdkonnas.
8. Liikmesriigid võivad vabastada konkreetsed üksused, mis tegutsevad riigi julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamise, uurimise, avastamise ja nende eest vastutusele võtmisega seotud tegevused, või mis osutavad teenuseid üksnes käesoleva artikli lõikes 7 osutatud avaliku halduse üksustele, artiklis 21 või 23 sätestatud kohustuste täitmisest seoses nimetatud tegevuste ja teenustega. Sellistel juhtudel VII peatükis osutatud järelevalve- ja täitemeetmeid nende konkreetsete tegevuste või teenuste suhtes ei kohaldata. Kui üksused tegelevad üksnes sellist liiki tegevusega või osutavaid üksnes sellist liiki teenuseid, millele on osutatud käesolevas lõikes, võivad liikmesriigid otsustada need üksused ka artiklites 3 ja 27 sätestatud kohustuste täitmisest vabastada.
9. Lõikeid 7 ja 8 ei kohaldata, kui üksus tegutseb usaldusteenuse osutajana.
NIS2-direktiivi artikli 2 lõiked 7 ja 8 on juba varem mööndustega üle võetud KüTSi § 1 lõikega 2 ning seda lõiget ei muudeta.

KüTSi § 1 lõige 3 tunnistatakse kehtetuks. Muudatus on seotud asjaoluga, et kehtetuks tunnistatava lõike olemus ning sisu on NIS2-direktiivist tulenevate iseärasustega arvestades sätestatud edaspidi KüTSi § 3 lõigetes 2–5 (iseäranis § 3 lõike 2 punktis 9, lõikes 3, lõike 4 punktis 8 ja lõikes 5).

KüTSi § 1 lõike 4 muutmine on seotud NIS2-direktiivi artikliga 4, mis sisustab olukorra, kus mõne üksuse jaoks kehtivad teisest õigusaktist tulenevad nõuded, mis on samaväärsed NIS2-direktiivi riskijuhtimismeetmete või olulistest intsidentidest teavitamise nõuetega. Sellises olukorras ei lähtu see üksus samaväärselt reguleeritud ulatuses (turvameetmete rakendamise, küberintsidentidest teavitamise või mõlema puhul) mitte KüTSis sätestatust, vaid vastavas valdkondlikus õigusaktis sätestatud nõuetest.
NIS2-direktiivi artikkel 4 on sõnastatud järgmiselt:
1. Kui valdkondlikes liidu õigusaktides nõutakse elutähtsatelt või olulistelt üksustelt küberturvalisuse riskijuhtimismeetmete võtmist või olulistest intsidentidest teatamist ning kui need nõuded on vähemalt samaväärse toimega kui [NIS2-direktiivis] sätestatud kohustused, ei kohaldata selliste üksuste suhtes [NIS2-direktiivi] asjakohaseid sätteid, sealhulgas VII peatükis sätestatud järelevalve- ja täitmise tagamise sätteid. Kui valdkondlikud liidu õigusaktid ei hõlma kõiki konkreetse sektori üksusi, mis kuuluvad [NIS2-direktiivi] kohaldamisalasse, kohaldatakse jätkuvalt [NIS2-direktiivi] asjakohaseid sätteid nende valdkondlike liidu õigusaktidega hõlmamata üksuste suhtes.
2. Käesoleva artikli lõikes 1 osutatud nõudeid käsitatakse samaväärse toimega kui [NIS2-direktiivis] sätestatud kohustused juhul, kui:
a) küberturvalisuse riskijuhtimismeetmed on mõjult vähemalt samaväärsed artikli 21 lõigetes 1 ja

2 sätestatud meetmetega või
b) valdkondlikus liidu õigusaktis nähakse ette [NIS2-direktiivi] kohane CSIRTide, pädevate asutuste või ühtsete kontaktpunktide viivitamatu, asjakohasel juhul automaatne ja otsene juurdepääs [NIS2-direktiivi] kohastele intsidenditeadetele ning kui olulistest intsidentidest teatamise nõuded on mõjult vähemalt samaväärsed [NIS2-direktiivi] artikli 23 lõigetes 1–6 sätestatud nõuetega.
3. [Euroopa Komisjon] annab hiljemalt 17. juuliks 2023 suunised, milles selgitatakse lõigete 1 ja 2 kohaldamist. Komisjon vaatab kõnealused suunised korrapäraselt läbi. Nende suuniste ettevalmistamisel võtab komisjon arvesse koostöörühma ja ENISA tähelepanekuid.
Muudatusega on seotud ka NIS2-direktiivi põhjendused 22–29 ja 31, mis selgitavad kommenteeritava muudatuse tausta ja mõtet.
(22) [NIS2-direktiivis] sätestatakse selle kohaldamisalasse kuuluvate sektorite küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse baastase. Selleks et vältida liidu õigusaktide küberturvalisuse sätete killustumist, kui küberturvalisuse kõrge taseme tagamiseks kogu liidus peetakse vajalikuks valdkondlikke lisasätteid, mis käsitlevad küberturvalisuse riskijuhtimismeetmeid ja teatamiskohustust, peaks komisjon hindama, kas sellised lisasätted võiks ette näha [NIS2-direktiivi] alla kuuluvas rakendusaktis. Kui sellised rakendusaktid ei ole selleks sobivad, võiksid liidu valdkondlikud õigusaktid aidata tagada kogu liitu hõlmava küberturvalisuse kõrge taseme, võttes ühtlasi täielikult arvesse asjaomaste sektorite eripära ja keerukust. Sel otstarbel ei välista [NIS2-direktiiv] ka niisuguste küberturvalisuse riskijuhtimismeetmeid ja intsidentidest teatamist käsitlevate edasiste valdkondlike liidu õigusaktide vastuvõtmist, milles võetakse igakülgselt arvesse vajadust luua terviklik ja ühtne küberturvalisuse raamistik. [NIS2-direktiiv] ei piira komisjonile mitmes sektoris, sealhulgas transpordi- ja energeetikasektoris antud rakendamisvolitusi.
(23) Kui valdkondlikes liidu õigusaktides on sätted, millega nõutakse elutähtsatelt[23] või olulistelt üksustelt küberturvalisuse riskijuhtimismeetmete võtmist või olulistest intsidentidest teatamist, ning kui need nõuded on vähemalt samaväärsed [NIS2-direktiivis] sätestatud kohustustega, tuleks neid sätteid, sealhulgas järelevalve- ja täitmise tagamise sätteid, niisuguste üksuste suhtes kohaldada. Kui valdkondlik liidu õigusakt ei hõlma kõiki konkreetse sektori üksusi, mis kuuluvad [NIS2-direktiivi] kohaldamisalasse, tuleks nimetatud liidu õigusaktiga hõlmamata üksuste suhtes kohaldada jätkuvalt [NIS2-direktiivi] asjakohaseid sätteid.
(24) Kui valdkondliku liidu õigusakti kohaselt peavad elutähtsad[24] või olulised üksused täitma teatamise kohustust, mille mõju on vähemalt samaväärne [NIS2-direktiivis] sätestatud teatamiskohustusega, tuleks tagada intsidenditeadete ühtne ja tulemuslik käsitlemine. Selleks tuleks intsidenditeateid käsitleva valdkondliku liidu õigusakti sätetega anda CSIRTidele, pädevatele asutustele või [NIS2-direktiivi] kohastele ühtsetele küberturvalisuse kontaktpunktidele (edaspidi „ühtsed kontaktpunktid“) vastavalt valdkondlikule liidu õigusaktile esitatud intsidenditeadetele viivitamata juurdepääs. Sellise viivitamatu juurdepääsu saab tagada eelkõige juhul, kui intsidenditeated edastatakse põhjendamatu viivituseta CSIRTile, pädevale asutusele või [NIS2-direktiivi] kohasele ühtsele kontaktpunktile. Kui see on asjakohane, peaksid liikmesriigid looma intsidenditeadete käsitlemiseks automaatse ja otsese teavitamise mehhanismi, mis tagab süstemaatilise ja vahetu teabevahetuse CSIRTide, pädevate asutuste või ühtse kontaktpunktiga. Teatamise lihtsustamiseks ning automaatse ja otsese teatamise mehhanismi rakendamiseks võiksid liikmesriigid kooskõlas valdkondliku liidu õigusaktiga kasutada ühtset kontaktpunkti.
(25) Valdkondlikes liidu õigusaktides, millega nähakse ette küberturvalisuse riskijuhtimismeetmed või teatamiskohustus, millel on [NIS2-direktiivis] sätestatuga vähemalt samaväärne mõju, võiks

[23] Eelnõus: „üliolulistelt üksustelt“.
[24] Eelnõus: „üliolulistelt üksustelt“.

ette näha, et nende õigusaktide kohased pädevad asutused kasutavad selliste meetmete või kohustustega seoses oma järelevalve- ja täitmise tagamise volitusi [NIS2-direktiivi] kohaselt määratud pädevate asutuste abil. Asjaomased pädevad asutused võivad sel eesmärgil kehtestada koostöökorra. Sellises koostöökorras võiks muu hulgas täpsustada järelevalvetegevuse koordineerimise korra, sealhulgas liikmesriigi õiguse kohaste uurimiste ja kohapealsete kontrollide korra ning pädevate asutuste vahelise järelevalvet ja täitmise tagamist käsitleva asjakohase teabe vahetamise mehhanismi, sealhulgas juurdepääsu kübervaldkonda puudutavale teabele, mida pädevad asutused [NIS2-direktiivi] kohaselt taotlevad.

(26) Kui valdkondlikes liidu õigusaktides on nõue, et üksused teataksid olulistest küberohtudest või pakutakse neile selleks stiimuleid, peaksid liikmesriigid samuti julgustama oluliste küberohtude jagamist CSIRTide, pädevate asutuste või [NIS2-direktiivi] kohaste ühtsete kontaktpunktidega, et tagada kõnealuste organite suurem teadlikkus küberohtudest ning võimaldada neil oluliste küberohtude realiseerumise korral tulemuslikult ja aegsasti reageerida.

(27) [NIS2-direktiivis] sätestatud mõisteid ning järelevalve- ja täitmise tagamise raamistikku tuleks tulevastes valdkondlikes liidu õigusaktides igakülgselt arvesse võtta.

(28) [NIS2-direktiiviga] seoses tuleks Euroopa Parlamendi ja nõukogu määrust (EL) 2022/2554 käsitada finantssektori ettevõtjate suhtes valdkondliku liidu õigusaktina. [NIS2-direktiivi] sätete asemel tuleks kohaldada määruse (EL) 2022/2554 sätteid, mis käsitlevad info- ja kommunikatsioonitehnoloogia (IKT) riskijuhtimist, IKT intsidentide haldamist ja eelkõige tõsistest IKT intsidentidest teavitamist, samuti digitaalse tegevuskerksuse testimist, teabevahetuse kokkuleppeid ja kolmandatest isikutest tulenevat IKT-riski. Seetõttu ei tohiks liikmesriigid [NIS2-direktiivi] sätteid, mis käsitlevad küberturvalisuse riskijuhtimist ja teatamiskohustust, järelevalvet ja täitmise tagamist, määruse (EL) 2022/2554 kohaldamisalasse jäävate finantssektori ettevõtjate suhtes kohaldada. Samal ajal on [NIS2-direktiivi] kohaselt oluline tihedate suhete ja teabevahetuse säilitamine finantssektoriga. Selleks võimaldab määrus (EL) 2022/2554 Euroopa järelevalveasutustel ja kõnealuse määruse kohastel pädevatel asutustel osaleda koostöörühma tegevuses ning vahetada teavet ja teha koostööd ühtsete kontaktpunktidega, samuti CSIRTidega ja [NIS2-direktiivi] kohaste pädevate asutustega. Määruse (EL) 2022/2554 kohased pädevad asutused peaksid edastama tõsiste IKT intsidentide ja asjakohasel juhul oluliste küberohtude üksikasjad ka CSIRTidele, pädevatele asutusele või [NIS2-direktiivi] kohastele ühtsetele kontaktpunktidele. See on saavutatav vahetu juurdepääsu tagamisega intsidenditeadetele ja nende otsese või intsidenditeadete ühtse kontaktpunkti edastamise kaudu. Lisaks peaksid liikmesriigid jätkuvalt kaasama finantssektori oma küberturvalisuse strateegiatesse ning CSIRTid võivad oma tegevuses hõlmata ka finantssektorit.

(29) Selleks et vältida lennundussektori üksustele kehtestatud küberturvalisuse kohustustes lünki ja kohustuste dubleerimist, peaksid Euroopa Parlamendi ja nõukogu määruste (EÜ) nr 300/2008 ja (EL) 2018/1139 kohased riiklikud asutused ning [NIS2-direktiivi] kohased pädevad asutused tegema seoses küberturvalisuse riskijuhtimismeetmete rakendamisega ja nende meetmete järgimise järelevalvega riiklikul tasandil koostööd. Kui üksus järgib määrustes (EÜ) nr 300/2008 ja (EL) 2018/1139 ning nende määruste alusel vastu võetud asjakohastes delegeeritud õigusaktides ja rakendusaktides sätestatud turvanõudeid, võivad [NIS2-direktiivi] kohased pädevad asutused käsitada seda [NIS2-direktiivis] sätestatud vastavate nõuete järgimisena.

(31) Digitaristu sektorisse kuuluvad üksused põhinevad sisuliselt võrgu- ja infosüsteemidel ning seetõttu peaksid neile üksustele [NIS2-direktiivi] alusel pandud kohustused nende üksuste küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse raames hõlmama terviklikult ka selliste süsteemide füüsilist turvalisust. Kuna need küsimused on hõlmatud [NIS2-direktiiviga], ei kohaldata selliste üksuste suhtes direktiivi (EL) 2022/2557 III, IV ja VI peatükis sätestatud kohustusi.

NIS2-direktiivi artikli 4 lõike 3 kohta on Euroopa Komisjon avaldanud 18. septembril 2023 teatise „Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta“ (2023/C 328/02).[25]
Kuna NIS2-direktiivi artikkel 4 näeb ette, et need erinõuded võivad tulla mõnest Euroopa Liidu õigusaktist (st ennekõike direktiivist, määrusest, rakendusmäärusest või delegeeritud määrusest), siis sõnastatakse kommenteeritav lõige vastavalt.
Arvestades NIS2-direktiivi eelpool viidatud põhjenduses esitatud selgitusi ning Euroopa Komisjoni 18. septembri 2023. a teatises sätestatut, on eelnõu koostamise ajal teada, et NIS2-direktiivi puhul on valdkondlik eriõigusakt finantssektoris kohalduv DORA määrus ning lennunduses kohalduvad määrused (EÜ) nr 300/2008 ja (EL) 2018/1139. Samas, arvestades NIS2-direktiivi artikli 4 avatud sõnastust, ei ole välistatud, et kui näiteks Euroopa Liidu seadusandja võtab veel mõnes teises valdkonnas vastu reeglid, mis tagavad selles valdkonnas NIS2-direktiiviga samaväärsed küberturvalisuse nõuded, siis saavad KüTSi § 1 lõike 4 alusel ka need normid KüTSis sätestatu suhtes erinormideks. Avalikul kooskõlastusel olnud eelnõu kavandis oli ka ette nähtud KüTSi § 1 lõige 4^1, mis oleks olnud volitusnorm võtta vastu määrus, millega sooviti täpsustada kommenteeritava lõike olukordi. Kavandile saabunud tagasiside ja edasiste arutelude tulemusena otsustati volitusnormist loobuda. Selle asemel on võimalik seda funktsiooni täita samasisuliste selgituste andmisega kas Justiits- ja Digiministeeriumi või Riigi Infosüsteemi Ameti võrgulehel. Tegemist oleks n-ö elava dokumendiga. Sel juhul puudub ka vajadus seda määrust uuendada, kui näiteks Euroopa või Eesti õigusaktist tuleneb *lex specialis* olukord.
Alljärgnevalt on illustreerival eesmärgil kirjeldatud finantssektoris kehtiva valdkondliku õigusakti (*lex specialis*) – DORA määruse – ja NIS2-direktiivi omavahelist koosmõju. DORA määruse nõudeid kohaldatakse NIS2-direktiivi kohaldamisalasse kuuluvate krediidiasutuste, kesksete vastaspoolte ja kauplemiskohtade suhtes. NIS2-direktiivi artikli 4 lõike 1 viimane lause sätestab, et „[kui] valdkondlikud liidu õigusaktid ei hõlma kõiki konkreetse sektori üksusi, mis kuuluvad käesoleva direktiivi kohaldamisalasse, kohaldatakse jätkuvalt [NIS2-direktiivi] asjakohaseid sätteid nende valdkondlike liidu õigusaktidega hõlmamata üksuste suhtes“. Seega kohaldub NIS2-direktiiv neile üksustele, kes on nimetatud NIS2-direktiivi artiklis 2[26] ning direktiivi I või II lisas, kuid mida ei peeta DORA määruse artikli 2 lõike 1 punktides a–t märgitud finantssektori üksuseks. Kui mingi üksus on NIS2-direktiivi artiklis 2 või I või II lisas nimetatud üksus ning samal ajal ka DORA määruse kohane finantssektori üksus, siis tuleks kohaldada mõlemat õigusakti, sh ka KüTSi. Sel juhul katab DORA määrus võrgu- ja infosüsteemide turvalisuse nõuded, mis toetavad DORA määruse artikli 1 lõike 2 kohase finantssektori üksuse äriprotsesse, samal ajal kui NIS2-direktiiv (st KüTS) kohaldub ainult neile teenustele, mis on nimetatud NIS2-direktiivi artiklis 2 või I või II lisas ning mis ei puuduta võrgu- ja infosüsteemide turvalisust ja toetavad finantssektori üksuse äriprotsesse.
NIS2-direktiivi artikli 4 tõttu ei kohaldata DORA määruse kohastele finantssektori üksustele erinevaid sätteid, sh ka NIS2-direktiivi artikli 23 lõiget 1 (kohustust teavitada olulise mõjuga küberintsidentidest). Samal ajal sätestab NIS2-direktiivi artikli 23 lõike 9 esimene lause, et „[ühtne] kontaktpunkt esitab ENISA-le iga kolme kuu tagant koondaruande, mis sisaldab anonüümseid koondandmeid käesoleva artikli lõike 1 ning artikli 30 kohaselt teatatud oluliste intsidentide,

[25] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0918%2801%29&qid=1726668543740
[26] Vt NIS2-direktiivi artikli 2 lõige 3, mis viitab CER-direktiivile, st NIS2-direktiivi (st KüTSi) kohaldamisalasse kuuluvad ka need üksused, kes on käsitatavad elutähtsa teenuse osutajatena. CER-direktiiv on üle võetud hädaolukorra seadusega ning selle § 36 lõige 3 sätestab finantssektoriga seotud elutähtsad teenused (makseteenus ja sularaharinglus), mis omakorda määrab teatud krediidiasutused elutähtsa teenuste osutajateks – vt Eesti Panga presidendi 13. juuli 2018. a määrus nr 7 „Makseteenuse ja sularaharingluse kirjeldus ja toimepidevuse nõuded” (https://www.riigiteataja.ee/akt/128062024010).

intsidentide, küber- ja napilt ära hoitud intsidentide kohta“. Kuna NIS2-direktiivi artikli 23 lõiget 1 ei saa kohaldada DORA määruse kohaste finantssektori üksuste suhtes, siis ei ole eelmainitud koondaruandes võimalik esitada ka DORA määruse artikli 19 alusel esitatavaid teateid. Samas näeb NIS2-direktiivi artikkel 30 (eelnõus KüTSi § 8^1) ette, et nii teenuseosutaja kui ka muu isik võib esitada teateid „oluliste intsidentide, intsidentide, küber- ja napilt ära hoitud intsidentide“ kohta vabatahtlikult. Seega kui DORA määruse kohane finantssektori üksus teavitab eelnõukohase KüTSi § 8^1 alusel olulise mõjuga küberintsidendist, küberintsidendist või küberohust, siis esitab Riigi Infosüsteemi Amet ka Euroopa Liidu Küberturvalisuse Ametile (ENISAle) eelmainitud infot sisaldava koondaruande.
Eeltoodu tulemusena ei kohaldata DORA määruse kohaldamisalas oleva finantssektori üksuse osutatavale DORA määruse kohaldamisalasse kuuluvale teenusele KüTSi §-e 3^1, 6, 6^1, 7 ja 8 ega ka nende rikkumisega seotud järelevalve- ja karistusnorme.
NIS2-direktiivi põhjendus 29 selgitab NIS2-direktiivi ja lennundusvaldkonna üksuste seost ning kohalduvaid nõudeid. Nende üksuste teenustele, kellele kohalduvad määrustes (EÜ) nr 300/2008 ja (EL) 2018/1139 ning nende määruste alusel vastu võetud asjakohastes delegeeritud õigusaktides ja rakendusaktides[27] sätestatud turvanõuded, kohaldatakse viidatud määruste nõudeid, mistõttu ei kohaldata neile teenustele KüTSi §-e 6, 6^1 ja 7. Nende üksuste puhul kohaldatakse küberintsidentidest teavitamise nõuet (KüTSi § 8), kuna sellele ei osuta eelviidatud põhjendus.

KüTSi §-s 2 esitatakse seaduses kasutatavate terminite loetelu. Eelnõuga kavandatakse seda täiendada uute, NIS2-direktiivi ülevõtmisest tulenevate terminitega. Kommenteeritava paragrahvi punktid esitatakse nende paljususe tõttu tähestikulises järjekorras. See ettepanek tehti autoritele ka eelnõu huvirühmadega kooskõlastamise käigus.

Eelnõukohase KüTSi § 2 punktiga 1 kavandatakse üle võtta NIS2-direktiivi artikli 6 punktis 31 kasutatud termin „andmekeskusteenus“. Kommenteeritava punktiga on seotud NIS2-direktiivi põhjendus 35:
(35) Andmekeskusteenuse osutajate pakutavaid teenuseid ei pakuta alati tingimata pilvandmetöötlusteenusena. Seega ei pruugi andmekeskused alati olla pilvandmetöötlustaristu osa. Kõigi võrgu- ja infosüsteemide turvalisusega seotud riskide juhtimiseks peaks seetõttu [NIS2-direktiivi] kohaldamisalasse kuuluma ka selliste andmekeskusteenuste pakkujad, mis ei ole pilvandmetöötlusteenused. [NIS2-direktiivi] kohaldamisel peaks mõiste „andmekeskusteenus“ kätkema sellise teenuse osutamist, mis hõlmab struktuure või struktuuride rühmi, mis on ette nähtud andmete talletamiseks, töötlemiseks ja edastamiseks kasutatava infotehnoloogia- (IT) ja võrguseadmete keskseks majutamiseks, omavahel sidumiseks ja käitamiseks, võttes arvesse ka energiajaotuse ja keskkonnajuhtimisega seotud rajatisi ja taristuid. Mõiste „andmekeskusteenus“ ei tohiks hõlmata asutusesiseseid andmekeskusi, mis kuuluvad asjaomasele üksusele ja mida käitatakse üksuse enda tarbeks.

Eelnõukohases KüTSi § 2 punktis 2 kavandatakse sätestada lühendtermin „digitaalse teenuse osutaja“, mis hõlmab mitut üksust. Nimetatud lühend on loodud ennekõike seetõttu, et eelnõu ülejäänud tekstis ei oleks vaja uuesti nimetada kõiki neid üksusi, mis on selle lühendiga hõlmatud. Selle asemel saabki kasutada kommenteeritava punktiga sätestatavat lühendit. Sama termin on kasutusel ka kehtivas seaduses, kus sellega tähistatakse üksnes § 4 lõikes 1 nimetatud infoühiskonna teenuse osutajaid (internetipõhise kauplemiskoha pakkuja, internetipõhise

[27] Näiteks: komisjoni rakendusmäärus (EL) 2015/1998, 5. november 2015, millega nähakse ette lennundusjulgestuse ühiste põhistandardite rakendamise üksikasjalikud meetmed, vt lisa p-d 1.0.6, 1.7, 11.1.2 ja 11.2.8, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02015R1998-20240901.

otsimootori pakkuja, pilvandmetöötlusteenuse osutaja). Käesoleva eelnõu kohaselt käsitatakse neid teenuseosutajaid jätkuvalt digitaalse teenuse osutajatena, kuid sama termini määratlusega on praktilistel kaalutlustel hõlmatud ka teatud hulk teisi NIS2-direktiivi subjekte, kelle suhtes on NIS2-direktiivis nõudeid muude subjektidega võrreldes teatud ulatuses diferentseeritud: domeeninimede süsteemi teenuse osutajad, tippdomeeninimede register, domeeninimede registreerimise teenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrguteenuse osutajad, haldusteenuse osutajad, infoturbeteenuse osutajad ja sotsiaalmeedia platvormi pakkujad.

Eelnõukohase KüTSi § 2 punktiga 3 on seotud sama paragrahvi punkt 2 ehk selles määratletakse viidatud punktis 2 nimetatud üksuse (digitaalse teenuse osutaja) esindaja. Kommenteeritava punktiga kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 34. Kommenteeritavas punktis esitatud definitsioonis viidatakse ainult Riigi Infosüsteemi Ametile seetõttu, et sellele ametile antakse küberintsidentide käsitlemise üksuse ehk CSIRTi ülesanded. Digitaalse teenuse osutaja kohustuste all on mõeldud neid kohustusi, mis tulenevad NIS2-direktiivi tulemusena ennekõike KüTSist, kuid olenevalt olukorrast ka Euroopa Komisjoni poolt NIS2-direktiivi alusel antud rakendusaktidest.

Eelnõukohase KüTSi § 2 punktiga 4 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 22, kuna selles esitatud termin on seotud KüTSi nõuetega hõlmatavate üksustega ning seda terminit kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides.
Domeeninimede registreerimise teenuse osutaja puhul tuleb arvestada asjaoluga, et NIS2-direktiiv ei määratle selliseid subjekte üliolulise üksuse ega ka olulise üksusena, samuti ei ole teda loetletud NIS2-direktiivi I ja II lisas. Eelöeldu põhjal kohalduvad neile ainult teatud NIS2-direktiivi nõuded. Erandiks on muidugi olukord, kus sama üksus osutab ka teisi teenuseid, mis kuuluvad NIS2-direktiivi kohaldamisalasse – nt kui domeeninimede registreerimise teenuseid osutav üksus on samal ajal ka domeeninimede süsteemi teenuse osutaja (vt eelnõukohase KüTSi § 2 punkt 6).
Domeeninimede registreerimise teenuse osutaja suhtes kohaldatakse ainult NIS2-direktiivi artikli 3 lõikeid 3–5 (need nõuded võetakse üle eelnõukohase KüTSi §-ga 3^1), artikleid 26 ja 27 (need nõuded võetakse üle eelnõukohase KüTSi §-ga 4) ja artiklit 28 (need nõuded võttis üle Eesti Interneti SA nõukogu, vt seletuskirjale lisatud vastavustabeli selgitusi). Teoreetiliselt saaks nende üksuste suhtes kohaldada ka NIS2-direktiivi artiklit 36, kuid see eeldaks eraldi väärteokoosseisu sätestamist olukorraks, kus eelviidatud nõudeid ei täideta. Kuid kuna samade nõuete täitmise eest ei ole NIS2-direktiivis ja seetõttu ka eelnõuga üliolulistе üksuste ja oluliste üksuste suhtes ette nähtud väärteovastutust, siis ei sätestata eelnõuga vastavat väärteokoosseisu ka domeeninimede registreerimise teenuse osutajate suhtes.
Eelnõu kooskõlastamise käigus märkis Eesti Interneti Sihtasutus (EIS), et EIS on käsitatav tippdomeeninimede registri pidajana, kuid EIS teeb järelevalvet kokku 51 akrediteeritud domeeni .ee registripidaja teenuse üle, 24 neist tegutsevad Eestis ja 27 välismaal.

Eelnõukohase KüTSi § 2 punktiga 5 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 19, kuna selles defineeritud termin on järgmises punktis esitatud termini osa.

Eelnõukohase KüTSi § 2 punktiga 6 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 20, kuna selles esitatud definitsioon on seotud KüTSi nõuetega hõlmatavate üksustega ning seda terminit kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides. Tegemist on terminiga (domeeninimede süsteemi teenuse osutaja), mis hõlmab kahte eri laadi üksust: esimene üksus osutab interneti lõppkasutajatele üldsusele kättesaadavat domeeninime rekursiivse teisendamise teenust ning teine üksus osutab kolmandatele isikutele kasutuseks domeeninime autoriteetse

teisendamise teenust, välja arvatud juurnimeserverid.
Kommenteeritava punktiga on seotud ka NIS2-direktiivi põhjendus 32:
(32) Usaldusväärse, vastupidava ja turvalise domeeninimede süsteemi (DNS) tagamine ja hoidmine on võtmetähtsusega, et säilitada interneti usaldusväärsus ning oluline, et tagada selle pidev ja stabiilne toimimine, millest sõltuvad digimajandus ja -ühiskond. Seepärast tuleks [NIS2-direktiivi] kohaldada tippdomeeninimede registrite ja domeeninimede süsteemi teenuse osutajate suhtes, mida tuleb käsitada üksustena, mis osutavad interneti lõppkasutajatele mõeldud üldkasutatavate domeeninimede rekursiivse teisendamise teenust või kolmandatele isikutele kasutamiseks mõeldud domeeninimede autoriteetse teisendamise teenust. [NIS2-direktiivi] ei tuleks kohaldada juurnimeserverite suhtes.
Kommenteeritavas punktis esitatud definitsioonis on ka märgitud, et tegemist peab olema üldsusele kättesaadava domeeninime rekursiivse teisendamise teenusega ehk kui näiteks seda teenust pakub eraisik oma pereliikmele, siis sel juhul pole tegemist üldsusele ehk kõigile soovijatele mõeldud teenusega.
Domeeninime autoriteetse teisendamise teenust pakutakse kolmandale isikule siis, kui nimetatud teenust pakutakse füüsilistele või juriidilistele isikutele, kes ei ole see sama teenuse osutaja. Sellega on tegu on näiteks juhul, kui domeeni autoriteetset nimeserverit ei halda domeeninime registreerija, vaid seda teenust pakub teine isik, näiteks domeeninimede registreerimise teenuse osutaja (registripidaja) või DNS-majutusteenuse pakkuja (inglise keeles *DNS hosting service provider*); kusjuures viimast peetakse domeeninime autoriteetse teisendamise teenuse pakkujaks kolmandale isikule.

Eelnõukohase KüTSi § 2 punktiga 7 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 39. Kuigi direktiivi ametlik eestikeelne tõlge kasutab sellele mõistele osutamiseks terminit „hallatud teenuse osutaja“, on eelnõu autorite hinnangul, arvestades mh eelnõu kooskõlastusringil saadud tagasiside ja valdkondlikus praktikas juurdunud terminoloogiaga, selgem kasutada terminit „haldusteenuse osutaja“. Haldusteenuse osutaja tegevus hõlmab näiteks kliendi sidevõrkude haldamist, sh viitab ka tegevustele, mida tehakse kliendi ruumides. Definitsioonis nimetatud tegevused on alternatiivsed ehk haldusteenuse osutaja ei pea kõiki definitsioonis nimetatud teenuseid pakkuma, vaid piisab ühest.

Eelnõukohase KüTSi § 2 punktiga 8 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 14, kuna NIS2-direktiivis kasutatavad ning KüTSi üle võetavad õigusnormid sisaldavad asjaomast terminit. Seetõttu on vaja ka selgelt määratleda, mida IKT-protsessi all mõeldakse. Kuna IKT-protsess on defineeritud juba kehtivas Euroopa Liidu määruses, siis on eelnõus viidatud sellele määrusele. Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (edaspidi *määrus (EL) 2019/881*) artikli 2 punkti 13 kohaselt on IKT-protsess „tegevused, mille käigus projekteeritakse või töötatakse välja IKT-toode või -teenus, seda tarnitakse või hallatakse“. Kuna kõnealune definitsioon on esitatud Euroopa Liidu määruses, on selle taasesitamine Vabariigi Valitsuse 22. detsembri 2011 määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ kohaselt võimalik ainult sellele viidates (vt viidatud määruse § 29 lg 3; sama põhimõte, kuigi esmapilgul seaduse teksti koormav, kohaldub kollisioonide vältimiseks kohustuslikult analoogia korras kõigi terminite puhul, mille definitsioonid sisalduvad Euroopa Liidu määrustes). Kui direktiivide puhul on mõeldavad erandid, siis määruste puhul mitte – sellel on väga praktiline põhjus, kuivõrd viimaste muutmise korral (olukorras, kus riigisiseses õiguses ei ole muudetavale õigusaktile viidatud) võivad tekkida vastuolud riigisisese ja ELi õiguse vahel. Ka Euroopa Kohus on märkinud,

et liikmesriigi poolt Euroopa Liidu määruse ülevõtmine selle sätete riigisisesesse õigusesse ümberkirjutamise abil ei ole lubatav (vt Euroopa Kohtu 7. veebruari 1973. aasta otsus asjas 39/72: komisjon *vs*. Itaalia. EKL 1973, lk 101; 2. veebruari 1977. aasta otsus asjas 50/76: Amsterdam Bulb BV *vs*. Produktschap voor Siergewassen, EKL 1977, lk 137).

Eelnõukohase KüTSi § 2 punktiga 9 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 13, kuna NIS2-direktiivis kasutatavad ning KüTSi üle võetavad õigusnormid sisaldavad asjaomast terminit. Seetõttu on vaja ka selgelt määratleda, mida IKT-teenuse all mõeldakse. Kuna IKT-teenus on defineeritud juba kehtivas Euroopa Liidu määruses, siis on eelnõus viidatud sellele määrusele. Määruse (EL) 2019/881 artikli 2 punkti 13 kohaselt on IKT-teenus „teenus, mis koosneb täielikult või peamiselt võrgu- ja infosüsteemide kaudu teabe edastamisest, säilitamisest, väljavõtmisest või töötlemisest“.

Eelnõukohase KüTSi § 2 punktiga 10 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 12, kuna NIS2-direktiivis kasutatavad ning KüTSi üle võetavad õigusnormid sisaldavad asjaomast terminit. Seetõttu on vaja ka selgelt määratleda, mida IKT-toote all mõeldakse. Kuna IKT-toode on defineeritud juba kehtivas Euroopa Liidu määruses, siis on eelnõus viidatud sellele määrusele. Määruse (EL) 2019/881 artikli 2 punkti 12 kohaselt on IKT-toode „võrgu- või infosüsteemi element või elementide rühm“.

Eelnõukohase KüTSi § 2 punktiga 11 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 40 (turbetarnija). NIS2-direktiivi eestikeelse versiooni algses sõnastuses kasutati terminit „turbetarnija“, kuid kõnesoleva eelnõu koostamise käigus on see termin asendatud terminiga „hallatud teenuste osutaja“. Samalaadset terminit kasutatakse ka kübersolidaarsuse määruse eelnõus[28]: nimelt „hallatud turbeteenuste osutaja“, mille defineerimisel omakorda viidatakse ka eelmainitud NIS2-direktiivi sättele. Eelnõus onnende terminite asemel kasutatud terminit „infoturbeteenuse osutaja“, kuna see termin, olgugi et on direktiivis kasutatavast originaalkeelsest terminist mõnevõrra erinev, on eelnõu kooskõlastusringil saadud tagasiside ja valdkondlikus praktikas väljakujunenud terminoloogiat arvestades tähenduselt selgem kui „turbetarnija“.
Kommenteeritavas punktis nimetatud üksuse (infoturbeteenuse osutaja) osutatavateks teenusteks võivad olla näiteks eelnõujärgses KüTSi § 7 lõikes 2 kavandatavad nõuete täitmisega seotud teenused – näiteks võib ta pakkuda IKT-valdkonnas küberintsidendi haldamise või lahendamise teenust.
Infoturbeteenuse osutaja on üksus, kes osutab enda teenust ennekõike äriklientidele (ingl *business-to-business*). Infoturbeteenuse osutajaga on näiteks tegemist siis, kui kontserni emaettevõtja osutab enda tütarettevõtjatele teenuseid, mis on hõlmatud infoturbeteenuse osutaja definitsiooniga.

Eelnõukohase KüTSi § 2 punktiga 12 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 18, kuna selles esitatud termin on seotud KüTSi nõuetega hõlmatavate üksuste terminiga (interneti sõlmpunkt). Eelnõus on kasutatud direktiivi originaalversiooni termini „interneti vahetuspunkt“ asemel terminit „interneti sõlmpunkt“, kuna see termin, olgugi et on direktiivi originaalterminist erinev, on eelnõu kooskõlastusringil saadud tagasisidet arvestades tähenduselt selgem kui „interneti vahetuspunkt“.

KüTSi § 2 punkt 13 on seotud NIS2-direktiivi artikli 6 punkti 28 ülevõtmisega, mis viitab Euroopa Parlamendi ja nõukogu direktiivi 2005/29/EÜ, mis käsitleb ettevõtja ja tarbija vaheliste tehingutega

[28] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32025R0038

seotud ebaausaid kaubandustavasid siseturul ning millega muudetakse nõukogu direktiivi 84/450/EMÜ, Euroopa Parlamendi ja nõukogu direktiive 97/7/EÜ, 98/27/EÜ ja 2002/65/EÜ ning Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 2006/2004 (edaspidi *direktiiv 2005/29/EÜ*), artikli 2 punktis n määratletud internetipõhisele kauplemiskohale. Direktiivi 2005/29/EÜ artikli 2 punktis n on internetipõhine kauplemiskoht määratletud kui „teenus, mis võimaldab tarbijatel sõlmida teiste ettevõtjate või tarbijatega kauglepinguid, kasutades selleks tarkvara, sealhulgas veebisaiti, veebisaidi osa või rakendust, mida käitab ettevõtja või mida käitatakse ettevõtja nimel“. Tarbijakaitseseaduse § 2 punkti 7 kohaselt on internetipõhine kauplemiskoht „kauplemiskoht, kus tarbija saab sõlmida teise kaupleja või tarbijaga lepinguid sidevahendi abil, kasutades selleks tarkvara, sealhulgas veebilehte, veebilehe osa või rakendust, mida käitab kaupleja või mida käitatakse kaupleja nimel“. Võlaõigusseaduse § 54^3 lõike 1 kohaselt on internetipõhine kauplemiskoht „kauplemiskoht, kus tarbija saab sõlmida teise ettevõtja või tarbijaga lepinguid sidevahendi abil, kasutades selleks tarkvara, sealhulgas veebilehte, veebilehe osa või rakendust, mida käitab ettevõtja või mida käitatakse ettevõtja nimel“. Sama paragrahvi lõike 2 kohaselt on internetipõhise kauplemiskoha pidaja „ettevõtja, kes pakub tarbijatele internetipõhist kauplemiskohta“.
Direktiivi 2005/29/EÜ artikli 2 punkti a kohaselt on tarbija „füüsiline isik, kes [direktiiviga 2005/29/EÜ] hõlmatud kaubandustavade raames tegutseb eesmärkidel, mis ei ole seotud tema kaubandus-, majandus-, käsitöö- ega kutsetegevusega“. Tarbijakaitseseaduse § 2 punkti 1 kohaselt on tarbija „füüsiline isik, kes tegutseb eesmärgil, mis ei ole seotud tema majandus- või kutsetegevusega“. Võlaõigusseaduse § 1 lõike 5 kohaselt on tarbija tolle seaduse tähenduses „füüsiline isik, kes teeb tehingu, mis ei seondu iseseisva majandus- või kutsetegevuse läbiviimisega“.
Direktiivi 2005/29/EÜ artikli 2 punkti b kohaselt on ettevõtja „füüsiline või juriidiline isik, kes [direktiiviga 2005/29/EÜ] hõlmatud kaubandustavade raames tegutseb eesmärkidel, mis on seotud tema kaubandus-, majandus-, käsitöö- või kutsetegevusega, ning ettevõtja nimel või huvides tegutsev isik“. Tarbijakaitseseaduse § 2 punkt 2 kohaselt on kaupleja „füüsiline või juriidiline isik, sealhulgas avalik-õiguslik juriidiline isik, kes tegutseb eesmärgil, mis on seotud tema majandus- või kutsetegevusega“. Võlaõigusseaduse § 1 lõike 6 kohaselt on ettevõtja tolle seaduse tähenduses „isik, sealhulgas avalik-õiguslik juriidiline isik, kes teeb tehingu, mis seondub iseseisva majandus- või kutsetegevuse läbiviimisega“.
Direktiivi 2005/29/EÜ artikli 2 punktis n sätestatud internetipõhise kauplemiskoha definitsioon on sisult sama mis tarbijakaitseseaduse § 2 punktis 7 ja võlaõigusseaduse § 54^3 lõikes 1 esitatud internetipõhise kauplemiskoha definitsioon. Kommenteeritavasse eelnõu punkti on otsustatud lisada viide vastavale tarbijakaitseseaduse terminile.

Eelnõukohase KüTSi § 2 punktis 14 kavandatakse sätestada lühendtermin „keskvalitsuse avaliku halduse üksus“, mis hõlmab mitut üksust, kes kuuluvad kehtiva KüTSi kohaldamisalasse. Kommenteeritav lühend on seotud ka NIS2-direktiivi artikli 2 lõike 2 punkti f alapunktiga i (*üksus on: keskvalitsuse avaliku halduse üksus, nagu see on kindlaks määratud liikmesriigi poolt kooskõlas tema õigusega*). Kommenteeritaval punktil on seos ka avaliku halduse üksuse mõistega, mis on defineeritud NIS2-direktiivi artikli 6 punktis 35 (mida eelnõuga eraldi üle ei võta). Kommenteeritava punkti puhul on tegemist ka kehtiva õiguse säilitamisega, kuna asjaomane mõiste hõlmab KüTSi kehtiva versiooni § 3 lõike 4 punktides 3, 5, 6, 7, 8, 11, 12 ja 14 nimetatud üksusi.

Eelnõukohase KüTSi § 2 punktis 15 kavandatakse sätestada, sarnaselt eelkommenteeritud punktiga, lühendtermin „kohaliku omavalitsuse avaliku halduse üksus“, mis on seotud NIS2-

direktiivi artikli 6 punktis 35 sätestatud mõistega, kuid nimetatud lühendtermin on seotud ka NIS2-direktiivi artikli 2 lõike 5 punkti a rakendamisega (*Liikmesriigid võivad ette näha, et [NIS2-direktiivi] kohaldatakse: a) kohaliku tasandi avaliku halduse üksuste suhtes*.) ning kehtiva õiguse säilitamisega (vt KüTSi kehtiva versiooni § 3 lõike 4 punktis 4 kasutatud termin „kohaliku omavalitsuse üksus“ ja punkt 13). Kommenteeritaval punktil pole seost NIS2-direktiivi artikli 2 lõike 2 punkti f alapunktiga ii (*üksus on: ii) liikmesriigi poolt tema õiguse kohaselt kindlaks määratud piirkondliku tasandi üksus, mis vastavalt riskipõhisele hindamisele osutab teenuseid, mille häirel võib olla oluline mõju kriitilise tähtsusega ühiskondlikule või majandustegevusele*), kuna kõnealuse alapunkti sisu on seotud piirkondliku (ingl *regional*) tasandi üksustega ehk Eesti puhul maavalitsustega, mida enam ei ole.
Kui kommenteeritava NIS2-direktiivi sätte ülevõtmisel otsustatakse, et see võetakse kitsamalt üle ja kehtivat õigust ei säilitata, siis võib see kaasa tuua olukorra, kus kohalike omavalitsuste ja nende haldusala asutuste suhtes ei kohaldata ühtseid küberturvalisuse nõudeid. See omakorda võib tuua kaasa tõrkeid ja probleeme nende osutatavate avalike teenuste osutamisel või nende võrgu- ja infosüsteemide puhul, sh ka nende üksuste valduses olevate (isiku)andmete turvalisusega seoses.

Eelnõukohase KüTSi § 2 punktiga 16 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 27, milles on kasutatud ka sama artikli punktis 26 kasutatud terminit (kvalifitseeritud usaldusteenus). See punkt sätestatakse, kuna see on seotud KüTSi nõuetega hõlmatavate üksuste terminiga ning seda terminit kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides. Euroopa Parlamendi ja nõukogu määruse (EL) 910/2014 e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ (edaspidi *määrus (EL) 910/2014*) artikli 3 punkti 20 kohaselt on kvalifitseeritud usaldusteenuse osutaja „usaldusteenuse osutaja, kes osutab üht või mitut kvalifitseeritud usaldusteenust ning kellele järelevalveasutus on andnud kvalifitseeritud staatuse“.

Eelnõukohase KüTSi § 2 punktiga 17 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 8, seostades toimingud ja menetlused, mille eesmärk on küberintsidenti ennetada, tuvastada, analüüsida, ohjata või lahendada ja sellest taastuda. Eelnõus on kasutatud direktiivi originaaltekstis kasutatud termini „intsidendi käsitlemine“ asemel terminit „küberintsidendi käsitlemine“, tagamaks kehtivas õiguses kasutusel oleva ja praktikas juurdunud terminoloogia võimalikult suures ulatuses säilimine ka NIS2-direktiivi ülevõtmise protsessis.

Eelnõukohases KüTSi § 2 punktis 18 sätestada kavandatud termin vastab kehtiva seaduse § 2 punktis 3 sätestatud terminile „küberintsident“ ning selle määratlus NIS2-direktiivi artikli 6 punktis 6 esitatud termini „intsident” definitsioonile. Kõnealuse termini tähendus jääb samaks mis kehtivas õiguses. Selle definitsioon hõlmab ka NIS2-direktiivi artikli 6 punktis 5 sätestatud „intsidendiohtu“ (definitsioon: „sündmus, mis oleks võinud kahjustada salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust ja konfidentsiaalsust, kuid mis õnnestus ära hoida või mis ei tekkinud“) ning NIS2-direktiivi artiklites kasutatud terminit „napilt ära hoitud intsident“ (ingl *near miss*).

Eelnõukohases KüTSi § 2 punktis 19 sätestada kavandatud termin vastab olemuselt kehtiva seaduse § 2 punktis 8 kasutatud terminile „küberturbe intsidentide lahendamise üksus“ ning selle määratlus NIS2-direktiivi artikli 1 lõike 2 punktis a esitatud CSIRTi definitsioonile. Eelnõus on just viimasest tulenevalt, arvestades ka kooskõlastusringi käigus saadud tagasisidega, siiski otsustatud asendada terminis sisalduv sõna „lahendamine“ sõnaga „käsitlemine“. Sellist lähenemist

toetab ka NIS2-direktiivi ingliskeelne versioon, mille artikli 11 lõike 3 punkti c kohaselt on CSIRTi ülesanne „responding to incidents“ ja vajaduse korral teenuse osutajatele abi pakkumine, mitte aga „resolve incidents“ ehk lahendamine, millele vastaks kehtivas õiguses kasutatud termin. Samale viitab ka NIS2-direktiivi põhjendus 42, sätestades, et: „The CSIRTs are tasked with incident handling“ (eestikeelses versioonis „CSIRTide ülesandeks on intsidentide käsitlemine“).

Eelnõukohase KüTSi § 2 punktiga 20 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 10, kuna NIS2-direktiiv näeb ette küberohtudega seotud teabe vahetamist ja jagamist. Seetõttu on vaja ka selgelt määratleda, mida „küberohu“ all mõeldakse. Kuna küberoht on defineeritud juba kehtivas Euroopa Liidu määruses, siis saab termini defineerida viidates, mistõttu ongi eelnõus esitatud viide sellele määrusele. Määruse (EL) 2019/881 artikli 2 punkti 8 kohaselt on küberoht „võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada“.

Eelnõukohase KüTSi § 2 punkti 21 eesmärk on määratleda termin „küberturvalisus“, mis on defineeritud juba kehtivas Euroopa Liidu määruses, andes ka selguse, kuidas sisustada muid KüTSi õigusnorme, milles on küberturvalisust mainitud. Tegemist on ka NIS2-direktiivi artikli 6 punkti 3 ülevõtmisega. Määruse (EL) 2019/881 artikli 2 punkti 1 kohaselt on küberturvalisus „tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest“.

Eelnõukohase KüTSi § 2 punktiga 22 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 11, kuna NIS2-direktiiv näeb ette „oluliste küberohtudega“ seotud teabe vahetamise ja jagamise. Kommenteeritavas punktis sätestatav termin hõlmab ka termini „küberoht“ tähendust ja see termin on juba varem KüTSi § 2 punktis 20 sisustatud. Olulise küberohu puhul on seega tegemist mistahes võimaliku olulise asjaolu, sündmuse või tegevusega, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil märkimisväärset kahju tekitada – näiteks uut tüüpi, varasemast efektiivsemad või sagenenud lunavararünded, turvahaavatavuse avastamine mõnes konkreetses sektoris laialdaselt kasutusel olevas tarkvaras jm.

Eelnõukohane KüTSi § 2 punkt 23 on seotud NIS2-direktiivi artikli 6 punkti 30 ülevõtmisega ehk kehtiva KüTSi § 2 punktis 7 määratletud termini „pilvandmetöötlusteenus“ tähenduse täpsustamisega võrreldes NIS2-direktiivis määratletud terminiga. Kommenteeritav punkt on seotud KüTSi nõuetega hõlmatavate üksuste terminiga ning seda terminit kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides. Kommenteeritava punktiga on seotud ka NIS2-direktiivi põhjendused 33 ja 34:
(33) Pilvandmetöötlusteenused peaksid hõlmama digiteenuseid, mis võimaldavad jagatavate andmetöötlusressursside skaleeritava ja paindliku kogumi nõudepõhist haldamist ning ulatuslikku kaugpääsu sellele kogumile, muu hulgas juhul, kui need ressursid paiknevad hajutatult erinevates kohtades. Andmetöötlusressursid on näiteks võrgud, serverid ja muu taristu, operatsioonisüsteemid, tarkvara, talletusruum, rakendused ja teenused. Pilvandmetöötluse teenusemudelid hõlmavad muu hulgas taristut teenusena (IaaS), platvormi teenusena (PaaS), tarkvara teenusena (SaaS) ja võrku teenusena (NaaS). Pilvandmetöötluse korraldusmudelid peaksid hõlmama privaat-, ühis-, avalikku ja hübriidpilve. Mõistetel „pilvandmetöötlusteenus“ ja „korraldusmudel“ on sama tähendus nagu nimetatud mõistetel standardi ISO/IEC 17788:2014 määratluses. Pilvandmetöötlusteenuse kasutaja võimekust tagada endale ühepoolselt andmetöötlusvõimekus, nagu serveriaeg või võrgu talletusruum, ilma pilvandmetöötlusteenuse osutaja inimesepoolse sekkumiseta, võiks nimetada nõudepõhiseks haldamiseks.

Mõistega „ulatuslik kaugpääs“ peetakse silmas seda, et pilvevõimalusi pakutakse võrgu kaudu ja need on kättesaadavad mehhanismide kaudu (sealhulgas mobiiltelefonid, tahvelarvutid, sülearvutid ja tööjaamad), mis toetavad heterogeensete nn kõhnade või paksude kliendiplatvormide kasutamist. Mõiste „skaleeritav“ osutab andmetöötlusressurssidele, mis on nõudluse kõikumisega toimetulekuks pilveteenuse osutaja poolt paindlikult jaotatavad olenemata ressursside geograafilisest asukohast. Mõistet „paindlik kogum“ kasutatakse andmetöötlusressursside kirjeldamiseks, mida pakutakse ja mis tehakse kättesaadavaks vastavalt nõudlusele, et kättesaadavaid ressursse suurendada või vähendada sõltuvalt töökoormusest. Mõistet „jagatav“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse paljudele kasutajatele, kellel on ühine juurdepääs teenusele, kuid mille puhul andmete töötlemine toimub iga kasutaja jaoks eraldi, olgugi et teenust osutatakse samadest elektroonilistest seadmetest. Mõistet „hajusad“ kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mis asuvad erinevates võrguga ühendatud arvutites või seadmetes ning mis suhtlevad omavahel ja kooskõlastavad omavahelist tegevust sõnumite edastamise teel.
(34) Kuna maad võtavad uuenduslikud tehnoloogiad ja ärimudelid, tulevad eeldatavasti tarbijate muutuvate vajaduste järgi siseturule uued pilvandmetöötlusteenuse ja korraldusmudelid. Sellises kontekstis võib pilvandmetöötlusteenuseid osutada väga hajusal kujul, mille puhul töötlus toimub andmete loomise või kogumise kohale veelgi lähemal; seega liikudes nn traditsiooniliselt mudelilt väga hajusale mudelile (servtöötlus).

Eelnõukohase KüTSi § 2 punktiga 24 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 9, kuna NIS2-direktiiv näeb ette riskidega seotud teabe vahetamise ja jagamise. Seetõttu on vaja ka selgelt kindlaks määrata, mida „riski“ all mõeldakse ehk see termin määratleda. Termini definitsioon, kuigi seda võiks praktilistel põhjustel mõneti korrigeerida, peab vastama NIS2-direktiivi omale ja sellest riigisiseselt kõrvale kalduda ei saa.

Eelnõukohase KüTSi § 2 punktiga 25 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 32 (sisulevivõrk). Kommenteeritav punkt on seotud KüTSi nõuetega hõlmatavate üksuste terminiga ning seda terminit kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides. Kommenteeritava termini puhul on NIS2-direktiivis esitatud definitsioonis kasutatud sõna „digiteenus“, kuid kõnesolevas eelnõus on selle asemel kasutatud terminit „infoühiskonna teenus“, et siduda see infoühiskonna teenuse mõistega, mis on defineeritud infoühiskonna teenuste seaduse § 2 punktis 1 kui: „teenus, mida osutatakse majandus- või kutsetegevuse raames teenuse kasutaja otsesel taotlusel ja mille puhul andmeid töödeldakse, säilitatakse ja edastatakse digitaalkujul andmete töötlemiseks ja säilitamiseks mõeldud elektrooniliste vahendite abil, kusjuures osapooled ei viibi üheaegselt samas kohas. Infoühiskonna teenus peab olema täielikult üle kantud, edastatud ja vastu võetud elektrooniliste sidevahendite abil. Infoühiskonna teenus ei ole faksi ega telefonikõne abil edastatud teenus ega televisiooni- või raadioteenus“. Selles definitsioonis on digisisu all silmas peetud kõiki digiandmeid (ingl *digital data*), nii staatiliselt kui ka dünaamiliselt vahetatavaid andmeid.

Eelnõukohase KüTSi § 2 punktiga 26 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 33 (sotsiaalvõrguteenuse platvorm). Kommenteeritav punkt on seotud KüTSi nõuetega hõlmatavate üksuste terminiga ning seda terminit kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides. Üheselt mõistetavuse huvides on terminit direktiiviga võrreldes täpsustatud (sotsiaalmeediaplatvorm).

Eelnõukohase KüTSi § 2 punktiga 27 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 41

(teadusasutus). Kommenteeritav punkt on seotud KüTSi nõuetega hõlmatavate üksuste definitsiooniga. Kommenteeritava punktiga on seotud NIS2-direktiivi põhjendus 36:
(36) Teadusuuringutel on uute toodete ja protsesside väljatöötamisel võtmeroll. Paljusid neist tegevustest viivad ellu üksused, mis jagavad, levitavad või kasutavad oma teadusuuringute tulemusi ärilistel eesmärkidel. Need üksused võivad seega olla olulised osalejad väärtusahelates, mis muudab nende võrgu- ja infosüsteemide turvalisuse siseturu üldise küberturvalisuse lahutamatuks osaks. Teadusorganisatsioone tuleks käsitada nii, et need hõlmavad üksusi, mis pühendavad olulise osa oma tegevusest rakendusuuringutele või tootearendusele Majanduskoostöö ja Arengu Organisatsiooni 2015. aasta Frascati käsiraamatu „Guidelines for Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing and marketing of a product, process or the provision of a service" („Teadus- ja arendustegevuse andmete kogumise ja esitamise suunised, et kasutada nende tulemusi ärilistel eesmärkidel, näiteks toote, protsessi või teenuse tootmiseks või turustamiseks")[29] tähenduses.

Eelnõukohase KüTSi § 2 punktiga 28 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 21, kuna selles esitatud termin on seotud KüTSi nõuetega hõlmatavate üksuste terminiga ning seda kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides (tippdomeeninimede register). Kommenteeritava punkti definitsiooni lauselõpp on „välja arvatud juhul, kui register kasutab tippdomeeninimesid ainult enda tarbeks". Tippdomeeninimede register kasutab tippdomeeninimesid ainult enda tarbeks siis, kui tippdomeeninime register sisaldab kõiki asjaomase keskkonna registreeringuid, seda ennekõike ühtse registreerija mudeli (ingl *single-registrant model*) puhul. Sellega on tegu näiteks olukorras, kus mõnel ettevõtjal on mõne brändi tippdomeen ja ta on samal ajal ka selle brändi tippdomeeninime registreerija, et takistada kolmandatel isikutel selle brändiga seotud tippdomeeninime registreerimist.

Eelnõukohase KüTSi § 2 punktiga 29 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 15, mille direktiivi eestikeelses versioonis kasutatakse terminit „nõrkus". Eelnõus on kasutatud sama mõiste tähistamiseks terminit „turvahaavatavus", kuna see termin on, olgugi et on direktiivi originaalterminist mõnevõrra erinev, eelnõu kooskõlastusringil saadud tagasiside ja valdkondlikus praktikas väljakujunenud terminoloogiaga arvestades tähenduselt selgem kui „nõrkus". Termin defineeritakse, kuna NIS2-direktiiv näeb ette turvahaavatavusega seotud teabe vahetamise ja jagamise. Termini definitsioon, kuigi sedagi võiks praktilistel põhjustel mõneti korrigeerida, peab vastama NIS2-direktiivi omale ja sellest riigisiseselt kõrvale kalduda ei saa.

Eelnõukohases KüTSi § 2 punktis 30 määratletav termin (turvameetmed) vastab kehtiva KüTSi § 2 punktis 2^1 sätestatud terminile ning säilitatakse olemasolevas tähenduses.

Eelnõukohase KüTSi § 2 punktiga 31 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 7. Liikmesriigi all on mõeldud Euroopa Liidu liikmesriiki. Märkimisväärse mõju kohta vt NIS2-direktiivi artikkel 23 (mis võetakse üle eelnõukohase KüTSi §-ga 8), sh ennekõike selle lõikeid 1, 3 ja 11. Siinjuures on ka asjakohased NIS2-direktiivi põhjendused 68–73, sh ennekõike põhjendus 69:
(*68) Liikmesriigid peaksid aitama kaasa komisjoni soovituses (EL) 2017/1584 ette nähtud küberturvalisuse kriisidele reageerimise ELi raamistiku loomisele olemasolevate koostöövõrgustike, eelkõige Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule (EU-*

[29] https://www.oecd.org/en/publications/frascati-manual-2015_9789264239012-en.html

CyCLONe), CSIRTide võrgustiku ja koostöörühma tegevuse kaudu. EU-CyCLONe ja CSIRTide võrgustik peaksid tegema koostööd menetluskorra alusel, milles määratakse kindlaks kõnealuse koostöö üksikasjad, ning vältima ülesannete dubleerimist. EU-CyCLONe menetluskorras tuleks täpsustada võrgustiku toimimist puudutav kord, muu hulgas rollid, koostööviisid, teiste asjaomaste osalejatega suhtlemine, teabevahetuse vormid ja kommunikatsioonivahendid. Liidu tasandi kriisiohje puhul peaksid asjaomased pooled lähtuma nõukogu rakendusotsuses (EL) 2018/1993 sätestatud kriisidele poliitilist reageerimist käsitlevast ELi integreeritud korrast (edaspidi „IPCRi kord“). Komisjon peaks selleks rakendama üldise kiirhoiatussüsteemi ARGUS kõrgetasemelise valdkondadevahelise kriisikoordineerimise menetlusprotsessi. Kui kriisil on oluline välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, tuleks käivitada Euroopa välisteenistuse kriisidele reageerimise mehhanism.

(69) Soovituse (EL) 2017/1584 lisa kohaselt tuleks ulatusliku küberturbeintsidendina mõista intsidenti, mille põhjustatud häired on niivõrd laialdased, et ühe liikmesriigi suutlikkusest nendega toimetulekuks ei piisa, või millel on märkimisväärne mõju vähemalt kahele liikmesriigile. Olenevalt nende põhjusest ja mõjust võivad ulatuslikud küberturbeintsidendid eskaleeruda ning muutuda täieulatuslikuks kriisiks, mis takistab siseturu tõrgeteta toimimist või kujutab endast mitme liikmesriigi või kogu liidu üksustele või kodanikele tõsist avaliku julgeoleku- või turvalisusriski. Võttes arvesse selliste intsidentide ulatuslikku haaret ja (enamikul juhtudel) piiriülest laadi, peaksid liikmesriigid ning asjaomased liidu institutsioonid, organid ja asutused tegema koostööd nii tehnilisel, operatiiv- kui ka poliitilisel tasandil, et reageerimist liidu ulatuses nõuetekohaselt koordineerida.

(70) Liidu tasandi ulatuslike küberturbeintsidentide ja kriiside puhul tuleb kiire ja tõhusa reageerimise tagamiseks võtta koordineeritud meetmeid, kuna sektorite ja liikmesriikide omavaheline sõltuvus on väga suur. Kübervastupidavusvõimeliste võrgu- ja infosüsteemide olemasolu ning andmete kättesaadavus, konfidentsiaalsus ja terviklus on väga olulised liidu julgeoleku ning liidu kodanike, ettevõtjate ja institutsioonide kaitsmiseks intsidentide ja küberohtude eest ning samuti selleks, et suurendada üksikisikute ja organisatsioonide usaldust liidu võimekuse vastu edendada ja kaitsta üleilmset, avatud, vaba, stabiilset ja turvalist küberruumi, mis põhineb inimõigustel, põhivabadustel, demokraatial ja õigusriigil.

(71) EU-CyCLONe peaks ulatuslike küberturbeintsidentide ja kriiside korral toimima vahendajana tehnilise ja poliitilise tasandi vahel ning tõhustama operatiivtasandi koostööd ja toetama otsuste tegemist poliitilisel tasandil. Võttes arvesse komisjoni pädevust kriisiohje valdkonnas, peaks EU-CyCLONe koostöös komisjoniga tuginema CSIRTide võrgustiku järeldustele ja kasutama oma võimekust, et koostada ulatuslike küberturbeintsidentide ja kriiside mõjuanalüüs.

(72) Küberründed on oma olemuselt piiriülesed ning oluline intsident võib häirida ja kahjustada elutähtsaid teabetaristuid, millest sõltub siseturu sujuv toimimine. Kõigi asjaomaste osalejate rolli käsitletakse soovituses (EL) 2017/1584. Lisaks vastutab komisjon Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL loodud liidu elanikkonnakaitse mehhanismi raames üldiste valmisolekumeetmete eest, mis hõlmavad hädaolukordadele reageerimise koordineerimiskeskuse ning ühise hädaolukordade side- ja infosüsteemi haldamist, olukorrateadlikkuse ja analüüsivõime säilitamist ja edasiarendamist ning liikmesriigi või kolmanda riigi abitaotluse korral eksperdirühmade mobiliseerimise ja lähetamise võimekuse loomist ja haldamist. Komisjon vastutab ka rakendusotsuse (EL) 2018/1993 kohase IPCRi korra analüüsiaruannete esitamise eest, muu hulgas seoses küberturvalisuse olukorrateadlikkuse ja valmisolekuga, samuti olukorrateadlikkuse ja kriisidele reageerimisega põllumajanduse, ebasoodsate ilmastikutingimuste, konfliktide kaardistamise ja prognooside, loodusõnnetuste varajase hoiatamise süsteemide, tervisealaste hädaolukordade, nakkushaiguste seire, taimetervise, keemiliste ainetega seotud juhtumite, toidu- ja söödaohutuse, loomatervise, rände, tolli,

tuumaavariide ja kiirguslike avariiolukordade ning energeetika valdkonnas.
(73) Kui see on asjakohane, võib liit kooskõlas ELi toimimise lepingu artikliga 218 sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldab neil osaleda ja korraldada osalust mõningates koostöörühma, CSIRTide võrgustiku ning EU-CyCLONe tegevuses. Selliste lepingutega tuleks tagada liidu huvid ja piisaval tasemel andmekaitse. See ei tohiks välistada liikmesriikide õigust teha nõrkuste haldamisel ja küberturvalisuse riskijuhtimisel koostööd kolmandate riikidega, hõlbustades liidu õiguse kohast teatamist ja üldist teabevahetust.
Ulatuslik küberintsident hõlmab ka neid küberintsidente, mida käsitatakse olulise mõjuga küberintsidentidena (vt KüTSi § 8 lõiked 2 ja 3), kuid mitte vastupidi ehk kõik olulise mõjuga küberintsidendid ei pruugi muutuda ulatuslikuks küberintsidendiks.

Eelnõukohase KüTSi § 2 punktiga 32 kavandatakse üle võtta NIS2-direktiivi artikli 6 punktid 24 ja 25. Asjaomased terminid defineeritakse, kuna see on seotud KüTSi nõuetega hõlmatavate üksuste terminiga ning seda terminit kasutatakse NIS2-direktiivist KüTSi üle võetavates õigusnormides. Määruse (EL) 910/2014 artikli 3 punktis 19 on usaldusteenuse osutaja defineeritud kui: „füüsiline või juriidiline isik, kes osutab üht või mitut usaldusteenust kas kvalifitseeritud või kvalifitseerimata usaldusteenuse osutajana“. Sama määruse artikli 3 punktis 16 on usaldusteenus defineeritud kui „elektrooniline teenus, mida tavaliselt osutatakse tasu eest ja mis hõlmab üht järgmistest:
a) e-allkirja sertifikaatide, e-templi sertifikaatide, veebisaidi autentimise sertifikaatide või muude usaldusteenuste osutamiseks vajalike sertifikaatide väljastamine;
b) e-allkirja sertifikaatide, e-templi sertifikaatide, veebisaidi autentimise sertifikaatide või muude usaldusteenuste osutamiseks vajalike sertifikaatide valideerimine;
c) e-allkirjade või e-templite loomine;
d) e-allkirjade või e-templite valideerimine;
e) e-allkirjade, e-templite, e-allkirja sertifikaatide või e-templi sertifikaatide säilitamine;
f) e-allkirja või e-templi kaugloomise vahendite haldamine;
g) elektrooniliste tõendite väljastamine;
h) elektrooniliste tõendite valideerimine;
i) e-ajatemplite loomine;
j) e-ajatemplite valideerimine;
k) registreeritud e-andmevahetusteenuste osutamine;
l) registreeritud e-andmevahetusteenuste kaudu edastatud andmete ja nendega seotud tõendite valideerimine;
m) elektrooniliste andmete ja e-dokumentide elektrooniline arhiveerimine;
n) elektrooniliste andmete kandmine elektroonilisse arvestusraamatusse“.
2024. a mais jõustusid muudatused, mis laiendasid usaldusteenuse mõistet ehk NIS2-direktiivi vastuvõtmise ajal oli selle mõistega hõlmatud vähem elektroonilisi teenuseid. Kõnesoleva eelnõuga ei ole võimalik ka seda mõistet kitsendada (ehk piiritleda see mõiste ainult enne 2024. a maid olemas olnud usaldusteenustega), kuna vastasel juhul tekib olukord, kus usaldusteenuste osutajad peavad hakkama küberturvalisuse valdkonnas täitma erinevaid nõudeid, st osadele kehtivad NIS2-direktiivist tulenevad nõuded ja osadele (2024. a maist lisandunud usaldusteenustele) justkui konkreetseid nõudeid KüTSi alusel ei kehtiks.

Eelnõukohase KüTSi § 2 punktiga 33 seotud muudatused (võrreldes kehtiva KüTSi § 2 punktis 6 sätestatud terminiga) tulenevad NIS2-direktiivi artikli 6 punkti 29 ülevõtmise vajadusest. Viimane viitab Euroopa Parlamendi ja nõukogu määruse (EL) 2019/1150, mis käsitleb õigluse ja

läbipaistvuse edendamist veebipõhiste vahendusteenuste ärikasutajate jaoks (edaspidi *määrus 2019/1150*), artikli 2 punktis 5 määratletud internetipõhisele otsingumootorile. NIS2-direktiivi eestikeelses tõlkes on ekslikult märgitud, et tegemist on direktiiviga, kuid tegelikkuses on tegemist määrusega. Seetõttu on ka eelnõus viidatud määrusele, mitte direktiivile. Määruse 2019/1150 artikli 2 punktis 5 on internetipõhine otsingumootor „digitaalne teenus, mis võimaldab kasutajatel sisestada päringuid, et teha otsinguid üldjuhul kõikidel veebisaitidel või teatavas keeles kõikidel veebisaitidel mis tahes teemal võtmesõna, häälkäskluse, fraasi või muu sisendi vormis tehtud päringu alusel, ning saadab vastuseks mis tahes vormingus tulemused, kust võib leida teavet taotletud sisu kohta“.
Määruse 2019/1150 artikli 2 punkti 5 eestikeelses versioonis ei ole kasutatud terminit „internetipõhine otsingumootor“ (nagu on NIS2-direktiivi eestikeelses versioonis), vaid terminit „veebipõhine otsingumootor“. Seetõttu on kommenteeritavas punktis (st ka määruse 2019/1150 viites) kasutatud terminit „veebipõhine otsingumootor“. Samalaadset terminit on kasutatud näiteks ka tarbijakaitseseaduse § 17 lõikes 2^2: „veebipõhiste otsingumootorite pakkujad“.

Eelnõukohases KüTSi § 2 punktis 34 määratletav termin (võrgu- ja infosüsteem) vastab kehtiva KüTSi § 2 punktis 1 sätestatud terminile ning säilitatakse olemasolevas tähenduses. Võrreldes kehtiva sõnastusega on termini lõppu keeleliselt parandatud.

Eelnõukohases KüTSi § 2 punktis 35 määratletav termin (võrgu- ja infosüsteemi turvalisus) vastab kehtiva KüTSi § 2 punktis 2 sätestatud terminile ning säilitatakse peaaegu üksüheselt olemasolevas tähenduses. Ainus muudatus on seotud asjaoluga, et eelnõujärgses sättes kasutatud sõna „sündmus“ tähendus on laiem kui kehtivas redaktsioonis kasutatud sõna „tegevus“ oma ning see tähistab võrgu- ja infosüsteemi turvalisuse mõistet paremini. Muudatuse tulemusena on kommenteeritav termin ka selgemini kooskõlas NIS2-direktiivi artikli 6 punktis 2 kasutatud terminiga „võrgu- ja infosüsteemide turvalisus“, mille defineerimisel kasutatakse samuti sõna „sündmus“.

Eelnõukohase KüTSi § 2 punktiga 36 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 38: „füüsiline isik või juriidiline isik, kes on asutatud ja keda tunnustatakse tema tegevuskohajärgse riigisisese õiguse kohaselt, kes võib enda nimel omada õigusi ja kanda kohustusi“. Kommenteeritava punkti selgituses on märgitud, et sättes viidatud „õiguse” puhul on tegemist tegevuskohajärgse riigisisese õigusega, kuna näiteks digitaalse teenuse osutajate korral võib tekkida olukord, kus konkreetne isik ei ole Eestis asutatud, kuid ta osutab teenuseid ka Eestis olevatele klientidele. Kommenteeritavat terminit „üksus“ kasutatakse ka eelnõuga KüTSi §-i 3 lisatavates uutes lõigetes ning KüTSis puudus parem samalaadne sõna, mis sõna „üksus“ olemust paremini iseloomustaks. Näiteks ei ole siinjuures võimalik kasutada lühendit/terminit „teenuse osutaja“, kuna sellel on teine kontekst, vt ka KüTS § 3 lõike 1 muutmise selgitust. Terminiga „üksus” ei viidata ühe organisatsiooni struktuuriüksusele (nt osakonnale), vaid selle all mõeldakse organisatsiooni tervikuna, s.o juriidilist isikut või asutust. Kui organisatsiooni üks struktuuriüksus osutab mingit teenust, mis on nimetaud eelnõu §-s 3, siis kvalifitseerub see vastav organisatsioon tervikuna KüTSi teenuseosutajaks – kuid sel juhul tuleb lisaks hinnata, et millise osa puhul selle organisatsiooni tegevusest tuleb järgida KüTSi nõudeid (vt ka KüTSi § 1 lg 4 muutmise selgitust).

Eelnõukohane KüTSi § 2 punkt 37 on seotud termini „üldkasutatava elektroonilise side teenus“ määratlemisega. NIS2-direktiiv ei määratle iseenesest terminit „üldkasutatav elektroonilise side teenus“ ega viita mõnele direktiivi (EL) 2018/1972 artikli 2 punktile. Siiski on NIS2-direktiivis kasutatud terminit „üldkasutatava elektroonilise side teenuse osutaja“, mistõttu selgitatakse

seletuskirjas üheselt mõistetavuse tagamiseks vastavat teenust.
Kaudselt on kommenteeritav termin seotud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (edaspidi *direktiiv (EL) 2018/1972*), artikli 2 järgmiste punktidega:

- punkt 13: „kasutaja“ – juriidiline või füüsiline isik, kes kasutab üldkasutatavat elektroonilise side teenust või taotleb selle kasutamist;
- punkt 14: „lõppkasutaja“ – kasutaja, kes ei paku üldkasutatavaid elektroonilise side võrke ega üldkasutatavaid elektroonilise side teenuseid;
- punkt 15: „tarbija“ – füüsiline isik, kes kasutab üldkasutatavat elektroonilise side teenust või taotleb selle kasutamist eesmärkidel, mis ei ole seotud tema kaubandustegevuse, äritegevuse, oskustöö või erialaga;
- punkt 31: „kõne“ – üldkasutatava isikutevahelise side teenuse abil loodud ühendus, mis võimaldab kahepoolset kõnesidet;
- punkt 32: „kõneside teenus“ – üldkasutatav elektroonilise side teenus, mis otse või kaudselt võimaldab riigisiseste või riigisiseste ja rahvusvaheliste kõnede algatamist ja vastuvõtmist riigi või riigi ja rahvusvahelisse numeratsiooniplaani kuuluva numbri või numbrite abil.

Kommenteeritava termini ja eelnimetatud direktiivis (EL) 2018/1972 kasutatud terminitega on seotud elektroonilise side seaduse § 2 järgmised punktid:

- punkt 5 „elektroonilise side ettevõtja“ (lühendina *sideettevõtja*) – isik, kes osutab lõppkasutajale või teisele üldkasutatava elektroonilise side teenuse osutajale üldkasutatavat elektroonilise side teenust;
- punkt 7: „elektroonilise side teenuse kasutaja“ (lühendina *sideteenuse kasutaja*) – isik, kes kasutab üldkasutatavat elektroonilise side teenust;
- punkt 8^4 „internetiühenduse teenus“ – üldkasutatav elektroonilise side teenus, millega võimaldatakse juurdepääsu internetile ja selle kaudu internetiga ühendatud lõpp-punktidele sõltumata kasutatavast võrgutehnoloogiast või terminalseadmest;
- punkt 9^1 „isikutevahelise side teenus“ – üldkasutatav elektroonilise side teenus, mis ei hõlma teenuseid, mis võimaldavad isikutevahelist vastastikust suhtlust teise teenusega lahutamatult seotud vähem olulise lisavõimalusena, kuid võimaldab üldkasutatava elektroonilise side võrgu kaudu isikutevahelist vastastikust suhtlust lõpliku arvu isikute vahel ning mille puhul side algatanud või selles osalevad isikud määravad kindlaks teabe saaja;
- punkt 11 „kaabelleviteenus“ – üldkasutatav elektroonilise side teenus, mis seisneb lõppkasutajale televisiooni- või raadiosaadete või televisiooni- või raadioprogrammide edastamises kokkulepitud tasu eest;
- punkt 15 „klient“ – üldkasutatavat elektroonilise side teenust kasutav isik, kellel on üldkasutatava elektroonilise side teenuse kasutamiseks leping sideettevõtjaga;
- punkt 27 „lõppkasutaja“ – klient, kes ise ei osuta üldkasutatavat elektroonilise side teenust;
- punkt 31 „mobiiltelefoniteenus“ – üldkasutatav elektroonilise side teenus, mis võimaldab kindlaks määramata asukohas riigisiseste ja rahvusvaheliste kõnede tegemist ja vastuvõtmist ning juurdepääsu hädaabiteenustele Eesti või rahvusvahelisse numeratsiooniplaani kuuluva numbri või sellega seotud lühivalikukoodi abil osalise või täieliku raadioside loomise teel;
- punkt 38 „püsiliiniteenus“ – üldkasutatav elektroonilise side teenus, mis seisneb kliendile püsiliini kasutada andmises;
- punkt 58 „telefoniteenus“ – üldkasutatav elektroonilise side teenus, mis võimaldab riigisiseste ja rahvusvaheliste kõnede tegemist ning vastuvõtmist Eesti või rahvusvahelisse

numeratsiooniplaani kuuluva numbri abil;
- punkt 64 „virtuaalvõrguteenus“ – sideettevõtja poolt osutatav üldkasutatav elektroonilise side teenus, mis põhineb teisele sideettevõtjale kuuluvas üldkasutatavas elektroonilise side võrgus loodaval näival ühendusel või vahendil.

Üldkasutatava elektroonilise side teenuse näited on esitatud eelmise lõigus, kuid see termin on ka elektroonilise side seaduses eraldi defineeritud. Elektroonilise side seaduse § 2 punkti 68 kohaselt on üldkasutatav elektroonilise side teenus „teenus, mida sideettevõtja pakub vastaval sideteenuse turul üldistel alustel kõikidele isikutele, ilma et isikud peaksid vastama mingitele neid teistest sarnastest isikutest eristavatele tunnustele. Teenus on üldkasutatav eelkõige siis, kui selle osutamine on kestev ja järjepidev ning seda pakutakse sisuliselt ühesugustel tingimustel“. Seetõttu on kommenteeritavas punktis viidatud elektroonilise side seaduse vastavale terminile.

Eelnõukohase KüTSi § 2 punktiga 38 kavandatakse üle võtta NIS2-direktiivi artikli 6 punkt 36, mis viitab direktiivi (EL) 2018/1972 artikli 2 punktis 8 määratletud üldkasutatavale elektroonilise side võrgule. Direktiivi (EL) 2018/1972 artikli 2 punktis 8 on üldkasutatav elektroonilise side võrk defineeritud kui „elektroonilise side võrk, mida kasutatakse ainult või peamiselt avalikult kättesaadavate elektroonilise side teenuste pakkumiseks ning mis toetab teabe edastamist võrgu lõpp-punktide vahel“. Elektroonilise side seaduse § 2 punkti 71 kohaselt on üldkasutatav elektroonilise side võrk „võrk, mille kaudu osutatakse üldkasutatavat elektroonilise side teenust, mis võimaldab teabe edastamist elektroonilise side võrgu lõpp-punktide vahel“. Vt selgitust üldkasutatava elektroonilise side teenuse termini kohta.
Direktiivi (EL) 2018/1972 artikli 2 punktis 1 on elektroonilise side võrk defineeritud kui „ülekandesüsteemid, mis võivad, aga ei pruugi põhineda püsitaristul või kesksel juhtimisel, ja vajaduse korral lülitus- ja marsruutimisseadmed ning muud vahendid, sealhulgas võrguelemendid, mis ei ole aktiivsed, mis võimaldavad edastada signaale kaabli kaudu, raadio teel, optiliselt või muude elektromagnetiliste vahendite abil, kasutades sealhulgas satelliitvõrke, püsivõrke (ahel- ja pakettkommuteeritud võrgud, k.a internet) ja mobiilsidevõrke, elektrikaabelsüsteeme, kui neid kasutatakse signaalide edastamiseks, raadio- ja teleringhäälinguvõrke ja kaabeltelevisioonivõrke, olenemata sellest, millist teavet nende kaudu edastatakse“. Elektroonilise side seaduse § 2 punktis 8 on elektroonilise side võrk defineeritud kui „ülekandesüsteem koos selle tööks vajalike lülitusseadmete ning muude tugisüsteemidega, mis võimaldab signaalide edastamist ja suunamist kaabli kaudu, samuti raadio, optiliste või muude elektromagnetiliste vahenditega. Muu hulgas on elektroonilise side võrkudeks, sõltumata nende kaudu edastatava informatsiooni iseloomust, satelliitvõrk, telefonivõrk, andmesidevõrk, mobiiltelefonivõrk, ringhäälinguvõrk, kaabellevivõrk ja elektrikaablisüsteem, kui seda kasutatakse signaalide edastamiseks või suunamiseks.“
Direktiivi (EL) 2018/1972 artikli 2 punktis 9 on võrgu lõpp-punkt defineeritud kui „füüsiline koht, kus lõppkasutajale pakutakse juurdepääsu üldkasutatavale elektroonilise side võrgule ning kus identifitseeritakse võrgu lõpp-punkt konkreetse võrguaadressi abil, juhul kui võrgus kasutatakse kommuteerimist või marsruutimist, mis võib olla seotud lõppkasutaja numbri või nimega“. Elektroonilise side seaduse § 2 punkti 70 kohaselt on üldkasutatav elektroonilise side võrgu lõpp-punkt „üldkasutatava elektroonilise side võrgu füüsiliselt kindlaks määratud punkt, kus kliendile on loodud juurdepääs või võimalus juurdepääsuks üldkasutatavale elektroonilise side võrgule“. Seetõttu on kommenteeritavas punktis viidatud elektroonilise side seaduse vastavale terminile.

Eelnõukohases KüTSi §-s 3 defineeritakse sarnaselt kehtiva KüTSiga termin „teenuseosutaja“ ja määratakse seeläbi suuresti kindlaks ka KüTSi kohaldamisala. Kõnealuse paragrahvi ja eelnõu subjektide ringiga seoses on asjakohased NIS2-direktiivi alltoodud põhjendused 4–7 ja 16, mis selgitavad NIS2-direktiiviga ette nähtud küberturvalisuse nõuete järgimise kohustusega subjektide

ringi täiendamist ning vajadust varasem küberturvalisuse direktiiv (direktiiv (EL) 2016/1148) kehtetuks tunnistada ja lähtuda Euroopa Komisjoni soovitusest 2003/361/EÜ:
(4) Direktiivi (EL) 2016/1148 õiguslik alus oli Euroopa Liidu toimimise lepingu artikkel 114, mille eesmärk on siseturu rajamine ja toimimise tagamine riigisiseste normide ühtlustamise meetmete tõhustamise abil. Teenuseid osutavatele või majanduslikult olulist tegevust ellu viivatele üksustele kehtestatud küberturvalisuse nõuded erinevad liikmesriigiti märkimisväärselt nii nõuete liigi, üksikasjalikkuse kui ka järelevalvemeetodi poolest. Need erisused toovad kaasa lisakulusid ning põhjustavad raskusi piiriüleselt kaupu või teenuseid pakkuvatele üksustele. Ühe liikmesriigi kehtestatud nõuded, mis erinevad teise liikmesriigi kehtestatud nõuetest või on nendega lausa vastuolus, võivad sellist piiriülest tegevust oluliselt pärssida. Lisaks mõjutab küberturvalisuse nõuete ebatõhus kavandamine või rakendamine ühes liikmesriigis tõenäoliselt küberturvalisuse taset ka teistes liikmesriikides, kui piiriülene suhtlus on sedavõrd intensiivne. Direktiivi (EL) 2016/1148 läbivaatamise käigus selgus, et liikmesriigid kohaldavad seda väga erinevalt, muu hulgas seoses selle kohaldamisalaga, mille piiritlemine jäeti suuresti liikmesriikide otsustada. Direktiiviga (EL) 2016/1148 anti liikmesriikidele ka väga ulatuslik kaalutlusõigus direktiivis sätestatud turvalisuse tagamise ja intsidentidest teatamise kohustuse rakendamisel. Seega rakendati neid kohustusi liikmesriigi tasandil väga erinevalt. Sarnaseid lahknevusi oli ka direktiivi (EL) 2016/1148 järelevalve- ja täitmise tagamise sätete rakendamisel.
(5) Kõik need erinevused põhjustavad siseturu killustumist ja võivad kahjustada selle toimimist, mõjutades eelkõige teenuste piiriülest osutamist ja kübervastupidavusvõime taset, kuna rakendatavad meetmed on erinevad. Lõppkokkuvõttes võivad need erinevused tuua kaasa selle, et mõni liikmesriik on küberohtude vastu vähem kaitstud, millel võib olla ülekanduv mõju kogu liidus. [NIS2-direktiivi] eesmärk on kõrvaldada sellised suured erinevused liikmesriikide vahel, sätestades koordineeritud reguleeriva raamistiku toimimisega seotud miinimumnormid, kehtestades liikmesriikide vastutavate asutuste tulemuslikuks koostööks vajalikud mehhanismid, ajakohastades selliste sektorite ja tegevuste loetelu, mille suhtes küberturvalisusega seotud kohustusi kohaldatakse, ning nähes ette tõhusad õiguskaitsevahendid ja täitemeetmed, mis on olulised nende kohustuste tulemusliku täitmise tagamiseks. Seega tuleks direktiiv (EL) 2016/1148 kehtetuks tunnistada ja asendada [NIS2-direktiiviga].
(6) Direktiivi (EL) 2016/1148 kehtetuks tunnistamisega tuleks sektoripõhist kohaldamisala laiendada suuremale osale majandusest, et hõlmata võimalikult täielikult kõik sektorid ja teenused, mis on siseturu peamise ühiskondliku ja majandustegevuse jaoks elutähtsad. Eelkõige on [NIS2-direktiivi] eesmärk kõrvaldada puudused, mis on seotud elutähtsate teenuste osutajate ja digiteenuse osutajate eristamisega, mis on osutunud iganenuks, kuna ei kajasta sektorite või teenuste tähtsust siseturu ühiskondliku ja majandustegevuse jaoks.
(7) Direktiivi (EL) 2016/1148 kohaselt oli liikmesriikidel kohustus kindlaks teha üksused, mis vastavad oluliste teenuste operaatori kriteeriumidele. Et kõrvaldada sellest tulenevad liikmesriikidevahelised suured erinevused ning tagada kõigile asjaomastele üksustele küberturvalisuse riskijuhtimismeetmete ja teatamiskohustusega seoses õiguskindlus, tuleks kehtestada ühtne kriteerium, mille alusel tehakse kindlaks [NIS2-direktiivi] kohaldamisalasse kuuluvad üksused. See kriteerium peaks põhinema suuruse ülempiiri reegli kohaldamisel, mille kohaselt jäävad [NIS2-direktiivi] kohaldamisalasse kõik üksused, mida käsitatakse komisjoni soovituse 2003/361/EÜ lisa artikli 2 kohaselt keskmise suurusega ettevõtjana või mis ületavad keskmise suurusega ettevõtja ülemmäärasid, mis on esitatud kõnealuse artikli lõikes 1, ning tegutsevad [NIS2-direktiiviga] hõlmatud sektorites, osutavad teenuseid või viivad ellu tegevusi, mis kuuluvad selle kohaldamisalasse. Liikmesriigid peaksid samuti ette nägema, et [NIS2-direktiivi] kohaldamisalasse kuuluvad teatavad kõnealuse soovituse lisa artikli 2 lõigetes 2 ja 3 määratletud väikesed ettevõtjad ja mikroettevõtjad, mis vastavad konkreetsetele kriteeriumidele,

mis näitavad ühiskonna, majanduse või konkreetsete sektorite või teenuseliikide võtmerolli.
(16) Vältimaks seda, et üksusi, millel on partnerettevõtjad või mis on sidusettevõtjad, peetaks elutähtsateks[30] või olulisteks üksusteks, kui see oleks ebaproportsionaalne, on liikmesriikidel võimalik soovituse 2003/361/EÜ lisa artikli 6 lõike 2 kohaldamisel võtta arvesse üksuse oma partneritest või sidusettevõtjatest sõltumatuse määra. Eelkõige on liikmesriikidel võimalik võtta arvesse asjaolu, et üksus on oma partner- või sidusettevõtjatest sõltumatu teenuste osutamisel kasutatavate võrgu- ja infosüsteemide osas, ja teenuste osas, mida üksus osutab. Selle põhjal võivad liikmesriigid asjakohasel juhul leida, et nimetatud üksust ei saa käsitada 2003/361/EÜ lisa artikli 2 kohase keskmise suurusega ettevõtjana või et üksus ei ületa keskmise suurusega ettevõtja kõnealuse artikli lõikes 1 esitatud ülemmäärasid, kui pärast selle üksuse sõltumatuse määra arvestamist üksnes tema enda andmete arvesse võtmisel ei käsitataks teda keskmise suurusega ettevõtjana või neid ülemmäärasid ületavana. See ei mõjuta [NIS2-direktiivi] kohaldamisalasse kuuluvate partner- ja sidusettevõtjate [NIS2-direktiivis] sätestatud kohustusi.
Lisaks eeltoodule on asjakohased NIS2-direktiivi põhjendused 20 ja 21:
(20) Komisjon peaks koostöös koostöörühmaga ja pärast konsulteerimist asjaomaste sidusrühmadega andma mikroettevõtjate ja väikeste ettevõtjate suhtes kohaldatavate kriteeriumide rakendamise suunised, et hinnata, kas nad kuuluvad [NIS2-direktiivi] kohaldamisalasse. Samuti peaks komisjon tagama, et asjakohaseid suuniseid antakse [NIS2-direktiivi] kohaldamisalasse kuuluvatele mikroettevõtjatele ja väikestele ettevõtjatele. Komisjon peaks liikmesriikide toetusel tegema sellekohase teabe mikroettevõtjatele ja väikestele ettevõtjatele kättesaadavaks.
(21) Komisjon peaks andma suunised, mille eesmärk on abistada liikmesriike kohaldamisala käsitlevate [NIS2-direktiivi] sätete rakendamisel ja [NIS2-direktiivi] kohaselt võetavate meetmete proportsionaalsuse hindamisel, eelkõige seoses üksustega, millel on keerukad ärimudelid või tegevuskeskkonnad, mille puhul võib üksus vastata korraga nii elutähtsa[31] kui ka olulise üksuse kriteeriumidele või viia samal ajal ellu tegevusi, millest osa kuulub [NIS2-direktiivi] kohaldamisalasse ja osa mitte.
Eelnõukohane KüTSi § 3 on üles ehitatud järgmiselt. Lõikes 1 esitatakse üldine teenuseosutaja määratlus: teenuseosutaja on eelnõu kohaselt ühiskonna toimimise seisukohast ülioluline ja oluline üksus, mida eelnõus nimetatakse edaspidi lühemalt vastavalt „ülioluline üksus“ ja „oluline üksus“. Lõigetes 2 ja 3 loetletakse KüTSi tähenduses üliolulised üksused ning lõigetes 4 ja 5 KüTSi tähenduses olulised üksused. Kuivõrd nii üliolulise kui ka olulise üksuse määramisel tugineb NIS2-direktiiv ja ka eelnõu osaliselt Euroopa Komisjoni soovitusele 2003/361/EÜ, siis on kommenteeritava paragrahvi lõigetes 6 ja 7 täpsustatud teatavaid nimetatud soovituse kohaldamisel järgitavaid aspekte. Ühtlasi tuleb tähele panna, et teatud üksused (vastavalt kommenteeritava paragrahvi lõike 2 punktides 1–9 ja lõike 4 punktides 1–9 nimetatud üksused) kvalifitseeruvad NIS2-direktiivi järgi vastavalt ülitähtsaks või oluliseks sõltumata oma suurusest ehk finants- ja tööjõunäitajatest (vt ka NIS2-direktiivi põhjenduse 7 viimane lause).
Eelnõukohase §ga 3 võetakse üle NIS2-direktiivi artiklis 3 ning lisades I ja II ette nähtud elutähtsa (eelnõus üliolulise) ja olulise üksuse mõisted ning nendega seotud NIS2-direktiivi puudutavad kohaldamisala reeglid, mis on sätestatud artiklis 2.
Eelnõu kooskõlastusringil saadud tagasiside alusel on KüTSi teenuseosutaja mõistega seotud sätted koondatud ühte paragrahvi (kommenteeritav KüTSi § 3) ja püütud seeläbi teha KüTSi kohaldamisala seaduse rakendajale paremini loetavaks ja mõistetavaks. Seaduse rakendaja peaks vaatama kommenteeritavat paragrahvi 3 ning tuvastama, kas ta on lõigete 2 või 3 kohane ülioluline üksus või lõigete 4 ja 5 kohane oluline üksus.
Osa eelnõukohases KüTSi §-s 3 nimetatud isikutest kuuluvad KüTSi kohaldamisalasse sõltumata

[30] Eelnõus „üliolulisteks üksusteks“.
[31] Eelnõus „üliolulise üksuse“.

nende suurusest ja käibest, näiteks kui tegemist on elutähtsa teenuse osutajaga hädaolukorra seaduse tähenduses või keskvalitsuse avaliku sektori üksusega jne. Arvestades selliste üksuste rolli ühiskonnas ja võimalikke küberturvalisusega seotud riskide laialdast mõju, on Euroopa Liidu seadusandja pidanud NIS2-direktiivi reeglite rakendamist nende puhul vajalikuks sõltumata nende suurusest.

Osa eelnõukohases KüTSi §-s 3 nimetatud isikutest kuuluvad KüTSi kohaldamisalasse aga üksnes siis, kui nad vastavad teatavatele töötajate arvu ning käibe- või bilansimahu piirmääradele. See tähendab, et Euroopa Liidu seadusandja on pidanud nende allutamist direktiivist tulenevatele reeglitele vajalikuks üksnes siis, kui nad on teatud suuruses (finants- ja tööjõunäitajate põhjal). NIS2-direktiivi artikli 2 lõike 1 kohaselt tuleb lähtuda üksuse töötajate arvust ning bilansi- või käibemahust, arvestades Euroopa Komisjoni soovitusega 2003/361/EÜ.

Seejuures on oluline, et töötjate arv ning bilansi- või käibemahtude piirmäärad on ette nähtud nii üliolulistele kui ka olulistele üksustele, kuid neile rakenduvad piirmäärad on erinevad. Vastavatest piirmääradest lähtumine on ülioluliste üksuste puhul ette nähtud KüTSi § 3 lõike 2 punktis 9 ja lõikes 3 ning oluliste üksuste puhul KüTS § 3 lõike 4 punktis 8 ja lõikes 5. Nimetatud sätetes on ära nimetatud ka konkreetsel juhul rakenduvad piirmäärad.

Kuna töötajate arvu ning bilansi- või käibemahu piirmäärade arvutamise üldine lähtealus on Euroopa Komisjoni soovitus 2003/361/EÜ, siis selgitatakse alljärgnevalt esmalt nende üldist kohaldumise loogikat. Iga konkreetse eelnõukohase KüTSi § 3 lõike või punkti kohaldamisel saab mh arvestada nende üldisemate selgitustega.

Euroopa Komisjoni soovituse 2003/361/EÜ kohaselt on keskmise suurusega ettevõtja ettevõtja, kellel on a) vähemalt 50 töötajat ning b) kelle bilansimaht või aastakäive ületab 10 miljonit eurot. Mõlemad tingimused peavad olema täidetud, st kui ettevõtjal on näiteks vähemalt 50 töötajat, kuid bilansimaht või aastakäive on väiksem kui 10 miljonit eurot, siis pole tegemist keskmise suurusega ettevõtjaga; bilansimaht või aastakäive ei tohi olla väiksem kui 10 miljonit eurot. Sama loogika ja tulemus kehtivad ka vastupidi ehk kui bilansimaht või aastakäive on vähemalt 10 miljonit eurot, kuid ettevõtjal on vähem kui 50 töötajat, ei ole tegemist keskmise suurusega ettevõtjaga; bilansimahu ja aastakäibe puhul on vaja, et vähemalt üks neist oleks suurem kui 10 miljonit eurot. Siinset selgitust tuleb arvestada koosmõjus järgmiste selgitusega.

Euroopa Komisjoni soovituse 2003/361/EÜ lisa artiklites 2–6 selgitatakse mh, millised on ettevõtjate suuruste kategooriad ja milliseid asjaolusid tuleb arvesse võtta, kui arvutatakse töötajate arvu ning bilansimahtu või aastakäivet. Näiteks selle soovituse lisa artikkel 3 näeb ette, mis laadi ettevõtjaid (ingl *enterprise*) tuleb arvestada töötajate arvu ja finantsnäitajate väljaselgitamisel, eristades autonoomseid, partner- ja sidusettevõtjaid (ingl vastavalt *autonomous, partner and linked enterprises*). Nende artiklite sisu tuleb arvesse võtta nimetatud soovituse alusel töötajate arvu ja finantsnäitajate väljaselgitamisel. Näiteks ei saa töötajate arvu ja finantsnäitajate suuruse kindlakstegemisel hinnata ainult tegevusi, mis on kirjas NIS2-direktiivi I ja II lisas, vaid lähtuvalt soovituse 2003/361/EÜ lisast tuleb analüüsida kogu organisatsiooni.

Analüüsimisel on abiks Euroopa Liidu Väljaannete Talituse veebilehel avaldatud „VKEde määratlust käsitlev teatmik“[32] (edaspidi *teatmik*), milles selgitatakse, millised ettevõtjad on mikro- ning väikese ja keskmise suurusega. Tegemist on teatmikuga, mis on mõeldud väike- ja keskmise suurusega ettevõtjatele (edaspidi *VKE*) abiks ELi toetuste taotlemisel, kuid see selgitab ka soovituse 2003/361/EÜ sisu ja olemust. Teatmikus on selgitatud kokkuvõtlikult (lk 7, 9, 11–15 ja 24):

- ettevõtja – määratluse kohaselt on ettevõtja „majandustegevusega tegelev mis tahes üksus olenemata selle õiguslikust vormist”. See sõnastus kajastab terminoloogiat, mida Euroopa

[32] https://op.europa.eu/et/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1/language-et

Kohus kasutab oma otsustes. Määrav tegur on majandustegevus, mitte õiguslik vorm. Praktikas tähendab see, et ettevõtjana võib käsitada füüsilisest isikust ettevõtjaid, pereettevõtjaid, ühinguid ja ühendusi või mis tahes muid üksusi, mis tegelevad korrapärase majandustegevusega. Majandustegevuse all mõistetakse tavaliselt toodete või teenuste müüki konkreetse hinna eest konkreetsel/otsesel turul;

- VKEna käsitamine – selleks et ettevõtjat saaks käsitada VKEna, peab olema täidetud töötajate arvu kriteerium. Samas võib ettevõtja ise valida, kas täidetakse käibe- või siis bilansimahu ülemmäära kriteerium. Ettevõtja ei pea täitma mõlemat kriteeriumi ning võib ületada ühe ülemmäära, ilma et see mõjutaks tema VKE staatust;
- kasutatavad andmed:
    - arvutuste tegemisel peaks kasutama viimases heakskiidetud raamatupidamise aastaaruandes sisalduvaid andmeid;
    - uus ettevõtja, kellel heakskiidetud raamatupidamise aastaaruanne veel puudub, saab kasutada deklaratsiooni, mis sisaldab majandusaasta käigus heas usus koostatud prognoosi (äriplaani kujul). Äriplaan peaks hõlmama kogu perioodi (majandusaastaid) kuni ajani, mil üksusel tekib käive *[vt teatmiku lisa artikkel 4, lk 44]*;
    - olenemata sellest, kas ettevõtja koostab konsolideeritud aastaaruande või mitte, peaksid lõpuks arvessevõetavad andmed hõlmama järgmist: selle ettevõtja, kelle VKE staatust hinnatakse, partnerettevõtjate andmed; selle ettevõtjaga, kelle VKE staatust hinnatakse, seotud ettevõtjate andmed; asjaomase ettevõtja partnerettevõtjatega seotud ettevõtjate andmed; selle ettevõtjaga, kelle VKE staatust hinnatakse, seotud ettevõtjatega seotud ettevõtjate andmed; selle ettevõtjaga, kelle VKE staatust hinnatakse, seotud ettevõtjate partnerettevõtjate andmed.
    - selleks et vältida keerulisi ja lõputuid arvutusi, sisaldab ettevõtja määratlus reeglit, et kui partnerettevõtjal on omakorda partnerettevõtjad, tuleb arvesse võtta vaid nende partnerettevõtjate andmeid, mis asuvad asjaomasest ettevõtjast tootmisahelas vahetult ees- või tagapool *[vt soovituse 2003/361/EÜ lisa artikli 6 lõike 2 kohta teatmiku lk-l 43 ning lk-l 26 esitatud näide nr 2]*;
    - kui selle ettevõtja partnerettevõtja, kelle VKE staatust hinnatakse, on seotud teise ettevõtjaga, juhul tuleb selle ettevõtja partnerettevõtja andmetesse lisada kõik seotud ettevõtjate andmed *[vt ka teatmiku lk 21–22 „Kas mul on seotud ettevõte?“); kasutada tuleks partnerettevõtte osalusega võrdelist osa andmetest (vt soovituse 2003/361/EÜ lisa artikli 6 lõige 3 teatmiku lk-l 43 ning lk-l 22 „Kuidas arvutada seotud ettevõtete andmeid?”]*;
- autonoomne ettevõtja – kui ettevõtja on kas täiesti sõltumatu või kui tal on teiste ettevõtjatega üks vähemusosalusega seotud suhe või mitu sellist suhet (igaüks neist alla 25%); *[vt täpsemalt teatmiku lk-d 16–17 „Kas mul on autonoomne ettevõte?“]*;
- partnerettevõtja – kui Teie osalus teises ettevõttes või teise ettevõtja osalus Teie ettevõttes moodustab vähemalt 25%, kuid mitte üle 50%, siis käsitatakse seda suhet partnerettevõtjate vahelise suhtena; *[vt täpsemalt teatmiku lk-d 18–20 „Kas mul on partnerettevõte?“]*; soovituse 2003/361/EÜ lisa artikli 3 lõikes 2 on sätestatud erandid, mil tegemist pole partnerettevõtjaga;
- sidusettevõtja – kui Teie osalus teises ettevõttes või teise ettevõtja osalus Teie ettevõttes ületab 50% künnise, on tegemist sidusettevõtjaga; *[vt täpsemalt teatmiku lk-d 21–22 „Kas mul on seotud ettevõte?“]*; ettevõtjaid, kes koostavad konsolideeritud aastaaruande või kelle andmed lisatakse teise ettevõtja konsolideeritud aastaaruandesse täieliku konsolideerimise teel, käsitatakse tavaliselt sidusettevõtjatena;
- kontroll – VKE määratluse puhul on oluline ka kontroll ning seda nii juriidilise kui ka tegeliku kontrolli tähenduses. Kontroll määrab kindlaks selle, kas ettevõtjat saab käsitada

partnerettevõtjana või sidusettevõtjana. Hinnata ei tule mitte pelgalt kapitali või osalust, vaid ka kontrolli, mis ühel ettevõtjal teise üle on;

- töötajate arv – see on aasta tööühikute (edaspidi *ATÜ*) arv. Töötajate arvu käsitleva kriteeriumiga on hõlmatud täistöökohaga, osalise tööajaga, ajutised ja hooajalised töötajad, sealhulgas järgmised isikud: töötajad, isikud, kes töötavad ettevõtja heaks ja kes on asjaomasesse ettevõttesse lähetatud ning keda käsitatakse liikmesriigi õiguse alusel töötajatena (nende hulka võivad olla arvatud ka ajutised töötajad), omanikud-tegevjuhid ning ettevõtja korrapärases tegevuses osalevad partnerid, kes saavad ettevõttest rahalist kasu. Töötajate hulka ei arvestata praktikante ja üliõpilasi, kes on praktika- või kutseõppelepingu alusel kutseoskusi omandamas ning rasedus- ja sünnituspuhkusel või lapsehoolduspuhkusel olevaid töötajaid. Üheks ühikuks loetakse kogu vaatlusaasta jooksul ettevõttes või selle nimel täiskohaga töötanud isikute arv; nende isikute töö, kes ei töötanud terve aasta, ning osalise tööajaga isikute ja hooajatöötajate töö võetakse arvesse ATÜ murdosadena;
- aastakäive – selle kindlaksmääramiseks leitakse tulu, mille ettevõtja sai asjaomasel aastal toodete müügist ja teenuste osutamisest oma tavapärase tegevuse tulemusel ning millest on maha arvatud kõik mahahindlused. Käive ei tohiks sisaldada käibemaksu ega muid kaudseid makse;
- aastabilansi kogumaht – näitab ettevõtja peamiste varade väärtust;
- soovituse 2003/361/EÜ lisa:
    - artikli 4 lõikega 2 tagatakse stabiilsus ja kindlustunne ettevõtjatele, kelle näitajad on ülemmäärade lähedal ja kellel on oht neid erandlikul aastal ja/või ebastabiilsel turul ületada. Seega, kui ettevõtja ületab vaatlusaastal töötajate arvuga seotud või rahalised ülemmäärad, ei mõjuta see tema olukorda ning ta säilitab VKE staatuse, mis tal oli majandusaasta alguses. Ta kaotab selle staatuse, ületades ülemmäärad kahel järjestikusel aruandeperioodil. Samas võib ettevõtja saada VKE staatuse, kui ta oli varem suurettevõtja, kuid tema näitajad langesid ülemmääradest allapoole ja jäid sinna kaheks järjestikuseks aruandeperioodiks;
    - artikli 4 lõike 2 eesmärk on tagada, et kasvavaid ettevõtjaid ei karistataks VKE staatuse kaotusega, välja arvatud juhul, kui nad ületavad asjaomaseid künniseid püsivalt. Seda eesmärki silmas pidades ei kohaldata artikli 4 lõiget 2 nende ettevõtjate suhtes, kes ületavad asjaomased VKE staatusega seotud künnised ühinemise või omandamise tulemusel omandisuhetes toimunud selliste muutuste tõttu, mida ei peeta tavaliselt ajutiseks ja mis ei tulene volatiilsusest. Ettevõtjaid, mille puhul toimub omandisuhete muutus, tuleb hinnata nende omakapitali sellise struktuuri põhjal, mis valitses tehingu toimumise hetkel, mitte viimase majandusaasta aruande koostamise hetkel. Seetõttu võidakse VKE staatus kaotada kohe.

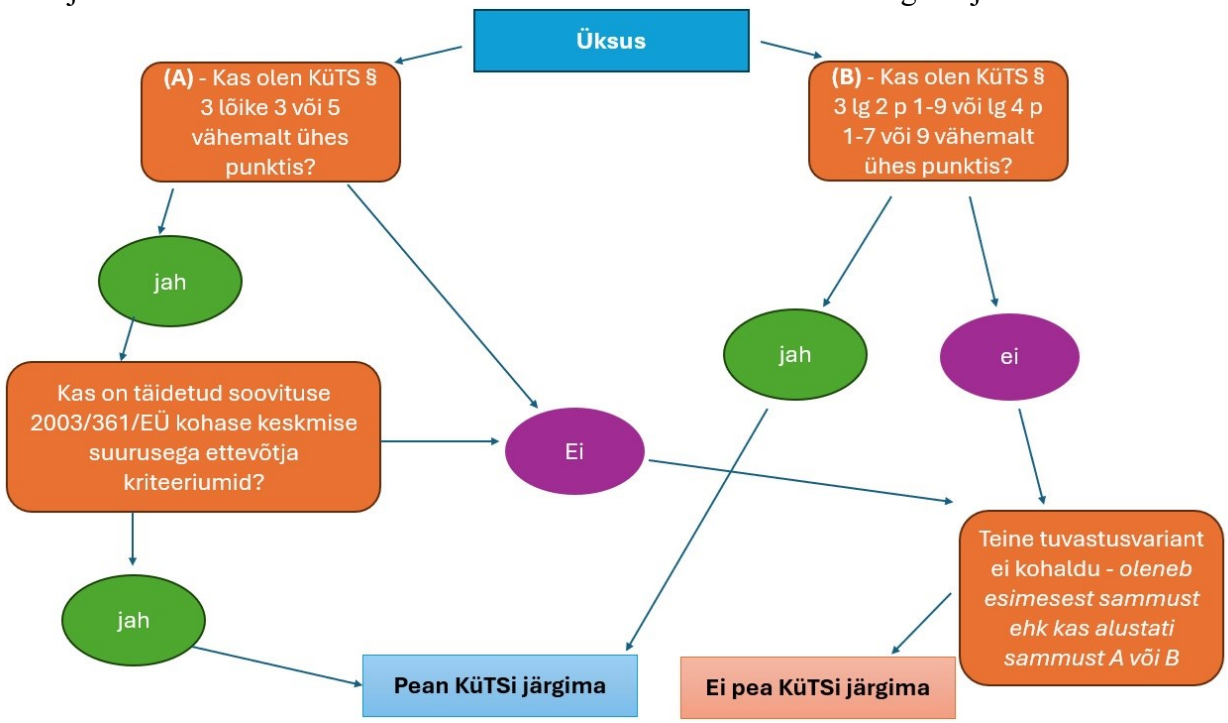
Sama teatmiku lk-del 25–31 on ka seitse näidet, milles on selgitatud ettevõtjate andmete arvutamist. Lisaks on teatmikus (lk-l 14) ka näitlik tabel 1, milles selgitatakse soovituse 2003/361/EÜ lisa artikli 4 lõike 2 loogikat (kus N on viimane heakskiidetud aruandeperiood).

Tabel 1. Soovituse 2003/361/EÜ lisa artikli 4 lõike 2 selgitus

Näite nr	N (vaatlusaasta)	N–1	N–2	VKE staatus
1	VKE	mitte-VKE	mitte-VKE	mitte-VKE
2	VKE	VKE	mitte-VKE	VKE
3	VKE	VKE	VKE	VKE
4	VKE	mitte-VKE	VKE	VKE
5	mitte-VKE	VKE	VKE	VKE
6	mitte-VKE	mitte-VKE	VKE	mitte-VKE

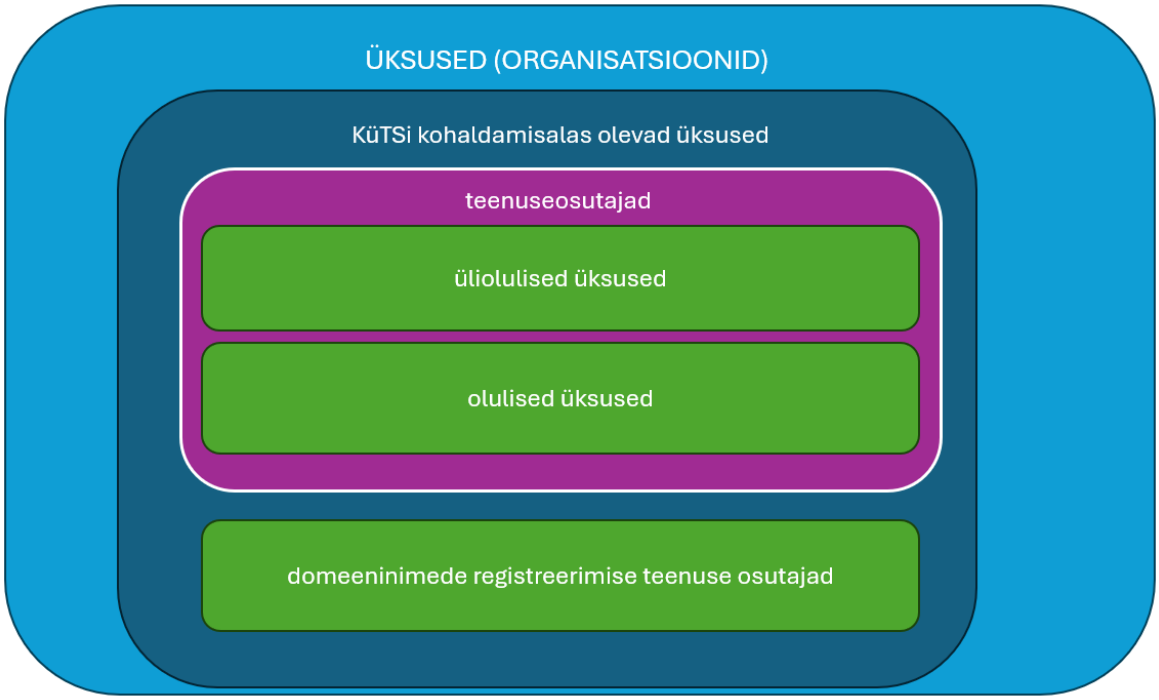
7	mitte-VKE	VKE	mitte-VKE	mitte-VKE
8	mitte-VKE	mitte-VKE	mitte-VKE	mitte-VKE

Sama teatmiku lk-del 46–56 on näidisdeklaratsioon, mida ettevõtjad saavad kasutada, et määrata kindlaks oma VKE staatus VKEde toetuskavadest abi taotlemisel. Teatmiku lk-del 49 ja 50 on esitatud selgitav märkus töötajate arvu ja finantsnäitajate määramisel arvesse võetud ettevõtjate liikide kohta ehk sisuliselt eelneva selgituse kokkuvõte.
Eraldi väärib märkimist, et eelnõukohastes KüTSi § 3 lõigetes 6 ja 7 on ette nähtud kõnealuse soovituse rakendamisel tehtavad erandid (soovituse artikli 3 lg 4 kohaldamata jätmine ning partner- ja sidusettevõtja näitajate võimalik arvestamata jätmine). Vt nende kohta täpsemaid selgitusi allpool.
Arvestades eeltoodut, on soovitatavad etapid konkreetse üksuse KüTSi kohaldamisalasse kuulumise tuvastamiseks järgmised: a) esimese sammuna (tuvastusvariant A) tuleks tuvastada, kas tegemist on mõne KüTSi § 3 lõike 3 või 5 mõnes punktis nimetatud teenuse või tegevusega: b) kui selgub, et tegemist on ühe neis lõigetes nimetatud teenuse või tegevusega, tuleb teise sammuna tuvastada, kas ettevõtja vastab soovituse 2003/361/EÜ kohase keskmise suurusega ettevõtja kriteeriumitele (st finants- ja tööjõunäitajad). Kui ettevõtja vastab neile kriteeriumitele, siis on tegemist üksusega, kes peab KüTSi järgima. Kui ettevõtja neile kriteeriumitele ei vasta, tasub kontrollida tuvastusvarianti B ehk seda, kas KüTSi nõuete järgimise kohustus võib tekkida KüTSi § 3 lõike 2 punktide 1–9 või lõike 4 punktide 1–7 või p 9 alusel. Nende punktide puhul puudub vajadus kontrollida üksuse finants- ja tööjõunäitajaid, sh ka üldkasutatava elektroonilise side võrgu teenuse osutaja ja üldkasutatava elektroonilise side teenuse osutaja (vt eelnõukohased KüTSi § 3 lg 2 p 9 ja lg 4 p 9) korral. Kui kontrollimist alustati tuvastusvariandist B, siis tuleb kontrollida ka tuvastusvarianti A. Kui mõlema tuvastusvariandi tulemus on negatiivne, siis üksus ei pea KüTSi nõudeid järgima ehk tegemist pole KüTSi kohase teenuseosutajaga.
Eelkirjeldatud KüTSi kohaldamisalasse kuuluva üksuse tuvastamist selgitab joonis nr 1.



Joonis 1. KüTSi subjektsuse tuvastamine

Eelnõu autorid rõhutavad, et eelmainitud tuvastamise kontroll ei kohaldu üksusele, kes on ainult domeeninimede registreerimise teenuse osutaja, kuna sellele üksusele kohalduvad ainult mõned KüTSi nõuded (vt ka eelnõukohase KüTS § 2 p 4 selgitusi). Samuti ei ole siinne kirjeldus mõeldud selgitamaks, kas konkreetne üksus on ülioluline üksus või oluline üksus. Seda selgitavad täpsemalt järgnevate lõigete ja punktide selgitused.
Lisaks selgitab mõistete „üksus“, „teenuseosutaja“, „ülioluline üksus“, „oluline üksus“ ja „domeeninimede registreerimise teenuse osutaja“ olemust joonis 2.



Joonis 2. Üksuse mõiste seos teiste asjaomaste mõistetega

Eelnõukohases KüTSi § 3 lõikes 1 defineeritakse teenuseosutaja mõiste. Teenuseosutajaks on KüTSi tähenduses ühiskonna toimimise seisukohast ülioluline üksus või ühiskonna toimimise seisukohast oluline üksus.
Lõike 1 eesmärk on siduda NIS2-direktiivis nimetatud liiki üksused kehtiva KüTSi sõnastusega ehk sõnaga „teenuseosutaja“. Kui KüTSis või selle alusel antud määruses on kasutatud sõna „teenuseosutaja“, siis kehtib asjaomane säte nii üliolulisele üksusele kui ka olulisele üksusele. Nende kaht liiki üksuse vaheline erinevus on ennekõike seotud nii nende suhtes kehtestatud järelevalvemeetmete ja -režiimiga (vt KüTSi 4. peatükk ja sellesse tehtavad muudatused) kui ka KüTSi nõuete rikkumiste korral nende üksuste suhtes ette nähtavate väärteokaristuste suurusega (vt KüTSi 5. peatükk ja sellesse tehtavad muudatused).
Kommenteeritava punktiga on seotud ka NIS2-direktiivi põhjendus 15:
(15) Küberturvalisuse riskijuhtimismeetmete järgimiseks ja teatamiskohustuse täitmiseks tuleks [NIS2-direktiivi] kohaldamisalasse kuuluvad üksused liigitada kahte kategooriasse – elutähtsad üksused[33] ja olulised üksused, mis näitab, mil määral on nad kriitilise tähtsusega nende sektori või osutatavate teenuste liigi, aga ka oma suuruse seisukohast. Sellega seoses tuleks igakülgselt arvesse võtta kõiki asjakohaseid valdkondlikke riskihindamisi või pädevate asutuste suuniseid, kui see on kohaldatav. Nende kahe üksuseliigi järelevalve- ja täitmise tagamise kord peaks olema erinev, et tagada õiglane tasakaal kohaldatavate riskipõhiste nõuete ja kohustuste ning nõuete

[33] Eelnõus „üliolulised üksused“.

täitmise järelevalvega seotud halduskoormuse vahel.
Domeeninimede registreerimise teenust osutava üksuse puhul tuleb arvestada asjaoluga, et NIS2-direktiiv ei määratle teda üliolulise üksuse ega olulise üksusena, mistõttu kohalduvad neile ainult teatud NIS2-direktiivi nõuded. Siin vt ka eelnõukohase KüTSi § 2 punkti 4 selgitusi.

KüTSi § 3 lõike 2 sõnastust muudetakse, kuna see sisaldab viidet NIS2-direktiiviga kehtetuks tunnistatavale direktiivile (EL) 2016/1148 ning kuna NIS2-direktiiv ei kasuta terminit „olulise teenuse operaator".
Eelnõukohase KüTSi § 3 lõike 2 eesmärk on määratleda NIS2-direktiivi artikli 3 lõike 1 kohaselt need üksused, kes on KüTSi järgi üliolulised üksused. Kooskõlastusele saadetud eelnõu versioonis kasutati termineid „elutähtis üksus" ja „elutähtsa teenuse osutaja" (defineeritud hädaolukorra seaduses), kuid neile definitsioonidele vastavaid isikuid ei saa alati samastada. Kõik elutähtsa teenuse osutajad on eelnõu varasema terminoloogia kohaselt küll automaatselt elutähtsad üksused (praeguses versioonis „üliolulised üksused"), kuid kõik üliolulised üksused ei ole automaatselt elutähtsa teenuse osutajad. Et vältida terminoloogilist segadust, on kooskõlastusringi järel loobutud KüTSis termini „elutähtis üksus" kasutamisest ja lähtutud terminist (ühiskonna toimimise seisukohalt) „üliolu̇line üksus", mis on selgemas kooskõlas ka seaduse reguleerimisalaga. Elutähtsa teenuse osutaja hädaolukorra seaduse tähenduses on aga KüTSi mõttes alati üliolu̇line üksus (vt eelnõukohane KüTSi § 3 lg 2 p 2).
Lõike 2 punktid 1–8 hõlmavad NIS2-direktiivi artikli 2 lõike 2 kohaselt selliseid KüTSi subjekte, kelle puhul ei sõltu „teenuseosutajaks" kvalifitseerumine ja seaduse kohaldamisalasse kuulumine finants- või tööjõunäitajatest. Osa kõnealuses lõikes nimetatud subjektidest on nimetatud ka NIS2-direktiivi I lisas (millele viitab ka NIS2-direktiivi artikli 2 lõige 1), kuid kuna NIS2-direktiivi artikli 2 lõige 2 sätestab, et ka need subjektid on kohustatud isikud sõltumata oma finants- või tööjõunäitajatest, siis on samadest põhimõtetest lähtutud ka eelnõus.
Lõike 2 punkt 9, mis määratleb üliolu̇liste üksustena ka elektroonilise side võrgu teenuse osutajad või üldkasutatava elektroonilise side teenuse osutajad, on eelnevatest punktidest selles mõttes erinev, et selle teenuseosutaja „üliolu̇liseks üksuseks" kvalifitseerumise küsimuse lahendamisel tuleb arvestada ka töötajate arvu ning bilansimahtu või aastakäivet.
Osaliselt on selles lõikes üliolu̇liste üksustena nimetatud sellised üksused, kes on NIS2-direktiivis otsesõnu märgitud üliolulise üksusena (nt elutähtsa teenuse osutaja). Osaliselt on aga tegemist riigisiseselt üliolu̇liste üksuste kindlaksmääramisega, arvestades NIS2-direktiivi artikli 2 lõike 2 punktides b–e sätestatud kriteeriume. Need kriteeriumid on järgmised:

> *b) üksus on liikmesriigis sellise teenuse ainuosutaja, mis on kriitilise tähtsusega ühiskondliku või majandustegevuse säilitamiseks;*
> *c) üksuse osutatava teenuse häirel võib olla oluline mõju avalikule turvalisusele, avalikule julgeolekule või rahvatervisele;*
> *d) üksuse osutatava teenuse häire võib tuua kaasa olulise süsteemse riski, eelkõige sektorites, kus sellisel häirel võib olla piiriülene mõju;*
> *e) üksus on kriitilise tähtsusega oma erilise olulisuse tõttu riiklikul või piirkondlikul tasandil konkreetse sektori või teenuseliigi või liikmesriigi muude üksteisest sõltuvate sektorite jaoks.*

Nimetatud NIS2-direktiivi punktid ei täpsusta enamal määral, milliseid üksusi on siin mõeldud, vaid siinkohal on igal liikmesriigil võimalus NIS2-direktiivi üle võtvas õigusaktis ise kindlaks määrata lisaüksused, kes vastavad kommenteeritava lõike kriteeriumitele ning kes tuleb lugeda riigisisese seaduse subjektiks. Seda on lõikes 2 nimetatud teatud subjektide üliolulisteks üksusteks määramisel ka tehtud (vt vastavaid selgitusi allpool konkreetsete punktide juures). Samas on loobutud NIS2-direktiivi artikli 2 lõike 2 eraldi ülevõtmisest, st eelnõu uues versioonis ei ole enam

kooskõlastusele saadetud eelnõus sisaldunud KüTSi § 1 lõiget 1^4, milles kavandati ette näha vastavad kriteeriumid, vaid eelnõus on juba nendest kriteeriumitest lähtudes teatavad üksused määratud üliolulisteks ja olulisteks üksusteks (nt kriitilise tähtsusega side, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja). Seeläbi välditakse olukorda, kus täidesaatval võimul tekib rakendusaktiga võimalus seaduse kohaldamisala liigselt ja subjektidele või potentsiaalsetele subjektidele ootamatult või läbipaistmatult laiendada. St uuendatud eelnõus ei ole kooskõlastusele saadetud eelnõu kohase KüTSi § 1 lõikega 1^6 kavandatud määruse kehtestamise volitusnormi.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 1 kavandatakse üle võtta NIS2-direktiivi artikli 3 lõike 1 punkt b (konkreetsemalt termin „domeeninimede süsteemi teenuse osutajad“) ja NIS2-direktiivi artikli 2 lõike 2 punkti a alapunkt iii, (konkreetsemalt selle termin „domeeninimede süsteemi teenuse osutajad“. Mõlema artikli kohaselt kuuluvad domeeninimede süsteemi teenuse osutajad NIS2-direktiivi kohaldamisalasse olenemata nende suurusest. Domeeninimede süsteem on defineeritud NIS2-direktiivi artikli 6 punktis 19, mis võetakse üle KüTSi § 2 punktiga 5 ning domeeninimede süsteemi teenuse osutaja on defineeritud NIS2-direktiivi artikli 6 punktis 20, mis võetakse üle KüTSi § 2 punktiga 6.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 2 kavandatakse üle võtta NIS2-direktiivi artikli 3 lõike 1 punkt f (elutähtsa teenuse osutaja) ning NIS2-direktiivi artikli 2 lõige 3 (*[NIS2-direktiivi] kohaldatakse [CER-direktiivi] kohaselt elutähtsa teenuse osutajatena käsitatavate üksuste suhtes olenemata nende suurusest*). Tegemist on ka kehtiva õiguse säilitamisega, kuna elutähtsa teenuse osutajad kuuluvad juba KüTSi kohaldamisalasse KüTSi kehtiva versiooni § 3 lõike 1 punkti 1 alusel. Praegu määrab elutähtsa teenuse osutaja olemuse kindlaks hädaolukorra seadus, kuid kavandatava tsiviilkriisi ja riigikaitse seaduse jõustumise järel reguleerib sellega seotud temaatikat nimetatud seadus. Hädaolukorra seaduse alusel tuvastatud elutähtsa teenuse osutaja ei pea tegutsema NIS2-direktiivi I või II lisas nimetatud sektoris selleks, et ta oleks kommenteeritava punkti alusel hõlmatud KüTSi nõuetega.
Tulevaste elutähtsa teenuste osutajate lisandumist on selgitatud CER-direktiivi üle võtvas hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõus nr 426 SE. Tsiviilkriisi ja riigikaitse seadusesse tehtavad muudatused on leitavad eelnõude infosüsteemi toimikust nr 21-0915 ning Riigikogus menetletavast tsiviilkriisi ja riigikaitse seaduse eelnõust nr 668 SE.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 3 kavandatakse üle võtta NIS2-direktiivi artikli 3 lõike 1 punkt d ja artikli 2 lõike 2 punkt f alapunkt i. Üliolulisteks üksuseks KüTSi tähenduses on keskvalitsuse avaliku halduse üksus. NIS2-direktiivi artikli 2 lõike 2 alapunkti i kohaselt on ülioluline üksus *keskvalitsuse avaliku halduse üksus, nagu see on kindlaks määratud liikmesriigi poolt kooskõlas tema õigusega*. „Keskvalitsuse avaliku halduse üksus“ on defineeritud KüTSi § 2 punktis 14, kuid see on seotud ka avaliku halduse üksuse mõistega, mis on defineeritud NIS2-direktiivi artikli 6 punktis 35 (mida eelnõuga eraldi üle ei võta). Kommenteeritava punkti puhul on tegemist ka kehtiva õiguse säilitamisega, kuna see mõiste hõlmab kehtiva KüTSi § 3 lõike 4 punktides 3, 5, 6, 7, 8, 11, 12 ja 14 nimetatud üksusi. Termini „keskvalitsuse avaliku halduse üksus“ kasutamise võimalikkust ja mõistlikkust on eelnõu koostamise käigus korduvalt kaalutud ning otsitud sobivamaid alternatiive, kuna kõnesoleva eelnõu kontekstis on tegemist NIS2-direktiivist pärit terminiga, mis on mõeldud ülevõtmiseks kõigile liikmesriikidele ja mis oma vormi ja sisu poolest seondub eelkõige föderatiivsete riikide õigusterminoloogiaga. Sellele vaatamata on kaalumise järel otsustatud hetkel parema alternatiivi puudumisel termin sellisel kujul säilitada, arvestades mh, et sarnast sõnastust („keskvalitsus“ koos seaduse puhul asjaomase täiendiga)

kasutatakse ka arvukates teistes Eesti õigusaktides – nende seas näiteks riigieelarve seaduses, riigivaraseaduses ja krediidiasutuste seaduses.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 4 kavandatakse määrata kohaliku omavalitsuse avaliku halduse üksus üliololiseks üksuseks, arvestades NIS2-direktiivi artikli 5 punkti a (*liikmesriigid võivad ette näha, et [NIS2-direktiivi] kohaldatakse kohaliku tasandi avaliku halduse üksuste suhtes*). Kommenteeritava punkti eesmärk on säilitada ka KüTSi kehtiva versiooni § 3 lõike 4 punktist 4 tulenev olukord, kus kohaliku omavalitsuse avaliku halduse üksused kuuluksid üliolulisele üksusele omase eelkontrollilaadse järelevalve alla. Vt siinjuures ka KüTSi § 2 punkti 15 kohta esitatud selgitust. Kommenteeritavas punktis määratletud mõiste on seotud ka avaliku halduse üksuse mõistega, mis on defineeritud NIS2-direktiivi artikli 6 punktis 35 (mida eelnõuga eraldi üle ei võta).
Nagu juba öeldud, on kohaliku omavalitsuse avaliku halduste üksuste üliolulise üksusena määramise eesmärk säilitada senine kord. Kui kommenteeritava NIS2-direktiivi sätte ülevõtmisel otsustataks, et see võetakse kitsamalt üle ja kehtivat õigust ei säilitataks, siis võib see kaasa tuua olukorra, kus kohalike omavalitsuste ja nende haldusala asutuste suhtes ei kohaldata ühtseid küberturvalisuse nõudeid ning see võib kaasa tuua tõrkeid ja probleeme nende osutatavate avalike teenuste osutamisel või nende võrgu- ja infosüsteemide puhul, sh ka nende üksuste valduses olevatele (isiku)andmete turvalisusega seoses. Eelnõuga on soovitud sellist tulemust vältida.
Kommenteeritavas punktis sätestatud üksus lisatakse KüTSi kohaldamisalasse üliolulise üksusena, arvestades NIS2-direktiivi artikli 2 lõike 2 punktides b, c ja e nimetatud kriteeriume.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 5 kavandatakse määrata kriitilise tähtsusega side, mereraadioside ja operatiivraadiosidevõrgu teenuse osutaja üliololiseks üksuseks, arvestades NIS2-direktiivi artikli 3 lõike 1 punkti g (*kui liikmesriigid nii ette näevad, siis üksused, mida liikmesriigid käsitasid enne 16. jaanuari 2023 oluliste teenuste operaatoritena vastavalt [...] liikmesriigi õigusele*). Sellised üksused kuuluvad kehtiva KüTSi kohaldamisalasse, mistõttu on kõnealuse punkti sätestamise eesmärk seotud kehtiva KüTSi § 3 lõike 1 punkti 9 säilitamisega. Eestis tegeleb kriitilise tähtsusega side, mereraadioside ja operatiivraadiosidevõrgu teenuse pakkumisega Riigi Infokommunikatsiooni Sihtasutus. Kõnealune üksus lisatakse KüTSi kohaldamisalasse üliolulise üksusena, arvestades ka NIS2-direktiivi artikli 2 lõike 2 punktides b, c, d ja e sätestatud kriteeriume.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 6 võetakse üle NIS2-direktiivi artikli 3 lõike 1 punkt b, konkreetsemalt termin „kvalifitseeritud usaldusteenuse osutajad“, hõlmates nad üliolulise üksuse mõiste alla. NIS2-direktiivi artikli 2 lõike 2 punkti a alapunkti ii kohaselt kuuluvad usaldusteenuse osutajad NIS2-direktiivi kohaldamisalasse olenemata nende suurusest. Usaldusteenuse osutaja mõiste hõlmab ka kvalifitseeritud usaldusteenuse osutajat (vt NIS2-direktiivi artikli 6 punkti 27 ja seda üle võtvat KüTSi § 2 punkti 16). Usaldusteenuse osutajatele on viidatud ka NIS2-direktiivi I lisas (vt I lisa p 8 seitsmes taane) .
Usaldusteenuse osutajatega on seotud ka NIS2-direktiivi põhjendus:
(11) Mõned üksused tegutsevad riikliku julgeoleku, avaliku julgeoleku, kaitse või õiguskaitse valdkonnas, sealhulgas kuritegude ennetamine, uurimine, avastamine ja nende eest vastutusele võtmine, osutades samal ajal ka usaldusteenuseid. Usaldusteenuse osutajad, kes kuuluvad Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 kohaldamisalasse, peaksid kuuluma [NIS2-direktiivi] kohaldamisalasse, et tagada turvanõuded ja järelevalve samal tasemel, mis oli juba eelnevalt nimetatud määruses sätestatud seoses usaldusteenuse osutajatega. Nii nagu määrust (EL) nr 910/2014 ei kohaldata teatavate konkreetsete teenuste suhtes, ei tuleks ka [NIS2-direktiivi]

kohaldada selliste usaldusteenuste osutamise suhtes, mida kasutatakse eranditult suletud süsteemides, mis tulenevad liikmesriigi õigusest või kindlaksmääratud osalejate vahelistest kokkulepetest.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 7 kavandatakse määrata riigi tegevusvaru haldaja ülioluliseks üksuseks, arvestades NIS2-direktiivi artikli 3 lõike 1 punkti e.
Kõnealune punkt on seotud ka NIS2-direktiivi I lisa punkti 1 alapunkti c kolmanda taandega (*Euroopa Liidu Nõukogu direktiivi 2009/119/EÜ, millega kohustatakse liikmesriike säilitama toornafta ja/või naftatoodete miinimumvarusid (edaspidi* direktiiv 2009/119/EÜ*), artikli 2 punktis f määratletud varude säilitamise kesküksused*). Direktiivi 2009/119/EÜ artikli 2 punktis f on varude säilitamise kesküksuseks (CSE) *asutus või talitus, kellele võib anda volitused tegutseda naftavarude, sealhulgas kriisivarude ja erivarude soetamiseks, säilitamiseks või müümiseks*. Vedelkütusevaru seaduse §-s 4 on sätestatud: varu „moodustab ja seda haldab hädaolukorra seaduse § 18^1 lõikes 1 sätestatud äriühing". Viidatud hädaolukorra seaduses lõikes on sätestatud: „Riigi tegevusvaru (edaspidi varu) moodustab, seda haldab ja selle kasutusele võtmise korraldab riigi äriühing, kelle põhikirjalise tegevuse eesmärk on varu moodustamine ja haldamine (edaspidi varu haldaja)". Sellest lähtudes on kommenteeritavas punktis kasutatud terminit „riigi tegevusvaru haldaja".
Kommenteeritavas punktis nimetatud üksus loetakse KüTSi ülioluliseks üksuseks, arvestades ka NIS2-direktiivi artikli 2 lõike 2 punktides b, c, d ja e nimetatud kriteeriume.

Eelnõukohase KüTSi § 3 lg 2 punktiga 8 kavandatakse üle võtta NIS2-direktiivi artikli 3 lõike 1 punkt b, konkreetsemalt termin „tippdomeeninimede registrid". NIS2-direktiivi artikli 2 lõike 2 punkti a alapunkti iii kohaselt kuuluvad tippdomeeninimede registrite pidajad NIS2-direktiivi kohaldamisalasse olenemata nende suurusest.
Kõnealuse punktiga võetakse samuti üle NIS2-direktiivi artikli 2 lõike 2 punkt a alapunkt iii (*tippdomeeninimede registrid ja domeeninimede süsteemi teenuse osutajad*) ja samal ajal ka NIS2-direktiivi lisa I punkti 8 kolmas taane (*tippdomeeninimede registrite pidajad*). Selle üksusega on ka seotud NIS2-direktiivi põhjendus 32:
(32) Usaldusväärse, vastupidava ja turvalise domeeninimede süsteemi (DNS) tagamine ja hoidmine on võtmetähtsusega, et säilitada interneti usaldusväärsus ning oluline, et tagada selle pidev ja stabiilne toimimine, millest sõltuvad digimajandus ja -ühiskond. Seepärast tuleks [NIS2-direktiivi] kohaldada tippdomeeninimede registrite ja domeeninimede süsteemi teenuse osutajate suhtes, mida tuleb käsitada üksustena, mis osutavad interneti lõppkasutajatele mõeldud üldkasutatavate domeeninimede rekursiivse teisendamise teenust või kolmandatele isikutele kasutamiseks mõeldud domeeninimede autoriteetse teisendamise teenust. [NIS2-direktiivi] ei tuleks kohaldada juurnimeserverite suhtes.
Tegemist on kehtiva õiguse säilitamisega ehk kehtiva KüTSi § 3 lõike 1 punkti 8 (*Eesti maatunnusega seotud tipptaseme domeeninimede registri haldaja*) säilitamisega teises sõnastuses. Tippdomeeninimede register on defineeritud NIS2-direktiivi artikli 6 punktis 21, mis kavandatakse üle võtta eelnõukohase KüTSi § 2 punktiga 28. Kommenteeritava punkti puhul ei ole võimalik säilitada kehtiva KüTSi asjakohase punkti lauseosa „registri pidamiseks kasutatava süsteemi ja tipptaseme nimeserveri teenuse osutamisel", kuna NIS2-direktiiv näeb ette, et sellised üksused saavad tervikuna KüTSi subjektiks.
Eelnõu kooskõlastamise käigus märkis Eesti Interneti Sihtasutus, et ta on käsitatav tippdomeeninimede registri pidajana, kuid sihtasutus teostab järelevalvet kokku 51 akrediteeritud domeeni .ee registripidaja teenuse osutamise suhtes, 24 neist tegutsevad Eestis ja 27 välismaal.

Eelnõukohase KüTSi § 3 lõike 2 punktiga 9 kavandatakse üle võtta NIS2-direktiivi artikli 3 lõike 1 punkt c. Kommenteeritava punkti kohaselt lisatakse KüTSi kohaldamisalasse üksus, kes vastab kõigile järgmistele tingimustele (arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ):
1) ta on üldkasutatava elektroonilise side võrgu teenuse osutaja või üldkasutatava elektroonilise side teenuse osutaja;
2) tal on majandusaasta jooksul 50 või rohkem töötajat;
3) tema aastane bilansimaht või aastakäive ületab 10 miljonit eurot (sh kas aastane bilansimaht või aastakäive on sellest summast suurem).
Kõnealuse punktiga on seotud NIS2-direktiivi artikli 2 lõike 2 punkt a alapunkt i (*üldkasutatavate elektroonilise side võrkude pakkujad või üldkasutatavate elektroonilise side teenuste osutajad*) ja samal ajal ka NIS2-direktiivi I lisa punkti 8 kaheksas taane (*üldkasutatavate elektroonilise side võrkude pakkujad*). Üldkasutatava elektroonilise side võrk on defineeritud NIS2-direktiivi artikli 6 punktis 36, mis kavandatakse üle võtta eelnõukohase KüTSi § 2 punktiga 38.
Kommenteeritava punktiga seoses vt ka eespoolset selgitust Euroopa Komisjoni soovituse 2003/361/EÜ rakendamise kohta.

Eelnõukohase KüTSi § 3 lõikega 3 kavandatakse üle võtta NIS2-direktiivi artikli 3 lõike 1 punkt a. Selle punkti alusel on üliolulise üksusega tegemist siis, kui on täidetud kõik järgmised tingimused, st tegemist on üksusega (arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ):
1) kellel on majandusaasta jooksul 250 või rohkem töötajat;
2) kelle aastane bilansimaht ületab 43 miljonit eurot või aastakäive ületab 50 miljonit eurot (sh kas aastane bilansimaht või aastakäive on nimetatud summadest suurem);
3) kes on nimetatud KüTSi § 3 lõike 3 punktides 1–41 ehk tegemist on vähemalt ühe selles lõikes viidatud 41 punktis nimetatud üksusega.
NIS2-direktiivi artikli 3 lõike 1 punkt a on kavandatud üle võtta kommenteeritavas sättes esitatud kujul selleks, et esitada ühes kohas ja ühel korral loetelu üliolulistest üksustest, kes kuuluvad selle määratluse alla, kuna nad on nimetatud NIS2-direktiivi I lisas. Mitu liikmesriiki on NIS2-direktiivi lisades sätestatud teenuseosutajate loetelud üle võtnud neile viidates või liikmesriigi muutmise seadustele lisatud lisade abil (nagu direktiivis), kuid Eesti õigusloomereeglistik sellist lähenemisviisi ei võimalda.
Kommenteeritava lõikega seoses vt ka eespoolset selgitust Euroopa Komisjoni soovituse 2003/361/EÜ rakendamise kohta.

Eelnõukohane KüTSi § 3 lõike 3 punkt 1 sätestab üliolulise üksusena andmekeskusteenuse osutaja, eeldusel et üksus vastab kõnesoleva lõike sissejuhatavas osas märgitud piirmääradele. Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 8 viies taane (*andmekeskusteenuse osutajad*). Andmekeskusteenus on defineeritud eelnõukohases KüTSi § 2 punktis 1 (vt eespool).

Eelnõukohane KüTSi § 3 lõike 3 punkt 2 sätestab üliolulise üksusena elektriettevõtja elektrituruseaduse tähenduses, kes tegeleb elektrienergia müügiga, kaasa arvatud selle edasimüügiga elektrienergia hulgimüüjale või lõpptarbijale, eeldusel et üksus vastab kõnesoleva lõike sissejuhatavas osas märgitud piirmääradele.
Kommenteeritava punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti a esimene taane (*Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/944 elektrienergia siseturu ühiste normide kohta ja millega muudetakse direktiivi 2012/27/EL* (edaspidi direktiiv (EL) 2019/944) *artikli 2 punktis 57 määratletud elektriettevõtjad, kes täidavad nimetatud direktiivi*

artikli 2 punktis 12 määratletud tarnimise ülesannet). Mainitud direktiivi kohaselt on elektriettevõtja „füüsiline või juriidiline isik, kes täidab vähemalt üht järgmistest ülesannetest: elektrienergia tootmine, ülekandmine, jaotamine, agregeerimine, tarbimiskaja, energia salvestamine, tarnimine või ostmine, ning kes vastutab nende ülesannetega seotud kaubanduslike, tehniliste või hoolduskusimuste eest; käesolev mõiste ei hõlma lõpptarbijaid“. Lõpptarbija on sama direktiivi kohaselt tarbija, kes ostab elektrienergiat oma tarbeks; st lõpptarbija ei müü elektrienergiat (hulgi) edasi. Eeldatavasti on lõpptarbija ka isik, kes toodab elektrienergiat näiteks päikesepaneeliga ning kasutab sellest saadud elektrienergiat enda vajaduste jaoks.
Direktiiv (EL) 2019/944 on üle võetud Eesti õigusesse elektrituruseaduse ja teiste seaduste muutmise seadusega (eelnõu nr 426 SE).[34] Nimetatud seaduse eelnõu seletuskirja lisas 1 esitatud vastavustabeli (edaspidi *426 SE vastavustabel*) kohaselt on direktiivis (EL) 2019/944 kasutatud termini vasteks elektrituruseaduse § 6 lõike 1 kohane elektriettevõtja, kes on „füüsiline või juriidiline isik, kes ei ole tarbija ja kes tegeleb: tootmisega, ülekandmisega, jaotamisega, agregeerimisega, tarbimise juhtimisega, salvestamisega, müümisega või, ostmisega“. NIS2-direktiiv on kitsendanud elektriettevõtja mõistet nii, et see ettevõtja tegeleb „tarnimisega“ ning samal ajal ei tohi ta olla „lõpptarbija“.
Siinse punktiga seonduvalt on asjakohased ka direktiivi (EL) 2019/944 artikli 2 punktid 1–3 ja 12:
1) „tarbija“ – elektrienergia hulgimüüja või lõpptarbija;
2) „hulgimüüja“ – füüsiline või juriidiline isik, kes ostab elektrienergiat edasimüümiseks võrgus, kuhu ta kuulub, või väljaspool seda;
3) „lõpptarbija“ – tarbija, kes ostab elektrienergiat oma tarbeks;
12) „tarnimine“ – elektrienergia müük, kaasa arvatud edasimüük tarbijatele.
Kui võrrelda direktiivi (EL) 2019/944 artikli 2 punktis 57 määratletud tegevusi (sh terminit *tarnimine*), siis elektrituruseaduse § 6 lõikes 1 on sõna „tarnimise“ asemel sobivam sõna „müümine“. Seetõttu on eelnõu sõnastuse järgi tegemist elektrienergia müümisega. Direktiivi (EL) 2019/944 artikli 2 punktide 1–3 ja 12 tõttu on mõiste selgituses ka lauseosa „kaasa arvatud selle edasimüügiga elektrienergia hulgimüüjale või lõpptarbijale“.

Eelnõukohane KüTSi § 3 lõike 3 punkt 3 sätestab üliolulise üksusena elektriettevõtja elektrituruseaduse tähenduses, kes tegeleb elektrienergia tootmisega, eeldusel et üksus vastab kõnesoleva lõike sissejuhatavas osas märgitud piirmääradele.
Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti a neljas taane (*direktiivi (EL) 2019/944 artikli 2 punktis 38 määratletud tootjad*). Mainitud direktiivi kohaselt on tootja „elektrienergiat tootev füüsiline või juriidiline isik“. 426 SE vastavustabeli kohaselt on direktiivi (EL) 2019/944 termini vasteks elektrituruseaduse § 7 lõike 1 kohane tootja, kes on „elektriettevõtja, kes toodab elektrienergiat ühe või mitme tootmisseadme abil“.

Eelnõukohane KüTSi § 3 lõike 3 punkt 4 sätestab üliolulise üksusena ettevõtja, kes tegeleb nõukogu direktiivi 91/271/EMÜ asulareovee puhastamise kohta (EÜT L 135, 30.05.1991, lk 40–52) (edaspidi *direktiiv 91/271/EMÜ*) artikli 2 punktides 1, 2 ja 3 määratletud asulareovee, olmereovee või tööstusreovee kogumise, ärajuhtimise või puhastamisega, välja arvatud ettevõtja, kelle puhul on asulareovee, olmereovee või tööstusreovee kogumine, ärajuhtimine või puhastamine tema üldise tegevuse väheoluline osa. Selline ettevõtja on üliolulise üksus eeldusel, et ta vastab käesoleva lõike sissejuhatavas osas märgitud piirmääradele.
Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 7 esimene taane. Direktiivi 91/271/EMÜ artikli 2 punktides 1, 2 ja 3 on asulareovesi, olmereovesi ja tööstusreovesi

[34] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/40352cd6-cbef-409f-ae11-c3af8ae0c613/elektrituruseaduse-ja-teiste-seaduste-muutmise-seadus/

defineeritud kui:
„1. asulareovesi – olmereovesi või olme- ja tööstusreovee ja/või mahasadanud vihmavee segu;
2. olmereovesi – asulate ja nendega seotud rajatiste reovesi, mis pärineb peamiselt inimeste ainevahetusest ja majapidamistegevusest;
3. tööstusreovesi – igasugune reovesi, mis väljub mis tahes kaubandusliku või tööstusliku tegevuse sooritamiseks kasutatavast hoonest ja mis ei ole ei olmereovesi ega mahasadanud vihmavesi“.
Reovee ärajuhtimist ühiskanalisatsiooni kaudu ja selle puhastamist reguleerib ühisveevärgi ja -kanalisatsiooni seadus, kuid selles ei ole eraldi defineeritud asulareovett, olmereovett ega tööstusreovett. Seetõttu on kommenteeritavas punktis viidatud direktiivi 91/271/EMÜ vastavatele sätetele.
NIS2-direktiiv ei anna selgust, mida tuleks silmas pidada „väheolulise osa“ all tegevusest, mistõttu seda lauseosa ei ole võimalik täiendavalt selgitada Direktiivi abstraktne sõnastus paneb aga seda üle võtvad liikmesriigid keerulisse olukorda – ühest küljest peab olema piisavalt selge, millised üksused kuuluvad NIS2-direktiivis (ja seaduses) esitatud määratluste alla ja seega selle kohaldamisalasse ja millised mitte. Teisest küljest oleks „väheolulise osa” kindlaksmääramine näiteks kindla protsentväärtusena meelevaldne ja riskantne, kuna sellega eksitaks NIS2-direktiivi kandva põhimõtte vastu, milleks on ühtlustada siseturuüleselt küberturvalisuse nõuded. Kindlate lävendite seaduses sätestamisel oleks aga (ning seda on juba ülevõtmisviiside võrdluses kohati näha) vastupidine tulemus ning tooks kaasa praktiliselt kindlasti realiseeruva sisulise rikkumismenetluse ohu. Sellest tulenevalt on eelnõu autorid, arvestades mh mitme teise liikmesriigi valitud lähenemisviisiga, otsustanud i) esitada Euroopa Komisjonile päringu kõnealuses küsimuses liikmesriikidele selgete suuniste andmiseks ja ii) seni, vastavate suuniste puudumisel, võtta kõnealune kriteerium üle täpselt ja ühetaoliselt NIS2-direktiivis toodud kujul ning möönda, et vajaduse korral ehk vähetõenäolistes vaidlusalustes olukordades tuleb see sisustada praktikas ja juhtumipõhiselt, arvestades iga kord asjaolude ja vaidlusaluse juhtumi objektiivsete tunnustega. Võrdluseks võib mainida, et sarnast lahendust on kasutatud ka teiste riikide NIS2-direktiivi ülevõtmiseks koostatud eelnõudes. Näiteks on see niiviisi kavandatud Eesti õiguskorra kujundamisel oluliseks eeskujuks olnud Saksa Liitvabariigi vastavas seaduseelnõus (kõnealuse eelnõu koostamise ajal ei ole Saksamaal veel eelnõu seadusena vastu võetud)[35] ning Belgia kuningriigi vastavas seaduses[36].

Eelnõukohase KüTSi § 3 lõike 3 punktiga 5 kavandatakse ette näha, et ülioluline üksus on Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 laevade ja sadamarajatiste turvalisuse tugevdamise kohta (ELT L 129, 29.04.2004, lk 6–91) I lisas meretranspordi puhul osutatud ettevõtja, kes tegeleb reisijate ja kauba vedamisega sisevetes, merel ja rannavetes, välja arvatud kõnealuse ettevõtja käitatavad üksikud laevad. Nagu ka kõigi teiste nimetatud lõike punktide puhul, on ka kõnesolevas punktis üliolulise üksusega tegemist juhul, kui üksus vastab nimetatud lõike sissejuhatavas osas märgitud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 2 alapunkti c esimene taane (*Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004, laevade ja sadamarajatiste turvalisuse tugevdamise kohta (edaspidi* määrus (EÜ) nr 725/2004*), I lisas meretranspordi puhul*

[35] Gesetzentwurf - der Bundesregierung. Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), kättesaadav: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html.

[36] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:72022L2555BEL_202402242 ja https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:72022L2555BEL_202402753

määratletud reisijate ja kauba vedamisega sisevetes, merel ja rannavetes tegelevad ettevõtjad, välja arvatud kõnealuste ettevõtjate käidatud üksikud laevad). Kommenteeritava punkti sõnastus on sama mis NIS2-direktiivi I lisas. Fraas „välja arvatud kõnealuse ettevõtja käidatud üksikud laevad“ tähendab, et kohaldamisalasse ei kuulu konkreetsed laevad ehk laevas olevad (ehk kasutatavad) võrgu- ja infosüsteemid.

Eelnõukohase KüTSi § 3 lõike 3 punktiga 6 kavandatakse ette näha, et ülioluline üksus on Euroopa Parlamendi ja nõukogu määruse (EL) 2022/123, mis käsitleb Euroopa Ravimiameti suuremat rolli ravimite ja meditsiiniseadmete alases kriisivalmiduses ja -ohjes (ELT L 20, 31.01.2022, lk 1–37), artiklis 22 nimetatud rahvatervise hädaolukorras esmatähtsa meditsiiniseadme tootja. Selline üksus on ülioluline üksus, kui ta vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 5 viies taane (*üksused, mis toodavad rahvatervise hädaolukorras kriitilise tähtsusega meditsiiniseadmeid (rahvatervise hädaolukorra esmatähtsate meditsiiniseadmete loetelu) Euroopa Parlamendi ja nõukogu määruse (EL) 2022/123, mis käsitleb Euroopa Ravimiameti suuremat rolli ravimite ja meditsiiniseadmete alases kriisivalmiduses ja -ohjes (edaspidi* määrus (EL) 2022/123*), artikli 22 tähenduses*). Määruse (EL) 2022/123 artikli 22 lõike 1 kohaselt, kohe pärast rahvatervise hädaolukorra olemasolu tunnistamist, konsulteerib meditsiiniseadmete nappuse juhtrühm sama määruse artikli 21 lõikes 5 osutatud juhtrühmaga; kohe pärast kõnealust konsulteerimist võtab meditsiiniseadmete nappuse juhtrühm vastu selliste meditsiiniseadmete kategooriate loetelu, mida ta peab rahvatervise hädaolukorras esmatähtsaks. Sama määruse artikli 22 lõike 3 kohaselt avaldab Euroopa Ravimiamet oma spetsiaalsel veebilehel järgmise teabe: *a) rahvatervise hädaolukorras esmatähtsate seadmete loetelu ja selle ajakohastatud versioonid ning b) teave rahvatervise hädaolukorras esmatähtsate seadmete loetellu kantud esmatähtsate meditsiiniseadmete tegeliku nappuse kohta.*
Euroopa Ravimiametis on selle teema jaoks loodud eraldi töörühm, millega seotud info leiab siit: https://www.ema.europa.eu/en/about-us/what-we-do/crisis-preparedness-management/executive-steering-group-shortages-medical-devices.
Määruse (EL) 2022/123 artikkel 2 punkt e defineerib „meditsiiniseadme“, viidates kahele Euroopa Liidu õigusaktile (vt täpsemalt KüTSi § 3 lõike 5 punkti 4 selgitus). Kui kõnesolevas punktis selgitatud meditsiiniseade on nimetatud eelmainitud rahvatervise hädaolukorras esmatähtsate seadmete loetelus, siis on nende seadmete tootja käsitatav elutähtsa üksusena NIS2-direktiivi tähenduses (eelnõus üliolulise üksusena KüTSi tähenduses) – kuid seda seni, kuni kõnealune meditsiiniseade on loetletud rahvatervise hädaolukorras esmatähtsate seadmete loetelus.
2024. aastal Riigikogus vastu võetud meditsiiniseadme seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (pädevuse andmine Ravimiametile) eelnõu nr 448 SE[37] seletuskirja (lk 2) peatükis 2 on märgitud:
„Meditsiiniseadmed on väga varieeruv ja suur rühm tooteid, mille kasutamine on igapäevane tervishoiuteenuse osutamisega tegelevates asutustes, kuid ka väga paljudes kodudes. Meditsiiniseadmed on näiteks plaastrid, termomeetrid ja kiirtestid, aga ka keerukad süsteemid, mida kasutatakse tervishoiuasutustes. Samuti on meditsiiniseadmetena määratletavad mõned tarkvarad, mida kasutatakse tervishoius ja meditsiinilistest toimingutes. Hinnanguliselt on meditsiiniseadmete andmekogu alusel Eestis ligikaudu 200 meditsiiniseadmete tootjat ja ligikaudu 650 levitajat. See arv on tegelikkuses suurem, kuna levitamisest teavitamise kohustus ei laiene kõige madalama riskitasemega seadmetele, samuti ei täida kahjuks kõik ettevõtjad oma seadusest

[37] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/7bc329c3-f351-44bb-aed6-30c8dadc5759/meditsiiniseadme-seaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus-padevuse-andmine-ravimiametile/

tulenevalt levitamisest teavitamise kohustust ja Eestis on väike hulk ettevõtjaid, kes tegutsevad volitatud esindaja või importijana.“
Esialgsel hinnangul kommenteeritavale punktile vastavaid üksusi hetkel pole. Kui meditsiiniseadmete nappuse juhtrühm võtab vastu selliste meditsiiniseadmete kategooriate loetelu, mida peetakse rahvatervise hädaolukorras esmatähtsaks ning loetelus toodud meditsiiniseadet toodetakse Eestis, siis saab vastavast meditsiiniseadet tootvast üksusest ka ülioluline üksus.

Eelnõukohane KüTSi § 3 lõike 3 punkt 7 sätestab üliolulise üksusena Euroopa Liidu majanduse tegevusalade statistilise klassifikaatori NACE Revision 2 C jao osas 21 osutatud põhifarmaatsiatoote ja ravimpreparaadi tootja. Selline üksus on ülioluline üksus, kui ta vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Kommenteeritava punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 5 neljas taane (*NACE Rev. 2 C jao osas 21 osutatud põhifarmaatsiatooteid ja ravimpreparaate tootvad üksused*). Üldjuhul ei viidata Eesti õigusaktides ELi klassifikaatorile NACE, vaid viidatakse EMTAK 2008 klassifikaatorile, kuid eelnõus ei ole võimalik EMTAKi klassifikaatorit kasutada, kuna see ei ühti üksüheselt NACE Revision 2 klassifikaatoriga. NACE Revision 2 jao C osa 21 sisu ei ole sama mis EMTAKi C jao 21. osa (EMTAKis on hõlmatud ka „provitamiinid“, „hormoonid“, „glükosiidid, taimsed alkaloidid ning nende derivaadid“, „lüsiin, selle estrid ja nende soolad, glutamiinhape ja selle soolad“, „luutaastustsementide tootmine“, „haavaplaastrite tootmine“ ning „kõrvaküünalde tootmine“). Kui kommenteeritavas punktis kasutada viidet EMTAK 2008 klassifikaatorile, siis seeläbi laiendataks NIS2-direktiivi kohaldamisala, kuid eelnõu eesmärk on võtta NIS2-direktiiv kitsalt üle. Seetõttu on kommenteeritavas punktis viidatud ELi NACE 2 klassifikaatorile.
Näiteks on kommenteeritava punktiga hõlmatud need üksused, kes toodavad põhifarmaatsiatooteid, mis muu hulgas hõlmab ka vere töötlemist. Vt selle kohta Euroopa Parlamendi ja nõukogu määruse (EL) 2024/1938, milles käsitletakse inimkasutuseks ettenähtud inimpäritolu materjali kvaliteedi- ja ohutusstandardeid ning millega tunnistatakse kehtetuks direktiiv 2002/98/EÜ ja direktiiv 2004/23/EÜ, põhjendus 15 ja artikli 2 lõike 1 punkt c.
Samuti on kommenteeritava üksusega hõlmatud apteegid, mis toodavad farmaatsiatooteid ja ravimpreparaate, kuna kommenteeritava punkti kohaldamisalasse kuuluvad põhifarmaatsiatoote ja ravimpreparaatide tootmisega tegelevad üksused.
1. jaanuaril 2025 hakkas kehtima EMTAK 2025, mis asendab EMTAK 2008 klassifikaatori, ning selle koostamisel on lähtutud NACE Revision 2.1 klassifikaatorist.[38] Kõige uuem klassifikaator on NACE Revision 2.1 ja kui viidata eelnõu kommenteeritavas punktis sellele klassifikaatorile või EMTAK 2025 klassifikaatorile, arvestades asjaolu, et mõlemad klassifikaatorid on eeldatavasti ulatuslikumad kui NACE Revision 2, siis võetaks asjakohane NIS2-direktiivi säte üle laiemalt. See on küll eeldus, kuna eelnõu koostamise käigus ei olnud võimalik nende versioonide erinevust täpsemalt üle kontrollida, kuid see eeldus lähtub eelmises lõigus osutatud erinevuste tuvastamisest NACE Revision 2 ja EMTAK 2008 vahel. Seetõttu ei ole eelnõus ka viidatud EMTAK 2025-le.

Eelnõukohane KüTSi § 3 lõike 3 punkt 8 sätestab üliolulise üksusena gaasiettevõtja maagaasi seaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega võetakse üle NIS2-direktiivi I lisa punkti 1 alapunkti d kuues taane (*direktiivi 2009/73/EÜ artikli 2 punktis 1 määratletud maagaasiettevõtjad*). Euroopa Parlamendi ja nõukogu direktiivi 2009/73/EÜ, mis käsitleb maagaasi siseturu ühiseeskirju ning millega tunnistatakse kehtetuks

[38] https://abiinfo.rik.ee/emtak/emtak2025

direktiiv 2003/55/EÜ (edaspidi *direktiiv 2009/73/EÜ*) artikli 2 punkti 1 kohaselt on maagaasiettevõtja „füüsiline või juriidiline isik, kelle vähemalt üks ülesanne on maagaasi, sealhulgas veeldatud maagaasi tootmine, ülekandmine, jaotamine, tarnimine, ostmine või hoiustamine, ning kes vastutab nende ülesannetega seotud kaubanduslike, tehniliste ja/või hoolduskü simuste eest, välja arvatud lõpptarbijaid“. Direktiiv 2009/73/EÜ tunnistati 3. augustil 2024 kehtetuks Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2024/1788, mis käsitleb taastuvatest energiaallikatest toodetud gaasi, maagaasi ja vesiniku siseturgude ühiseid norme ning millega muudetakse direktiivi (EL) 2023/1791 ja tunnistatakse kehtetuks direktiiv 2009/73/EÜ (edaspidi *direktiiv (EL) 2024/1788*). Direktiivi (EL) 2024/1788 artiklit 95 arvestades ning lähtudes selle direktiivi IV lisas esitatud direktiivi 2009/73/EÜ ja direktiivi (EL) 2024/1788 vastavustabelist, on direktiivi 2009/73/EÜ artikli 2 punkti 1 vasteks direktiivi (EL) 2024/1788 artikli 2 punkt 15. Direktiivi (EL) 2024/1788 artikli 2 punkt 15 on sõnastatud järgmiselt: „füüsiline või juriidiline isik, kes tegeleb maagaasi, sealhulgas veeldatud maagaasi tootmise, ülekandmise, jaotamise, tarnimise, ostmise või hoiustamisega ning kes vastutab nende ülesannetega seotud kaubanduslike, tehniliste või hoolduskü simuste eest, välja arvatud lõpptarbijad“.
Maagaasiseaduse §-s 4 on gaasiettevõtja defineeritud kui „ettevõtja, kes tegutseb vähemalt ühel tegevusalal, milleks on gaasi tootmine, import, ülekanne, jaotamine, hoiustamine või müük, ning kes vastutab selle tegevusega seonduva kaubandusliku või hoolduskü simuse lahendamise eest“. Seetõttu on kommenteeritavas punktis viidatud gaasiettevõtjale maagaasiseaduse tähenduses.

Eelnõukohane KüTSi § 3 lõike 3 punkt 9 sätestab üliolulise üksusena haldusteenuse osutaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 9 esimene taane (*hallatud teenuse osutajad*). Haldusteenuse osutaja on defineeritud NIS2-direktiivi artikli 6 punktis 39, mis võetakse üle KüTSi § 2 punktiga 7. Eelnõu varasemas versioonis on kasutatud selle asemel terminit „hallatud teenuse osutaja”. See termin asendati eelnõu kooskõlastamisel saadud tagasiside põhjal. Tegemist on IKT-ga seotud haldusteenustega.

Eelnõukohane KüTSi § 3 lõike 3 punkt 10 sätestab üliolulise üksusena hoidlatevõrgu halduri maagaasiseaduse tähenduses. Selline üksus on ülioluline üksus, kui ta vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga võetakse üle NIS2-direktiivi I lisa punkti 1 alapunkti d neljas taane (*direktiivi 2009/73/EÜ artikli 2 punktis 10 määratletud hoidlatevõrgu haldurid*). Direktiivi 2009/73/EÜ artikli 2 punkti 10 kohaselt on hoidlatevõrgu haldur „füüsiline või juriidiline isik, kes täidab gaasi hoiustamise ülesannet ja vastutab gaasihoidla kasutamise eest“. Direktiiv 2009/73/EÜ tunnistati 3. augustil 2024 kehtetuks direktiiviga (EL) 2024/1788. Direktiivi (EL) 2024/1788 artiklit 95 arvestades ning lähtudes selle direktiivi IV lisas esitatud direktiivi 2009/73/EÜ ja direktiivi (EL) 2024/1788 vastavustabelist, on direktiivi 2009/73/EÜ artikli 2 punkti 10 vasteks direktiivi (EL) 2024/1788 artikli 2 punkt 32: „füüsiline või juriidiline isik, kes täidab maagaasi hoiustamise ülesannet ja vastutab maagaasihoidla käitamise eest“.
Maagaasiseaduse § 2 punktis 17 on hoidlatevõrgu haldur defineeritud kui „isik, kes täidab gaasi hoiustamise ülesannet ja vastutab gaasihoidla nõuetekohase kasutamise eest“. Seetõttu on kommenteeritavas punktis viidatud hoidlatevõrgu haldurile maagaasiseaduse tähenduses.

Eelnõukohane KüTSi § 3 lõike 3 punkt 11 sätestab üliolulise üksusena infoturbeteenuse osutaja. Selline üksus on ülioluline üksus, kui ta vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.

Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 9 teine taane (*turbetarnijad*). Turbetarnija on defineeritud NIS2-direktiivi artikli 6 punktis 40, mis võetakse üle KüTSi § 2 punktiga 11. Eelnõu esialgses versioonis kasutati turbetarnija asemel terminit „hallatud turbeteenuste osutaja“, kuna eelnõu termin tundus tõlkes kasutatud terminist „turbetarnija“ esialgu selgem. Eelnõu kooskõlastamisel saadud tagasiside alusel otsustati seda muuta. Eelnõus kasutatakse nüüd terminit „infoturbeteenuse osutaja“.

Eelnõukohane KüTSi § 3 lõike 3 punkt 12 sätestab üliolulise üksusena interneti sõlmpunkti teenuse osutaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 8 esimene taane (*interneti vahetuspunkti teenuse osutajad*). Interneti vahetuspunkt on defineeritud NIS2-direktiivi artikli 6 punktis 18, mis võetakse üle KüTSi § 2 punktiga 12. Võrreldes kooskõlastusele saadetud eelnõuga on terminikasutus kooskõlastamisel saadud tagasiside tõttu muutunud. Eelnõu selles punktis kasutatakse NIS2-direktiivi originaaltekstis kasutatud termini „interneti vahetuspunkt“ asemel terminit „interneti sõlmpunkt“.

Eelnõukohane KüTSi § 3 lõike 3 punkt 13 sätestab üliolulise üksusena jaotusvõrgu ettevõtja elektrituru seaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1alapunkti a teine taane (*direktiivi (EL) 2019/944 artikli 2 punktis 29 määratletud jaotusvõrguettevõtjad*). Mainitud direktiivi kohaselt on jaotusvõrguettevõtja „füüsiline või juriidiline isik, kes vastutab jaotusvõrgu käitamise, hoolduse ja vajaduse korral arendamise eest teatud piirkonnas, ja asjakohasel juhul jaotusvõrgu sidumise eest teiste võrkudega, ning kes tagab võrgu pikaajalise võime rahuldada mõistlikku nõudlust elektrienergia jaotamise järele“. 426 SE vastavustabeli kohaselt on direktiivis (EL) 2019/944 kasutatud termini vasteks elektrituruseaduse § 8 lõike 3 kohane jaotusvõrguettevõtja, kes on „juriidiline isik, kes osutab võrguteenust jaotusvõrgu kaudu ning vastutab jaotusvõrgu käitamise, hoolduse ja arendamise eest oma teeninduspiirkonnas ja selle ühendamise eest teiste võrkudega. Jaotusvõrguettevõtja tagab võrgu pikaajalise võime rahuldada mõistlikku nõudlust elektrienergia jaotamise järele“.

Eelnõukohane KüTSi § 3 lõike 3 punkt 14 sätestab üliolulise üksusena kaugkütte- ja kaugjahutussüsteemi käitaja kaugkütteseaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti b esimene taane (*Euroopa Parlamendi ja nõukogu direktiivi (EL) 2018/2001 taastuvatest energiaallikatest toodetud energia kasutamise edendamise kohta (edaspidi* direktiiv (EL) 2018/2001*), artikli 2 punktis 19 määratletud kaugkütte ja kaugjahutuse pakkujad*). Mainitud direktiivi kohaselt on kaugküte ja kaugjahutus „soojusenergia jaotamine võrgu kaudu auru, kuuma vee või jahutatud vedelikena kesksest tootmisallikast või detsentraliseeritud tootmisallikatest mitmesse hoonesse või kohta, et kasutada seda kütteks või jahutamiseks ruumis või protsessides“. Direktiiv (EL) 2018/2001 kavandati üle võtta energiamajanduse korralduse seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõuga nr 382 SE.[39] Nimetatud seaduse eelnõu seletuskirja lisas 1 esitatud vastavustabeli kohaselt on direktiivis (EL) 2018/2001 kasutatud määratluse vasteks kaugkütteseaduse § 2 punkt 1: „soojuse tootmine ja võrgu kaudu jaotamine tarbijate varustamiseks

[39] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/18d86acd-7d58-4219-ac63-5fd6be58a90b/energiamajanduse-korralduse-seaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/

soojusega kaugküttesüsteemi kaudu“. Kaugkütteseaduses ei ole defineeritud kaugjahutust, mistõttu kommenteeritavas punktis sisalduv viide kaugkütteseadusele kohaldub ainult kaugkütte kohta. Energiamajanduse korralduse seaduses on sõnu *jahutus* või *kaugjahutus* kasutatud, kuid selles ei ole defineeritud *kaugjahutussüsteemi*. Ehitusseaduses on kasutatud terminit „kütte- või jahutussüsteem”, kuid neid ei defineerita. Eeldatavasti saab terminis *kaugjahutussüsteem* selguse siis, kui võetakse üle Euroopa Parlamendi ja nõukogu direktiiv (EL) 2024/1275 hoonete energiatõhususe kohta (uuesti sõnastatud) (ELT L, 2024/1275, 08.05.2024), mille artikli 2 punktis 42 on „jahutussüsteem” defineeritud kui “õhu töötlemise komponentide kombinatsioon temperatuuri kontrollimiseks või selle alandamiseks”. Selle direktiivi ülevõtmise tähtaeg on 29. mai 2026.[40]

Eelnõukohane KüTSi § 3 lõike 3 punkt 15 sätestab üliolulise üksusena kauplemiskoha korraldaja väärtpaberituru seaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 4 esimene taane (*Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL, finantsinstrumentide turgude kohta ning millega muudetakse direktiive 2002/92/EÜ ja 2011/61/EL (edaspidi direktiiv 2014/65/EL), artikli 4 punktis 24 määratletud kauplemiskohtade korraldajad*). Direktiivi 2014/65/EL artikli 4 punktis 24 on kauplemiskoht defineeritud kui „reguleeritud turg, mitmepoolne kauplemissüsteem või organiseeritud kauplemissüsteem“. Siinjuures on asjakohased sama direktiivi artikli punktid 21, 22 ja 23:
21) „reguleeritud turg” – turukorraldaja poolt korraldatav ja/või juhitav mitmepoolne süsteem, milles viiakse kokku mitmed kolmandate isikute omandamis- ja võõrandamishuvid seoses süsteemis olevate finantsinstrumentidega või hõlbustatakse nende kokkuviimist vastavalt ühetaolistele eeskirjadele, mille tulemuseks on lepingu sõlmimine seoses finantsinstrumentidega, mis on süsteemi eeskirjade ja/või süsteemide kohaselt kauplemisele lubatud, ning millel on tegevusluba ja mis toimib regulaarselt ja kooskõlas [direktiivi 2014/65/EL] III jaotisega;
22) „mitmepoolne kauplemissüsteem” – investeerimisühingu või turukorraldaja poolt korraldatav mitmepoolne süsteem, milles viiakse kokku mitmed kolmandate isikute omandamis- ja võõrandamishuvid seoses süsteemis olevate finantsinstrumentidega vastavalt ühetaolistele eeskirjadele, mille tulemuseks on lepingu sõlmimine kooskõlas [direktiivi 2014/65/EL] II jaotisega;
23) „organiseeritud kauplemissüsteem” – mitmepoolne süsteem, mis ei ole reguleeritud turg ega mitmepoolne kauplemissüsteem ning mis võimaldab erinevate kolmandate isikute omandamis- ja võõrandamishuvisid seoses võlakirjade, struktureeritud finantstoodete, lubatud heitkoguse väärtpaberite või tuletisinstrumentidega viia süsteemis kokku selliselt, et kõnealuse kokkuviimise tulemuseks on lepingu sõlmimine kooskõlas [direktiivi 2014/65/EL] II jaotisega.
Arvestades NIS2-direktiivi artiklit 4, kohaldatakse DORA määruse artikli 2 lõike 1 punkti i tõttu kauplemiskohtadele DORA määruse nõudeid (vt täpsemalt NIS2-direktiivi artikkel 4 ja DORA määruse põhjendused 15–18). Kommenteeritava punktiga seoses vt ka KüTSi § 1 lõike 4 muudatuste selgitusi.

Eelnõukohane KüTSi § 3 lõike 3 punkt 16 sätestab üliolulise üksusena keskse vastaspoole Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012 börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (ELT L 201, 27.07.2012, lk 1–59) artikli 2 punkti 1 tähenduses.
Kommenteeritava punkti lisamise eesmärk on võtta üle NIS2-direktiivi I lisa punkti 4 teine taane

[40] https://kliimaministeerium.ee/elukeskkond-ringmajandus/energiatohusus-ja-keskkonnasaast/hoonete-energiatohusus

(*Euroopa Parlamendi ja nõukogu määruse (EL) nr 648/2012, börsiväliste tuletisinstrumentide, kesksete vastaspoolte ja kauplemisteabehoidlate kohta (edaspidi* määrus (EL) nr 648/2012*), artikli 2 punktis 1 määratletud kesksed vastaspooled*). Määruse (EL) nr 648/2012 artikli 2 punktis 1 on keskne vastaspool defineeritud kui „ühel või mitmel finantsturul kaubeldavate lepingute vastaspoolte vahel asuv juriidiline isik, kes on iga müüja jaoks ostja ja iga ostja jaoks müüja“.
Arvestades NIS2-direktiivi artiklit 4, kohaldatakse DORA määruse artikli 2 lõike 1 punkti h tõttu kesksetele vastaspooltele DORA määruse nõudeid (vt täpsemalt NIS2-direktiivi artikkel 4 ja DORA määruse põhjendused 15–18). Kommenteeritava punktiga seoses vt ka KüTSi § 1 lõike 4 muudatuste selgitusi.

Eelnõukohane KüTSi § 3 lõike 3 punkt 17 sätestab üliolulise üksusena kosmosepõhise teenuse osutamist toetava ning Eesti Vabariigi või eraõigusliku isiku omandis oleva, hallatava või käitatava maapealse taristu käitaja, kes ei ole üldkasutatava elektroonilise side võrgu teenuse osutaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi I lisa punkti 11 esimene taane (*liikmesriigi või eraõiguslike isikute omandis olevate, hallatavate või käitatavate maapealsete taristute operaatorid, kes toetavad kosmosepõhiste teenuste osutamist, välja arvatud elektroonilise side võrkude pakkujad*).
Kommenteeritava punktiga on seotud ka NIS2-direktiivi põhjendus 37:
(37) Kasvav vastastikune sõltuvus tuleneb üha piiriülesemast ja üha enam vastastikku sõltuvast teenuste osutamise võrgustikust, mis kasutab kogu liidus selliste oluliste sektorite taristuid nagu energeetika, transport, digitaristu, joogi- ja reovesi, tervishoid, avaliku halduse teatavad harud ja ka kosmosetööstus, niivõrd kui viimase teatavate teenuste osutamine sõltub maapealsetest taristutest, mida omavad, haldavad ja käitavad kas liikmesriigid või eraõiguslikud isikud (seega ei hõlma see selliseid taristuid, mida omab, haldab või käitab liit või mida hallatakse või käitatakse liidu nimel liidu kosmoseprogrammi osana). Sellised vastastikused sõltuvussuhted tähendavad seda, et mis tahes häirel – isegi kui see puudutab algselt vaid üht üksust või sektorit – võib olla laiem astmeline mõju, mis võib avaldada kaugeleulatuvat ja pikaajalist negatiivset mõju teenuste osutamisele kogu siseturul. COVID-19 pandeemia ajal hoogustunud küberründed on näidanud, kui vähe kaitstud on meie üha enam üksteisest sõltuvad ühiskonnad väikese realiseerumisvõimalusega riskide esinemise korral.
NIS2-direktiiv ei anna rohkem selgitusi, milliste üksustega on selle puhul tegemist.

Eelnõukohane KüTSi § 3 lõike 3 punkt 18 sätestab üliolulise üksusena krediidiasutuse Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (ELT L 176, 27.06.2013, lk 1–337) artikli 4 punkti 1 tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi I lisa punkti 3 esimene taane (*Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013, krediidiasutuste ja investeerimisühingute suhtes kohaldatavate usaldatavusnõuete kohta ja määruse (EL) nr 648/2012 muutmise kohta (edaspidi* määrus (EL) nr 575/2013*), artikli 4 punktis 1 määratletud krediidiasutused*). Määruse (EL) nr 575/2013 artikli 4 punktis 1 on krediidiasutus defineeritud kui „ettevõtja, kelle äritegevus seisneb järgmises:
a) hoiuste või muude tagasimakstavate vahendite vastuvõtmine avalikkuselt ja oma arvel laenu andmine;
b) Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL I lisa A jao punktides 3 ja 6 osutatud tegevus, kui täidetud on üks järgmistest tingimustest ning ettevõtja ei ole kaubadiiler, lubatud

heitkoguse väärtpaberite diiler, investeerimisfond ega kindlustusandja:
i) ettevõtja konsolideeritud vara koguväärtus on 30 miljardit eurot või rohkem;
ii) ettevõtja vara koguväärtus on alla 30 miljardi euro ning ettevõtja kuulub konsolideerimisgruppi, mille puhul kõigi selliste sinna kuuluvate ettevõtjate, kes tegelevad direktiivi 2014/65/EL I lisa A jao punktides 3 ja 6 osutatud tegevusega ja kellest iga üksiku ettevõtja vara koguväärtus on alla 30 miljardi euro, konsolideeritud vara koguväärtus on 30 miljardit eurot või rohkem, või
iii) ettevõtja vara koguväärtus on alla 30 miljardi euro ning ettevõtja kuulub konsolideerimisgruppi, mille puhul kõigi selliste sinna kuuluvate ettevõtjate, kes tegelevad direktiivi 2014/65/EL I lisa A jao punktides 3 ja 6 osutatud tegevusega, konsolideeritud vara koguväärtus on 30 miljardit eurot või rohkem, kui konsolideeritud järelevalvet tegev asutus järelevalvekolleegiumiga konsulteerides nii otsustab, et käsitleda võimalikku nõuete täitmisest kõrvalehoidmise riski ja võimalikke liidu finantsstabiilsust ohustavaid riske;
punkti b alapunktide ii ja iii kohaldamisel, kui ettevõtja kuulub kolmanda riigi konsolideerimisgruppi, arvestatakse iga liidus tegevusloa saanud kolmanda riigi konsolideerimisgrupi filiaali koguvara kõigi konsolideerimisgruppi kuuluvate ettevõtjate vara koguväärtuse hulka.“
Arvestades NIS2-direktiivi artiklit 4, kohaldatakse DORA määruse artikli 2 lõike 1 punkti a tõttu krediidiasutustele DORA määruse nõudeid (vt täpsemalt NIS2-direktiivi artikkel 4 ja DORA määruse põhjendused 15–18). Kommenteeritava punktiga seoses vt ka KüTSi § 1 lõike 4 muudatuste selgitusi.

Eelnõukohane KüTSi § 3 lõike 3 punkt 19 sätestab üliolulise üksusena laadimispunkti käitaja elektrituruseaduse tähenduses, kes vastutab laadimispunkti haldamise ja käitamise eest, osutades lõppkasutajatele laadimisteenust, sealhulgas liikuvusteenuse osutaja nimel ja eest. Selline üksus on ülioluline üksus, kui see vastab ka käesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Kommenteeritava punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti a seitsmes taane (*laadimispunkti käitajad, kes vastutavad sellise laadimispunkti haldamise ja käitamise eest, mis osutab lõppkasutajatele laadimisteenust, sealhulgas liikuvusteenuse osutaja nimel ja eest*). NIS2-direktiiv ei viita siinjuures ühelegi muule Euroopa Liidu õigusaktile, kuid elektrituruseaduse § 3 punktis 13^1 on defineeritud laadimispunkt kui „liides, millega on võimalik laadida korraga ühte elektrisõidukit või vahetada korraga ühe elektrisõiduki aku“. Kaudselt on selle teemaga seotud ka energiasalvestusüksuse mõiste, mis on elektrituruseaduse § 3 punktis 8^4 defineeritud kui „elektripaigaldise osa, kus salvestatakse energiat, sealhulgas kahesuunalist laadimist võimaldav elektrisõiduki laadimispunkt“. Samuti on sellega seotud elektrituruseaduse peatükk 6^2 (võrguettevõtja kõrvaltegevusalad), mis käsitleb kahte küsimust: elektrisõidukite laadimispunkt ja energiasalvestusüksus.

Eelnõukohane KüTSi § 3 lõike 3 punkt 20 sätestab üliolulise üksusena lennuettevõtja Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002 (ELT L 97, 09.04.2008, lk 72–84), artikli 3 punkti 4 tähenduses, kes tegeleb ärilise lennutranspordiga. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 2 alapunkti a esimene taane (*kommertsvaldkonnas tegutsevad määruse (EÜ) nr 300/2008, mis käsitleb tsiviillennundusjulgestuse ühiseeskirju ja millega tunnistatakse kehtetuks määrus (EÜ) nr 2320/2002, artikli 3 punktis 4 määratletud lennuettevõtjad*). Viidatud määruse artikli 3 punkti 4 kohaselt on lennuettevõtja „kehtiva lennutegevusloaga või samaväärse loaga õhuveoettevõtja“. Kommenteeritavasse punkti on lisatud lauseosa „kes tegeleb ärilise lennutranspordiga“, et

kitsendada kõnealuse punkti kohaldamisala nii, nagu on ette nähtud NIS2-direktiivi I lisas.

Eelnõukohane KüTSi § 3 lõike 3 punkt 21 sätestab üliolulise üksusena lennujaama haldaja Euroopa Parlamendi ja nõukogu direktiivi 2009/12/EÜ lennujaamatasude kohta (ELT L 70, 14.03.2009, lk 11–16) artikli 2 punkti 1 tähenduses ning lennujaama abirajatiste käitaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punkti eesmärk on võtta üle NIS2-direktiivi I lisa punkti 2 alapunkti a teine taane (*Euroopa Parlamendi ja nõukogu direktiivi 2009/12/EÜ, lennujaamatasude kohta (edaspidi* direktiiv 2009/12/EÜ*), artikli 2 punktis 2 määratletud lennujaama juhtorganid, nimetatud direktiivi artikli 2 punktis 1 määratletud lennujaamad, sealhulgas Euroopa Parlamendi ja nõukogu määruse (EL) nr 1315/2013 II lisa 2. jaos loetletud põhivõrgu lennujaamad ning lennujaamades olevaid abirajatisi käitavad üksused*).
Direktiivi 2009/12/EÜ artikli 2 punkti 2 kohaselt on lennujaama juhtorgan „asutus, kelle ainuülesandeks või lisaülesandeks – olenevalt olukorrast – on riiklike õigus- või haldusaktide või lepingute alusel lennujaama või lennujaamade võrgustiku infrastruktuuri haldamine ja juhtimine ning asjaomases lennujaamas või lennujaamade võrgustikus tegutsevate eri käitajate tegevuse koordineerimine ja kontrollimine“. Direktiivi 2009/12/EÜ artikli 2 punkti 1 kohaselt on lennujaam „mis tahes maa-ala, mis on spetsiaalselt kohandatud õhusõidukite maandumiseks, õhkutõusmiseks ja manööverdamiseks, kaasa arvatud lennuliikluse ja -teenuste nõuete täitmiseks vajalikud abirajatised, sealhulgas ärilendude teenindamiseks vajalikud rajatised“.
Riigikogus 1. mail 2022 vastu võetud lennundusseaduse ja riigilõivuseaduse muutmise seaduse eelnõu 477 SE[41] seletuskirja (edaspidi *477 SE seletuskiri*) lk-del 57–58 on lennundusseaduse §-de 50^2 ja 50^3 kohta märgitud järgmist:
„LennS-i § 50^2 lg 1 jäetakse välja osa „(edaspidi käesolevas peatükis *lennujaam*)“. Terminit „lennujaam“ kasutab LennS läbivalt ega ole põhjendatud anda seaduse eri osades sellele erinev tähendus. Selleks, et LennS-i 8^2. peatükk kohalduks üksnes äriliseks lennuliikluseks avatud suurima reisijate arvuga lennujaamale, ei ole vajalik, et terminil „lennujaam“ oleks 8^2. peatükis ülejäänud seadusest erinev tähendus. Muudatus on vajalik, et LennS-i §-des 50^3 ja 50^4 defineeritud terminid oleksid kasutatavad ka eelnõuga LennS-i lisatavas peatükis 8^3. Ilma muudatuseta oleks 8^3. peatükis vaja uuesti defineerida terminid „lennujaama haldaja“ ja „lennujaama kasutaja“.
EL-i lennundusohutuse alusmäärus kasutab termini „lennujaam“ asemel terminit „lennuväli“. LennS-is on kasutatud mõlemat. Kuna direktiivis 96/67/EÜ kasutatakse terminit „lennujaam“, on eelnõus kasutatud maapealse teeninduse teenuste osutamise kontekstis samuti terminit „lennujaam“.
Et korrastada LennS-is terminite „lennujaam“ ja „lennuväli“ kasutamine, eeldab kogu seaduse süsteemset analüüsimist ja muutmist, ent see väljub käesoleva eelnõu raamest.
LennS-i § 50^3 muudetakse, et lennujaama haldaja definitsioon vastaks nii direktiivi 2009/12/EÜ artikli 2 punktile 2 kui ka direktiivi 96/67/EÜ artikli 2 punktile c.
Paragrahvile lisatakse lõige 2, milles täpsustatakse lennujaama haldaja definitsiooni direktiivi 96/67/EÜ artikli 3 lõike 1 kohaselt.
Lõikes 2 täpsustatakse, et kui lennujaama juhib või haldab mitu eri isikut või organit, on LennS-i tähenduses lennujaama haldaja iga selline isik või organ.
Paragrahvis 50^3 kasutatud termin „lennujaama haldaja“ erineb EL-i lennundusohutuse alusmääruse artikli 3 punktis 14 kasutatud terminist „lennuvälja käitaja“, sest direktiivides 2009/12/EÜ ja 96/67/EÜ on kasutusel alusmäärusest erinevad terminid.

[41] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/d2392b95-c13e-44e0-b03d-069c1855fb53/.

Et korrastada LennS-i terminite „lennujaama haldaja“ ja „lennuvälja käitaja“ kasutamine, eeldab kogu seaduse süsteemset analüüsimist ja muutmist, ent see väljub käesoleva eelnõu raamest.“
Lennundusseaduse § 50^3 lõikes 1 on märgitud, et „lennujaama haldaja on lennujaama haldav isik, kelle ülesanne on õigusaktide ja lepingute alusel hallata ja juhtida lennujaama taristut ning koordineerida ja kontrollida lennujaamas tegutsevate käitajate tegevust“ ning lõikes 2 on sätestatud, et „kui lennujaama haldab mitu isikut, on lennujaama haldaja iga selline isik“. Seetõttu ning arvestades 477 SE seletuskirjas esitatud selgitusi lennundusseaduse § 50^3 kohta, on kommenteeritavas punktis otsustatud viidata „lennujaama juhtorganite“ puhul lennundusseaduses kasutatud terminile „lennujaama haldaja“.
Euroopa Parlamendi ja nõukogu määrus (EL) nr 1315/2013 üleeuroopalise transpordivõrgu arendamist käsitlevate liidu suuniste kohta ja millega tunnistatakse kehtetuks otsus nr 661/2010/EL (edaspidi *määrus (EL) nr 1315/2013*), tunnistati 17. juulil 2024 kehtetuks Euroopa Parlamendi ja nõukogu määrusega (EL) 2024/1679, milles käsitletakse liidu suuniseid üleeuroopalise transpordivõrgu arendamise kohta ning millega muudetakse määrusi (EL) 2021/1153 ja (EL) nr 913/2010 ja tunnistatakse kehtetuks määrus (EL) nr 1315/2013 (edaspidi *määrus (EL) 2024/1679*). Määruse (EL) 2024/1679 artikli 68 kohaselt käsitatakse viiteid kehtetuks tunnistatud määrusele (EL) nr 1315/2013 viidetena määrusele 2024/1679 ja neid loetakse vastavalt VII lisas esitatud vastavustabelile. Määruse (EL) nr 1315/2013 II lisa 2. jaos on Eesti puhul põhivõrgu lennujaamadena märgitud Tallinn ja Tartu. Määruse (EL) 2024/1679 vastavustabeli (VII lisa) kohaselt vastab määruse (EL) nr 1315/2013 II lisa määruse (EL) 2024/1679 II lisale (üleeuroopalise transpordivõrgu transpordisõlmede loetelu), mille lennujaama tulbas on Eesti puhul põhivõrguna märgitud ainult Tallinn. Sama tabeli lennujaamade tulbas on üldvõrguna märgitud Kärdla, Kuressaare, Pärnu ja Tartu. Arvestades, et Tallinna lennujaam on hõlmatud ka direktiivi 2009/12/EÜ artikli 2 punkti 1 kohase lennujaama definitsiooniga, pole eelnõus eraldi viidatud Tallinnale kui määruse (EL) 2024/1679 II lisas märgitud põhivõrgu lennuväljale. Eelnõus on viidatud nimetatud direktiivile, mitte Eesti õigusele seetõttu, et lennundusseaduses ei ole lennujaama eraldi defineeritud.
NIS2-direktiiv ei täpsusta, mida peetakse silmas lennujaamas olevate abirajatisi käitavate üksustena, kuid eeldatavasti on siin Eesti puhul mõeldud nt Tallinna lennujaama maapealse teenindusega seotud rajatisi käitavaid isikuid. Maapealse teeninduse teenused hõlmavad näiteks maapealset juhtimist ja järelevalvet, kauba ja posti käitlust, perroonikäitlust,[42] õhusõiduki teenindamist, kütuse- ja õlikäitlust, õhusõiduki hooldust, lennutegevuse ja meeskonna juhtimise, maapealse transpordi ning erivedusid sisaldavaid teenuseid. Maapealse teeninduse teenuste loetelu on esitatud ELi nõukogu direktiivi 96/67/EÜ[43] lisas. Maapealse teenindusega seotud teenuseid võib täielikult või osaliselt pakkuda kolmas isik, aga sellega võib lennujaama kasutaja tegeleda ka iseseisvalt (omakäitleja)[44]. Sel teemal vt ka 477 SE seletuskirjas esitatud vastavate muudatuste selgitusi ja kõnesoleva eelnõuga lennundusseaduses tehtavaid muudatusi.

Eelnõukohane KüTSi § 3 lõike 3 punkt 22 sätestab üliolulise üksusena lennujaama haldaja

[42] Perroonikäitlus hõlmab õhusõiduki liikumise juhendamist maapinnal saabumisel ja väljumisel; abi õhusõiduki sildumisel ja sobivate seadmete kasutada andmist; sidepidamist õhusõiduki ja perrooniteeninduse osutaja vahel; õhusõiduki laadimist ja tühjakslaadimist, sh sobilike seadmetega varustamist ning nende käitamist, samuti meeskonna ja reisijate vedu õhusõiduki ning terminali vahel ning pagasi transporti õhusõiduki ja terminali vahel; õhusõiduki mootori käivitamiseks vajalike seadmetega varustamist ja nende käitamist; õhusõiduki teisaldamist saabumisel ja väljumisel, samuti sobilike seadmetega varustamist ja nende käitamist; toidu ja jookide transporti, nende õhusõidukile laadimist ja sealt mahalaadimist.
[43] Nõukogu direktiiv 96/67/EÜ juurdepääsu kohta maapealse käitluse turule ühenduse lennujaamades.
[44] Omakäitlus on olukord, kus lennujaama kasutaja (lennuettevõtja – näiteks Lufthansa, AirBaltic) osutab otseselt endale üht või mitut liiki maapealse teeninduse teenust ega sõlmi kolmanda isikuga selliste teenuste osutamise lepingut.

lennundusseaduse tähenduses. Selline üksus on üliolulline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
See punkt toimib koosmõjus eelmise punktiga ja teenib samuti NIS2-direktiivi I lisa punkti 2 alapunkti a teise taande ülevõtmise eesmärki. Kui eelmises punktis on viidatud lennujaama haldajale direktiivi 2009/12/EÜ tähenduses, siis selles punktis on viidatud lennujaama haldajale lennundusseaduse tähenduses. Viide riigisisesele lennundusseadusele on vajalik selleks, et hõlmata kõikvõimalikud muud isikud, kes võivad olla lennujaama haldajad ELi õigusest tulenevate nõuete alusel, et ei tekiks potentsiaalseid erinevusi riigisisestest nõuetest. Siinjuures vt ka eelmises punktis esitatud selgitusi määruse (EL) nr 1315/2013 ning selle määruse kehtetuks tunnistanud määruse (EL) 2024/1679 kohta.

KüTSi § 3 lõike 3 punkt 23 sätestab üliolulise üksusena lennujuhtimise teenust osutava lennuliikluskorraldusettevõtja Euroopa Parlamendi ja nõukogu määruse (EL) 2024/2803 ühtse Euroopa taeva algatuse rakendamise kohta (uuesti sõnastatud) artikli 2 punkti 6 tähenduses. Selline üksus on üliolulline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Kommenteeritava punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 2 alapunkti a kolmas taane (*Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 549/2004, millega sätestatakse raamistik ühtse Euroopa taeva loomiseks (raammäärus) (edaspidi* määrus (EÜ) nr 549/2004*) artikli 2 punktis 1 määratletud lennujuhtimise teenust osutavad liikluskorraldusettevõtjad*).
Määrus (EÜ) nr 549/2004 on alates 1. detsembrist 2024 kehtetuks tunnistatud Euroopa Parlamendi ja nõukogu määruse (EL) 2024/2803 ühtse Euroopa taeva algatuse rakendamise kohta (uuesti sõnastatud) (edaspidi *määrus (EL) 2024/2803*) artikliga 56. Sama määruse artiklis 58 („Üleminekusätted“) on sätestatud, millised määruse (EÜ) nr 549/2004 üksikud artiklid kehtivad piiratud tähtaja jooksul. Nende hulgas ei ole viidatud määruse (EÜ) nr 549/2004 artiklile 2 ehk terminite artiklile. Seetõttu tuleb määruse (EÜ) nr 549/2004 artikli 2 terminite puhul lähtuda määruse (EL) 2024/2803 II lisas[45] esitatud vastavustabelist.
Määruse (EÜ) nr 549/2004 artikli 2 punkti 1 kohaselt on lennujuhtimine „[teenus], mille eesmärk on: a) kokkupõrgete vältimine: i) õhusõidukite vahel ja ii) manööverdusalal olevate õhusõidukite ja takistuste vahel; ning (b) lennuliikluse sujuvuse parandamine ja säilitamine“. Määruse (EL) 2024/2803 II lisa kohaselt on selle punkti (täpsemalt artikli 2 punkti 1 punktide a ja b) vasteks määruse (EL) 2024/2803 artikli 2 esimese lõigu punkti 6 alapunktid a ja b, mis on sõnastatud järgmiselt: „lennujuhtimisteenus (ATC-teenus)“ – teenus, mille eesmärk on: a) kokkupõrgete vältimine: i) õhusõidukite vahel; ii) manööverdusalal olevate õhusõidukite ja takistuste vahel; b) lennuliikluse sujuvuse parandamine ja säilitamine“. See tähendab, et selle termini tähendus on sama.
Määruse (EÜ) nr 549/2004 artikli 2 punkti 10 kohaselt on lennuliikluse korraldamine „kõik õhus ja maa peal tehtavad toimingud (lennuliiklusteenused, õhuruumi korraldamine ja lennuliikluse voogude juhtimine), mis on nõutavad õhusõiduki ohutu ja tõhusa liikumise tagamiseks kõikides lennuetappides“. Määruse (EL) 2024/2803 II lisa kohaselt on selle punkti vasteks määruse (EL) 2024/2803 artikli 2 punkt 9, mis on sõnastatud järgmiselt: „lennuliikluse korraldamine (ATM)“ – kõik õhus ja maa peal tehtavad toimingud ja teenused, nimelt lennuliiklusteenused, õhuruumi korraldamine ja lennuliiklusvoo juhtimine, sealhulgas lennuprotseduuride kavandamine, mis on nõutavad õhusõiduki ohutu ja tõhusa liikumise tagamiseks kõikides lennuetappides“. See tähendab, et selle termini tähendus on sama. Eeltoodu tõttu on eelnõu kommenteeritavas punktis kasutatud terminit „lennuliikluskorraldusettevõtja“, et oleks arusaadavam, et tegemist on lennunduse

[45] Vastavustabel, milles on esitatud viited määruse (EÜ) nr 540/2008, määruse (EÜ) nr 550/2004 ja määruse (EÜ) nr 551/2004 seoste kohta määrusega 2024/2803.

valdkonnas tegutseva liiklust korraldava ettevõtjaga.

Eelnõukohane KüTSi § 3 lõike 3 punkt 24 sätestab üliolulise üksusena liiklusseaduse kohase intelligentse transpordisüsteemi käitaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 2 alapunkti d teine taane (*Euroopa Parlamendi ja nõukogu direktiivi 2010/40/EL, mis käsitleb raamistikku intelligentsete transpordisüsteemide kasutuselevõtmiseks maanteetranspordis ja liideste jaoks teiste transpordiliikidega (edaspidi* direktiiv 2010/40/EL*), artikli 4 punktis 1 määratletud intelligentsete transpordisüsteemide operaatorid*). Direktiivi 2010/40/EL artikli 4 punktis 1 on intelligentsed transpordisüsteemid defineeritud kui „süsteemid, milles info- ja sidetehnoloogiat rakendatakse maanteetranspordi valdkonnas (sh infrastruktuur, sõidukid ja kasutajad), liikluskorralduses ja liikuvuse juhtimises ning samuti liidesteks teiste transpordiliikidega“. Liiklusseaduse § 6^1 lõikes 1 on intelligentne transpordisüsteem defineeritud kui „süsteem, milles rakendatakse info- ja sidetehnoloogiat teeliikluse valdkonnas, sealhulgas infrastruktuur, sõidukid ja kasutajad, liikluskorralduses ja liikuvuse juhtimises ning samuti liidesena teise transpordiliigiga“. Seetõttu on viidatud ka liiklusseadusele. Käitaja all mõeldakse juriidilist isikut, kes haldab intelligentset transpordisüsteemi.
Kuigi direktiivi 2010/40/EL artikli 4 punktid 4–6 defineerivad nii „intelligentsete transpordisüsteemide teenuse“ (*intelligentsete transpordisüsteemide rakenduse pakkumine selgelt määratletud organisatsioonilise ja toimimisraamistiku abil, et aidata kaasa kasutusohutusele, tõhususele, kestlikule liikuvusele või mugavusele või transpordi- ja reisitoimingute hõlbustamisele ja toetamisele*), „intelligentsete transpordisüsteemide teenuse pakkuja“ (*avalik- või eraõiguslik intelligentsete transpordisüsteemide teenuse pakkuja*) kui ka „intelligentsete transpordisüsteemide kasutaja“ (*intelligentsete transpordisüsteemide rakenduste või teenuste kasutaja, sh reisijad, vähem kaitstud liiklejad, maanteetranspordi infrastruktuuri kasutajad ja ettevõtjad, sõidukiparkide haldajad ja hädaabiteenuste pakkujad*), ei ole direktiivis 2010/40/EL defineeritud terminit „intelligentsete transpordisüsteemide operaator“. Seetõttu tuleb NIS2-direktiivi I lisa taandes kasutatud termini „intelligentsete transpordisüsteemide operaator“ all mõista direktiivi 2010/40/EL artikli 4 punkti 5 kohast intelligentsete transpordisüsteemide teenuse pakkujat.
Direktiiv 2010/40/EL võeti üle 2. mai 2012. a liiklusseaduse muutmise seadusega (eelnõu nr 182 SE[46]). Nimetatud seaduse eelnõu seletuskirja lk-l 2 on selgitatud liiklusseaduse § 6^1 lõiget 1, sh on selles märgitud, et intelligentse transpordisüsteemi „alla liigituvad näiteks ühistranspordi kasutajatele mõeldud reaalaja infosüsteemid, samuti mitmesugused liikluse turvalisusele (automaatsed hoiatused jms) või liiklusoludest sõltuvalt optimaalse marsruudi planeerimisele suunatud rakendused“.
Eelnõu autorid juhivad seoses kõnealuse punktiga tähelepanu ka asjaolule, et Kliimaministeerium on kõnealuse eelnõu kooskõlastamise ajal esitanud kooskõlastamisele liiklusseaduse muutmise seaduse eelnõu, millega kavandatakse mh muuta ka intelligentsetele transpordisüsteemidele kohalduvaid nõudeid. See eelnõu (liiklusseaduse muutmise seadus) peaks eeldatavasti jõustuma 21. detsembril 2025 (eelnõu toimiku number 25-0547).[47] Selles eelnõus (I ringi versioonis) sooviti defineerida liiklusseaduse § 6^1 lõikes 2^1 „intelligentsete transpordisüsteemide teenus“ kui „intelligentsete transpordisüsteemide rakenduse pakkumine selgelt määratletud organisatsioonilise ja toimimisraamistiku abil, et aidata kaasa kasutusohutusele, tõhususele, kestlikule liikuvusele või mugavusele või transpordi- ja reisitoimingute hõlbustamisele ja toetamisele“. NIS2-direktiivi I lisa

[46] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/7cebb80f-133c-41b9-8e38-bd2b28661cb6/liiklusseaduse-muutmise-seadus/
[47] https://eelnoud.valitsus.ee/main/mount/docList/5a96d59f-1364-49ca-ae3f-279198089b8c

taandes kasutatud termini „intelligentsete transpordisüsteemide operaatori“ all, mis asendatakse Kliimaministeeriumi ette valmistatud eelnõu seadusena jõustumise järel terminiga „intelligentse transpordisüsteemi käitaja“, saab mõista endiselt direktiivi 2010/40/EL artikli 4 punkti 5 kohast „intelligentsete transpordisüsteemide teenuse pakkujat“. Sel juhul tähendab eelnimetatud eelnõu jõustumise järel liiklusseaduses edaspidi sätestatud termin „intelligentsete transpordisüsteemide teenus“ seda teenust, mida kommenteeritavas punktis nimetatud käitaja osutab.

Eelnõukohane KüTSi § 3 lõike 3 punkt 25 sätestab üliolulise üksusena maagaasi rafineerimise ja töötlemise rajatise käitaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti d seitsmes taane (*maagaasi rafineerimise ja töötlemise rajatiste haldurid*). Maagaasiseaduses sellekohast terminit pole, samuti mitte direktiivis 2009/73/EÜ ega selle direktiivi 3. augustil 2024 kehtetuks tunnistanud direktiivis (EL) 2024/1788, mistõttu on kasutatud NIS2-direktiivi I lisas kasutatud terminit.

Eelnõukohane KüTSi § 3 lõike 3 punkt 26 sätestab üliolulise üksusena maagaasi, sealhulgas veeldatud maagaasi müügiga ning hulgimüüjale, lõpptarbijale ja maagaasi ostvale gaasiettevõtjale maagaasi edasimüügiga tegeleva gaasiettevõtja maagaasiseaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga võetakse üle NIS2-direktiivi I lisa punkti 1 alapunkti d esimene taane (*Euroopa Parlamendi ja nõukogu direktiivi 2009/73/EÜ, mis käsitleb maagaasi siseturu ühiseeskirju ning millega tunnistatakse kehtetuks direktiiv 2003/55/EÜ, artikli 2 punktis 8 määratletud tarneettevõtjad*). Nimetatud direktiiv tunnistati 3. augustil 2024 kehtetuks direktiiviga (EL) 2024/1788. Direktiivi (EL) 2024/1788 artiklit 95 arvestades ning lähtudes selle direktiivi IV lisas esitatud direktiivi 2009/73/EÜ ja direktiivi (EL) 2024/1788 vastavustabelist, on direktiivi 2009/73/EÜ artikli 2 punkti 8 vasteks direktiivi (EL) 2024/1788 artikli 2 punkt 29. Direktiivi 2009/73/EÜ artikli 2 punktis 8 defineeriti tarneettevõtja kui „füüsiline või juriidiline isik, kes täidab tarneülesannet“. Direktiivi (EL) 2024/1788 artikli 2 punkti 29 kohaselt on tarneettevõtja definitsioon sama ehk „füüsiline või juriidiline isik, kes täidab tarneülesannet“. Väärib mainimist, et kõnesoleva tarneettevõtja definitsiooniga on seotud ka direktiivi 2009/73/EÜ artikli 2 punkt 7 (*„tarnimine” – maagaasi, sealhulgas veeldatud maagaasi müük, kaasa arvatud edasimüük tarbijale*), mille vaste uuendatud sõnastuses on direktiivi (EL) 2024/1788 artikli 2 punkt 28 (*„tarnimine“ – maagaasi, sealhulgas veeldatud maagaasi, või vesiniku, sealhulgas vedela orgaanilise vesiniku kandja kujul vesiniku või veeldatud vesiniku ja vesiniku derivaatide, sealhulgas ammoniaagi või metanooli müük, kaasa arvatud edasimüük tarbijatele*); samuti ka direktiivi 2009/73/EÜ artikli 2 punkt 24 (*„tarbija” – maagaasi hulgimüüja või lõpptarbija ja maagaasi ostev maagaasiettevõtja*), mille vaste uuendatud sõnastuses on direktiivi (EL) 2024/1788 artikli 2 punkt 47 (*„tarbija“ – maagaasi või vesiniku hulgimüüja või lõpptarbija ja maagaasi või vesinikku ostev maagaasi- või vesinikuettevõtja*).
Direktiiv 2009/73/EÜ võeti maagaasiseadusesse üle maagaasiseaduse muutmise seadusega (eelnõu 166 SE).[48] Nimetatud seaduse eelnõu seletuskirjas oleva vastavustabeli (edaspidi *166 SE vastavustabel*) kohaselt on direktiivi 2009/73/EÜ artikli 2 punktis 8 sätestatud termini vasteks maagaasiseaduse § 2 (täpsustamata konkreetset punkti), kuid tolles seaduses ei ole seda terminit rohkem selgitatud ega täpsustatud. Kui arvestada selle termini sisu eelviidatud direktiivides, siis eeldatavasti on see seotud maagaasiseaduse § 7 lõikega 4: „gaasi müük käesoleva seaduse tähenduses on gaasi üleandmine isikule tasu eest“. Kõigest eeltoodust lähtudes tähendab

[48] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5dea306a-39a3-43c7-9d74-e20d79ad6527/maagaasiseaduse-muutmise-seadus/

kommenteeritav punkt järgmist: tegemist on maagaasi edasimüügiga tegeleva gaasiettevõtjaga, kes müüb maagaasi (sh veeldatud maagaasi) maagaasi hulgimüüjale, lõpptarbijale ja maagaasi ostvale gaasiettevõtjale; või sama tegevus edasimüügina.
Eelnõu kommenteeritava punkti kooskõlastusele saadetud variandi sõnastuses lähtuti direktiivi 2009/73/EÜ sõnastusest (millele ka NIS2-direktiivis on viidatud), mitte direktiivist (EL) 2024/1788, millest lähtumine hõlmaks selle terminiga ka vesinikuga seotud sarnaseid tegevusi tegevad ettevõtjad. Maagaasiseaduse §-s 4 on gaasiettevõtja defineeritud kui „ettevõtja, kes tegutseb vähemalt ühel tegevusalal, milleks on gaasi tootmine, import, ülekanne, jaotamine, hoiustamine või müük, ning kes vastutab selle tegevusega seonduva kaubandusliku või hoolduskü simuse lahendamise eest“. Eelnõus on ka kooskõlastamise järel jäädud direktiivi 2009/73/EÜ (eelnõus pakutud) kitsama sõnastuse juurde. Seda põhjusel, et direktiivi (EL) 2024/1788 ülevõtmistähtaeg on direktiivi artikli 94 kohaselt 5. august 2026 ja Eesti maagaasiseadust ei ole uuest direktiivist tulenevalt veel muudetud. Seetõttu ei ole KüTSi eelnõu koostamise ajal veel võimalik gaasiettevõtja definitsiooni uue, kuid veel üle võtmata direktiiviga ühildada. Direktiivi (EL) 2024/1788 ülevõtmisel tuleb üle vaadata ka kõnealune KüTSi § 3 lõike 3 punkt 26 ning vajaduse korral seda muuta. Käesoleva eelnõu raames see veel võimalik ei ole.

Eelnõukohane KüTSi § 3 lõike 3 punkt 27 nimetab üliolulise üksusena määratud elektriturukorraldaja Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943, milles käsitletakse elektrienergia siseturgu (ELT L 158, 14.06.2019, lk 54–124), artikli 2 punkti 8 tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti a viies taane (*Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943, milles käsitletakse elektrienergia siseturgu (edaspidi* määrus (EL) 2019/943*), artikli 2 punktis 8 määratletud määratud elektriturukorraldajad*). Selle määruse kohaselt on määratud elektriturukorraldaja „turukorraldaja, kelle pädev asutus on nimetanud täitma ülesandeid ühtse järgmise päeva turu mehhanismis või ühtse päevasisese turu mehhanismis“.

Eelnõukohane KüTSi § 3 lõike 3 punkt 28 nimetab üliolulise üksusena nafta tootmise, rafineerimise ja töötlemise rajatiste käitamise ning nafta hoiustamise ja ülekandmisega tegeleva ettevõtja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi I lisa punkti 1 alapunkti c teine taane (*nafta tootmise, rafineerimise ja töötlemise rajatiste ning hoiustamise ja ülekandmisega tegelevad operaatorid*).

Eelnõukohane KüTSi § 3 lõike 3 punkt 29 sätestab üliolulise üksusena pilvandmetöötlusteenuse osutaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 8 neljas taane (*pilvandmetöötlusteenuse osutajad*). Termin „pilvandmetöötlusteenus“ on defineeritud NIS2-direktiivi artikli 6 punktis 30, mis on kavas üle võtta KüTSi § 2 punktiga 23. Kommenteeritava punktiga on seotud ka NIS2-direktiivi põhjendused 33 ja 34:
(33) Pilvandmetöötlusteenused peaksid hõlmama digiteenuseid, mis võimaldavad jagatavate andmetöötlusressursside skaleeritava ja paindliku kogumi nõudepõhist haldamist ning ulatuslikku kaugpääsu sellele kogumile, muu hulgas juhul, kui need ressursid paiknevad hajutatult erinevates kohtades. Andmetöötlusressursid on näiteks võrgud, serverid ja muu taristu, operatsioonisüsteemid, tarkvara, talletusruum, rakendused ja teenused. Pilvandmetöötluse

teenusemudelid hõlmavad muu hulgas taristut teenusena (IaaS), platvormi teenusena (PaaS), tarkvara teenusena (SaaS) ja võrku teenusena (NaaS). Pilvandmetöötluse korraldusmudelid peaksid hõlmama privaat-, ühis-, avalikku ja hübriidpilve. Mõistetel „pilvandmetöötlusteenus" ja „korraldusmudel" on sama tähendus nagu nimetatud mõistetel standardi ISO/IEC 17788:2014 määratluses. Pilvandmetöötlusteenuse kasutaja võimekust tagada endale ühepoolselt andmetöötlusvõimekus, nagu serveriaeg või võrgu talletusruum, ilma pilvandmetöötlusteenuse osutaja inimesepoolse sekkumiseta, võiks nimetada nõudepõhiseks haldamiseks. Mõistega „ulatuslik kaugpääs" peetakse silmas seda, et pilvevõimalusi pakutakse võrgu kaudu ja need on kättesaadavad mehhanismide kaudu (sealhulgas mobiiltelefonid, tahvelarvutid, sülearvutid ja tööjaamad), mis toetavad heterogeensete nn kõhnade või paksude kliendiplatvormide kasutamist. Mõiste „skaleeritav" osutab andmetöötlusressurssidele, mis on nõudluse kõikumisega toimetulekuks pilveteenuse osutaja poolt paindlikult jaotatavad olenemata ressursside geograafilisest asukohast. Mõistet „paindlik kogum" kasutatakse andmetöötlusressursside kirjeldamiseks, mida pakutakse ja mis tehakse kättesaadavaks vastavalt nõudlusele, et kättesaadavaid ressursse suurendada või vähendada sõltuvalt töökoormusest. Mõistet „jagatav" kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mida pakutakse paljudele kasutajatele, kellel on ühine juurdepääs teenusele, kuid mille puhul andmete töötlemine toimub iga kasutaja jaoks eraldi, olgugi et teenust osutatakse samadest elektroonilistest seadmetest. Mõistet „hajusad" kasutatakse selliste andmetöötlusressursside kirjeldamiseks, mis asuvad erinevates võrguga ühendatud arvutites või seadmetes ning mis suhtlevad omavahel ja kooskõlastavad omavahelist tegevust sõnumite edastamise teel.
(34) Kuna maad võtavad uuenduslikud tehnoloogiad ja ärimudelid, tulevad eeldatavasti tarbijate muutuvate vajaduste järgi siseturule uued pilvandmetöötlusteenuse ja korraldusmudelid. Sellises kontekstis võib pilvandmetöötlusteenuseid osutada väga hajusal kujul, mille puhul töötlus toimub andmete loomise või kogumise kohale veelgi lähemal; seega liikudes nn traditsiooniliselt mudelilt väga hajusale mudelile (servtöötlus).

Eelnõukohane KüTSi § 3 lõike 3 punkt 30 sätestab üliolulise üksusena põhivõrguettevõtja elektrituruseaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi I lisa punkti 1 alapunkti a kolmas taane (*direktiivi (EL) 2019/944 artikli 2 punktis 35 määratletud põhivõrguettevõtjad*). Mainitud direktiivi kohaselt on põhivõrguettevõtja „füüsiline või juriidiline isik, kes vastutab põhivõrgu käitamise, hoolduse ja vajaduse korral arendamise eest teatud piirkonnas, ja asjakohasel juhul põhivõrgu sidumise eest teiste võrkudega, ning kes tagab võrgu pikaajalise võime rahuldada mõistlikku nõudlust elektrienergia ülekandmise järele". 426 SE vastavustabeli kohaselt on direktiivis (EL) 2019/944 kasutatud termini vasteks elektrituruseaduse § 8 lõike 2 kohane põhivõrguettevõtja, kes on „elektriettevõtja, kes osutab võrguteenust põhivõrgu kaudu".

Eelnõukohane KüTSi § 3 lõike 3 punkt 31 sätestab üliolulise üksusena raudteeinfrastruktuuriettevõtja ja raudteeveoettevõtja, sealhulgas teenindusrajatise käitaja raudteeseaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 2 alapunkti b esimene taane (*Euroopa Parlamendi ja nõukogu direktiivi 2012/34/EL, millega luuakse ühtne Euroopa raudteepiirkond (edaspidi* direktiiv 2012/34/EL*), artikli 3 punktis 2 määratletud raudteeinfrastruktuuri-ettevõtjad*) ja teine taane (*direktiivi 2012/34/EL artikli 3 punktis 3 määratletud raudteeveo-ettevõtjad, sealhulgas nimetatud direktiivi artikli 3 punktis 12 määratletud teenindusrajatiste käitajad*).

Direktiivi 2012/34/EL artikli 3 punkti 2 kohaselt on raudteeinfrastruktuuri-ettevõtja „asutus või ettevõtja, kes vastutab raudteevõrgustikul raudteeinfrastruktuuri käitamise, hooldamise ja uuendamise ning samuti selle arendamises osalemise eest vastavalt liikmesriigi infrastruktuuri arendamise ja rahastamise üldise poliitika raames sätestatule“. Raudteeseaduse § 2 punkt 14 defineerib raudteeinfrastruktuurietteõtja kui: „raudtee-ettevõtja, kelle ülesanneteks on avalikul raudteevõrgustikul raudteeinfrastruktuuri majandamine, käitamine, hooldamine ja uuendamine ning raudteeinfrastruktuuri arendamises osalemine vastavalt [raudteeseaduse] § 73 lõikes 1 nimetatud tegevuskavale“. Raudteeseaduse § 2 punkt 13 defineerib raudtee-ettevõtja kui „füüsilisest isikust ettevõtja või äriühing, kelle tegevuseks on raudteevedu või kes täidab raudteeinfrastruktuurietteõtja ülesandeid“.
Direktiivi 2012/34/EL artikli 3 punkti 1 kohaselt on raudteeveo-ettevõtja „vastavalt [direktiivile 2012/34/EL] tegevusloa saanud avalik-õiguslik või eraõiguslik ettevõtja, kelle peamine tegevusala on osutada raudtee-kaubaveoteenuseid ja/või raudtee-reisijateveo teenuseid ja kes on kohustatud tagama veduriteenuse; see hõlmab ka ainult veduriteenust osutavaid ettevõtjaid“. Raudteeseaduse § 2 punkti 29 järgi on raudteeveoettevõtja „vastava tegevusloa saanud ettevõtja, kelle peamine tegevusala on raudteevedu ja kes on kohustatud tagama veduriteenuse, samuti isik, kes osutab ainult veduriteenust“. Raudteeseaduse § 2 punkti 25 järgi on raudteevedu „kauba- või reisijatevedu ja veduriteenuse osutamine raudteel või ainult veduriteenuse osutamine“.
Direktiivi 2012/34/EL artikli 3 punkti 12 kohaselt on teenindusrajatise käitaja „avalik-õiguslik või eraõiguslik isik, kes on vastutav ühe või mitme teenindusrajatise juhtimise või ühe või mitme [sama direktiivi] II lisa punktides 2–4 osutatud teenuse osutamise eest raudteeveo-ettevõtjatele“. Raudteeseaduse § 95 lõige 95 defineerib teenindusrajatise käitaja kui „ettevõtja, kes majandab ühte või mitut teenindusrajatist või osutab ühes või mitmes teenindusrajatises asjakohast teenust või [raudteeseaduse] § 94 lõikes 2 või 3 nimetatud teenust raudteeveoettevõtjale“.
Eeltoodu tõttu on kommenteeritavas punktis kasutatud raudteeseaduse vastavaid termineid.

Eelnõukohane KüTSi § 3 lõike 3 punkt 32 sätestab üliolulise üksusena sadama pidaja või sadamarajatise valdaja sadamaseaduse tähenduses, sealhulgas Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 725/2004 artikli 2 punktis 11 määratletud sadamarajatiste valdaja, ning sadamates tööde ja varustuse haldamisega tegelev üksus. Selline üksus on üliolulise üksus, kui see vastab ka käesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Kommenteeritava punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 2 alapunkti c teine taane (*Euroopa Parlamendi ja nõukogu direktiivi 2005/65/EÜ, sadamate turvalisuse tugevdamise kohta (edaspidi* direktiiv 2005/65/EÜ*), artikli 3 punktis 1 määratletud sadamate valdajad, sealhulgas nende määruse (EÜ) nr 725/2004 artikli 2 punktis 11 määratletud sadamarajatised ning sadamates tööde ja varustuse haldamisega tegelevad üksused*). Direktiivi 2005/65/EÜ artikli 3 punktis 1 on sadam defineeritud kui „teatud maa- ja veeala, mille piirid on määratlenud sadama asukoha liikmesriik ning mis koosneb kaubandusliku meretranspordi hõlbustamiseks ette nähtud seadmetest ja rajatistest“. Sadamaseaduse § 2 punktis 1 on sadam defineeritud kui „veesõidukite sildumiseks kohandatud ja sadamateenuse osutamiseks kasutatav maa- ja veeala ning seal asuvad sadama sihtotstarbeliseks kasutamiseks vajalikud ehitised“.
Kommenteeritav punkt on sõnastatud kehtiva KüTSi § 3 lõike 1 punkti 4 („sadamateenuse osutaja, kes on sadamaseaduse tähenduses sellise sadama pidaja või sellise sadamarajatise valdaja, mis teenindab 500-se ja enama kogumahutavusega laevu või rahvusvahelises meresõidus sõitvaid reisilaevu sadama toimimise teenuse osutamisel“) eeskujul. Seetõttu on kommenteeritavas punktis viidatud sadamaseadusele.
Määruse (EÜ) nr 725/2004 artikli 2 punktis 11 on sadamarajatis defineeritud kui „laeva ja sadama vahelise liidese koht; see hõlmab vastavalt asjaoludele ka selliseid alasid nagu ankrupaigad,

ooteplatvormid ja sildumisalad“. Sadamaseaduse § 2 punktis 9 on sadamarajatis defineeritud kui „sadama maa-alal või akvatooriumil (edaspidi mõlemad koos sadamaala) turvanõuete täitmiseks määratud laeva ja sadama vahelise koostöö ja liidese koht, mis hõlmab vajaduse korral ka sadama territooriumi, akvatooriumi ja sissesõiduteed“. Kuna NIS2-direktiiv viitab otsekohalduvale ELi määrusele, on kommentaaritavas punktis viidatud nii ELi määrusele kui ka sadamaseadusele.

Eelnõukohane KüTSi § 3 lõike 3 punkt 33 sätestab üliolulise üksusena sisulevivõrguteenuse osutaja. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi I lisa punkti 8 kuues taane (*sisulevivõrguteenuse osutajad*). Termin „sisulevivõrk“ on defineeritud NIS2-direktiivi artikli 6 punktis 32, mis on kavas üle võtta KüTSi § 2 punktiga 25.

Eelnõukohane KüTSi § 3 lõike 3 punkt 34 sätestab üliolulise üksusena turuosalise Euroopa Parlamendi ja nõukogu määruse (EL) 2019/943 artikli 2 punkti 25 tähenduses, kes osutab agregeerimis-, tarbimiskaja- või elektrienergia salvestamise teenust elektrituruseaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Kommenteeritava punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti a kuues taane (*määruse (EL) 2019/943 artikli 2 punktis 25 määratletud turuosalised, kes osutavad direktiivi (EL) 2019/944 artikli 2 punktides 18, 20 ja 59 määratletud agregeerimis-, tarbimiskaja- või energia salvestamise teenuseid*). Määruse (EL) 2019/943 artikli 2 punktis 25 on turuosalised defineeritud kui „füüsiline või juriidiline isik, kes toodab, ostab või müüb elektrit, tarbimiskaja või salvestamisteenuseid, mis hõlmab kauplemiskorralduste andmist ühel või mitmel elektriturul, sealhulgas tasakaalustamisenergia turgudel“. Direktiivi (EL) 2019/944 artikli 2 punktis 18 on agregeerimine defineeritud kui „füüsilise või juriidilise isiku tegevus, mille käigus ühendatakse paljude tarbijate tarbimiskoormus või toodetud elektrienergia elektriturul müümiseks, ostmiseks või oksjonile panemiseks“. 426 SE vastavustabeli kohaselt on direktiivi (EL) 2019/944 asjaomase punkti vasteks elektrituruseaduse § 3 punkt 1^3, mille kohaselt on see „tegevus, mille käigus ühendatakse tarbijate tarbimiskoormus või tootjate tootmisvõimsus elektriturul müümiseks või ostmiseks“. Direktiivi (EL) 2019/944 artikli 2 punktis 20 on tarbimiskaja defineeritud kui „elektri tarbimise koormuse muutmine lõpptarbijate poolt, mis seisneb normaalse või jooksva tarbimise muutmises vastuseks turusignaalidele, sealhulgas vastuseks ajas muutuvale elektrihinnale või rahalistele stiimulitele, või vastuseks lõpptarbija kas iseseisvalt või energiavahendaja kaudu tehtud ja aktsepteeritud pakkumisele müüa komisjoni rakendusmääruse (EL) nr 1348/2014 artikli 2 punktis 4 määratletud organiseeritud turu hinnaga tarbimise vähendamist või suurenemist“. 426 SE vastavustabeli kohaselt on direktiivi (EL) 2019/944 asjaomase punkti vasteks elektrituruseaduse § 3 punkt 23^3, mille kohaselt on see „elektri tarbimise koormuse juhtimine, mis seisneb tarbija iseseisvas tarbimise muutmises või agregaatori kaudu tehtud ja aktsepteeritud pakkumises müüa komisjoni rakendusmääruse (EL) nr 1348/2014, milles käsitletakse andmete esitamist ja millega rakendatakse energia hulgimüügituru terviklikkust ja läbipaistvust käsitleva Euroopa Parlamendi ja nõukogu määruse (EL) nr 1227/2011 artikli 8 lõiked 2 ja 6, artikli 2 punktis 4 määratletud organiseeritud turu hinnaga tarbimise vähendamist või suurendamist“. Direktiivi (EL) 2019/944 artikli 2 punktis 59 on energia salvestamine defineeritud kui „elektrivõrgus elektrienergia lõppkasutamise edasilükkamine tootmise hetkest hilisemal ajale või elektrienergia muundamine salvestatavaks energiaks, sellise energia salvestamine ning seejärel selle taasmuundamine elektrienergiaks või kasutamine muu energiakandjana“. 426 SE vastavustabeli kohaselt on direktiivi (EL) 2019/944 asjaomase punkti vaste elektrituruseaduse § 3 punkt 8^3, kuid õige vaste

peaks olema punkt 8^2 (elektrienergia salvestamine): „elektrienergia muundamine salvestatavaks energiaks, sellise energia salvestamine ja seejärel taasmuundamine elektrienergiaks või kasutamine muu energiakandjana eesmärgiga lükata elektrienergia lõppkasutamine tootmise hetkest hilisemale ajale või optimeerida koormusi elektrisüsteemis salvestusperioodi vältel“.

Eelnõukohane KüTSi § 3 lõike 3 punkt 35 näeb üliolulise üksusena ette veeldatud gaasi terminali halduri maagaasiseaduse tähenduses. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega võetakse üle NIS2-direktiivi I lisa punkti 1 alapunkti d viies taane (*direktiivi 2009/73/EÜ artikli 2 punktis 12 määratletud maagaasi veeldusjaamade haldurid*). Direktiivi 2009/73/EÜ artikli 2 punkti 12 kohaselt on maagaasi veeldusjaamade haldur „füüsiline või juriidiline isik, kes täidab maagaasi veeldamise või impordi, mahalaadimise ja taasgaasistamise ülesannet ning vastutab maagaasi veeldusjaama kasutamise eest“. Direktiiv 2009/73/EÜ tunnistati 3. augustil 2024 kehtetuks direktiiviga (EL) 2024/1788. Direktiivi (EL) 2024/1788 artiklit 95 arvestades ning lähtudes selle direktiivi IV lisas esitatud direktiivi 2009/73/EÜ ja direktiivi (EL) 2024/1788 vastavustabelist, on direktiivi 2009/73/EÜ artikli 2 punkti 12 vasteks direktiivi (EL) 2024/1788 artikli 2 punkt 34, mille kohaselt on asjaomane haldur: „füüsiline või juriidiline isik, kes täidab maagaasi veeldamise või veeldatud maagaasi impordi, mahalaadimise ja taasgaasistamise ülesannet ning vastutab maagaasi veeldusjaama kasutamise eest“.
Maagaasiseaduse § 2 punktis 18 on veeldatud gaasi terminali haldur defineeritud kui „isik, kes täidab gaasi veeldamise, impordi, ümberlaadimise ja taasgaasistamise ülesannet ning vastutab gaasi veeldusjaama nõuetekohase kasutamise eest“. Seetõttu on kommenteeritavas punktis viidatud veeldatud gaasi terminali haldurile maagaasiseaduse tähenduses.

Eelnõukohane KüTSi § 3 lõike 3 punkt 36 sätestab üliolulise üksusena veeliikluse juhtimise keskuse. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 2 alapunkti c kolmas taane (*Euroopa Parlamendi ja nõukogu direktiivi 2002/59/EÜ, millega luuakse ühenduse laevaliikluse seire- ja teabesüsteem ning tunnistatakse kehtetuks nõukogu direktiiv 93/75/EMÜ (edaspidi* direktiiv 2002/59/EÜ*), artikli 3 punktis o määratletud laevaliikluse juhtimise keskuste (VTS) operaatorid*). Direktiivi 2002/59/EÜ artikli 3 punktis o on laevaliikluse juhtimise keskus (VTS) defineeritud kui „talitus, mis on kavandatud laevaliikluse ohutuse ja tõhususe tõstmiseks ning keskkonna kaitsmiseks ning mis suudab laevaliiklusega seoses infot vahetada ja reageerida laevaliikluse juhtimise piirkonnas laevaliikluses tekkivatele olukordadele“.
Kommenteeritava punktiga seotud teemasid reguleerib meresõiduohutuse seaduse 12. peatükk, mille § 51 (laevaliikluse korraldamise süsteemi eesmärk) lõike 2 kohaselt korraldab nimetatud süsteemi tööd Transpordiamet (kes on ülioluline üksus ka eelnõukohase KüTSi § 3 lõike 2 punkti 3 alusel). Sama paragrahvi lõikes 2^2 on sätestatud: „Laevaliikluse korraldamise süsteemi tööpiirkond jaguneb laevaliiklusteeninduse piirkonnaks ja Soome lahe laevaettekannete süsteemi piirkonnaks.“

Eelnõukohane KüTSi § 3 lõike 3 punkt 37 näeb üliolulise üksusena ette veeseaduse § 17 lõike 1 kohase joogiveega varustaja ja selle jaotaja, välja arvatud jaotaja, kelle puhul on joogivee jaotamine tema üldise muude tarbekaupade ja kaupade tarnimise tegevuse väheoluline osa. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega kavandatakse üle võtta NIS2-direktiivi I lisa punkti 6 esimene taane (*Euroopa Parlamendi ja nõukogu direktiivi (EL) 2020/2184, olmevee kvaliteedi kohta (edaspidi* direktiiv 2020/2184*),*

artikli 2 punkti 1 alapunktis a määratletud olmeveega varustajad ja olmevee jaotajad, välja arvatud jaotajad, kelle puhul olmevee jaotamine on väheoluline osa nende üldisest muude tarbekaupade ja kaupade tarnimistegevusest). Direktiivi 2020/2184 artikli 2 punkti 1 alapunktis a on olmevesi defineeritud kui:
„a) vesi, algkujul või pärast töötlemist, mis on mõeldud joomiseks, keetmiseks, toiduvalmistamiseks ja muudeks olmeotstarveteks nii avalikes kui eravaldustes, olenemata vee päritolust ning sellest, kas veevarustus toimub jaotusvõrgu kaudu, vett antakse tsisternist või on vesi villitud pudelitesse või mahutitesse; hõlmatud on ka allikavesi;
b) vesi, mida toidukäitlemisettevõtja kasutab toiduks mõeldud toodete või ainete tootmiseks, töötlemiseks, säilitamiseks või turustamiseks".
Joogiveeseaduse §-s 17 on joogivesi defineeritud kui:
„(1) Joogivesi [joogiveeseaduse] tähenduses on algkujul või töödeldud vesi, sealhulgas allikavesi, mis on mõeldud joomiseks, keetmiseks, toiduvalmistamiseks või muuks olmeotstarbeks kõigis omandivormides, olenemata vee päritolust ning sellest, kas see toimetatakse tarbijani jaotusvõrgu kaudu, paagiga, pudelis või mahutis.
(2) Joogiveeks nimetatakse ka vett, mida toidukäitleja Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002, millega sätestatakse toidualaste õigusnormide üldised põhimõtted ja nõuded, asutatakse Euroopa Toiduohutusamet ja kehtestatakse toidu ohutusega seotud menetlused (EÜT L 31, 01.02.2002, lk 1–24), artikli 3 punkti 3 tähenduses kasutab inimesele tarbimiseks mõeldud toodete või ainete tootmiseks, töötlemiseks, säilitamiseks või turustamiseks."
Joogiveeseaduse § 17 lõikes 2 esitatud definitsioon on sama mis direktiivi 2020/2184 artikli 2 punkti 1 alapunktis b, kuid kuna NIS2-direktiiv hõlmab ainult seda alapunkti a, siis tuleb kommenteeritavas punktis täpsustada, et tegemist on joogiveega joogiveeseaduse § 17 lõike 1 tähenduses.
NIS2-direktiiv ei selgita, mida tuleks pidada „väheoluliseks osaks", sellega seoses vt ka eelnõujärgse KüTSi § 3 lõike 3 punkti 4 kohta esitatud selgitust.

Eelnõukohane KüTSi § 3 lõike 3 punkt 38 sätestab üliolulise üksusena vesiniku tootmise, hoiustamise ja ülekandmisega tegeleva ettevõtja. Selline üksus on üliioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi I lisa punkti 1 alapunkti e esimene taane (*vesiniku tootmise, hoiustamise ja ülekandmisega tegelevad operaatorid*). NIS2-direktiiv ei selgita, kes on vesiniku tootmise, hoiustamise ja ülekandmisega tegelev operaator (eelnõus „ettevõtja").
Ka direktiiv 2009/73/EÜ ei viita vesinikule ega sellega seotud üksustele, kuid selle direktiivi 3. augustil 2024 kehtetuks tunnistanud direktiivis (EL) 2024/1788 on artikli 2 punktis 14 vesinikuettevõtja defineeritud kui „füüsiline või juriidiline isik, kes täidab vähemalt üht järgmistest ülesannetest: vesiniku tootmine, transportimine, tarnimine, ostmine või hoiustamine või vesinikuterminali käitamine, ning kes vastutab nende ülesannetega seotud kaubanduslike, tehniliste või hoolduskusimuste eest, välja arvatud lõpptarbijad". Lisaks on direktiivi (EL) 2024/1788 artikli 2 punktis 5 vesinikuhoidla haldur defineeritud kui „füüsiline või juriidiline isik, kes täidab vesiniku hoiustamise ülesannet ja vastutab vesinikuhoidla käitamise eest". Direktiivi (EL) 2024/1788 artikli 2 punktis 26 on vesiniku ülekandevõrgu haldur defineeritud kui „füüsiline või juriidiline isik, kes vastutab vesiniku ülekandevõrgu käitamise, selle hoolduse tagamise ja vajaduse korral vesiniku ülekandevõrgu arendamise eest teatavas paikkonnas ja kohaldataval juhul selle teiste vesinikuvõrkudega ühendamise eest ning selle eest, et on tagatud võrgu pikaajaline võime rahuldada mõistlikku nõudlust vesiniku transportimise järele".
Eelnõus on kasutatud NIS2-direktiivi I lisa sõnastust (see on sama mis eelnõus). Vt kommenteeritava punktiga seoses ka eelnõukohase KüTSi § 3 lõike 3 punkti 26 selgitust.

Eelnõukohane KüTSi § 3 lõike 3 punkt 39 sätestab üliolulise üksusena sellise üksuse, kes tegeleb ravimiseaduse kohase ravimi, välja arvatud Euroopa Parlamendi ja nõukogu määruse (EL) 2019/6, mis käsitleb veterinaarravimeid ning millega tunnistatakse kehtetuks direktiiv 2001/82/EÜ (ELT L 4, 07.01.2019, lk 43–67), artikli 4 punktis 1 määratletud veterinaarravimi uurimise ja arendamisega.
Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi I lisa punkti 5 kolmas taane (*üksused, mis tegelevad Euroopa Parlamendi ja nõukogu direktiivi 2001/83/EÜ, inimtervishoius kasutatavaid ravimeid käsitlevate ühenduse eeskirjade kohta (edaspidi* direktiiv 2001/83/EÜ*), artikli 1 punktis 2 määratletud ravimite uurimise ja arendamisega*). Direktiivi 2001/83/EÜ artikli 1 punktis 2 on ravim defineeritud kui „a) aine või ainete kombinatsioon, mille omadused on ette nähtud inimeste haiguste raviks või nende ärahoidmiseks; või b) kõik sellised ained või ainete kombinatsioonid, mida võib kasutada või manustada inimeste meditsiiniliseks diagnoosimiseks või füsioloogilise talitluse taastamiseks, parandamiseks või modifitseerimiseks farmakoloogilise, immunoloogilise või ainevahetusliku toime avaldamise kaudu.“
Ravimiseaduse § 2 lõike 1 kohaselt on ravim „aine või ainete kombinatsioon, mis on mõeldud inimese haiguse või haigussümptomi vältimiseks, diagnoosimiseks või ravimiseks, haigusseisundi kergendamiseks või elutalitluse taastamiseks või muutmiseks farmakoloogilise, immunoloogilise või metaboolse toime kaudu“. Sama paragrahvi lõikes 2 on sätestatud: „[r]avimina käsitatakse ka veterinaarravimit Euroopa Parlamendi ja nõukogu määruse (EL) 2019/6 artikli 4 punkti 1 tähenduses“. Kuna NIS2-direktiivis mõeldakse siinjuures inimestega seotud ravimeid, siis on kommenteeritavasse punkti lisatud välistus, et tegemist ei ole veterinaarravimiga Euroopa Parlamendi ja nõukogu määruse (EL) 2019/6, mis käsitleb veterinaarravimeid ning millega tunnistatakse kehtetuks direktiiv 2001/82/EÜ, artikli 4 punkti 1 tähenduses.

Eelnõukohane KüTSi § 3 lõike 3 punkt 40 sätestab üliolulise üksusena üksuse, kes täidab maagaasi jaotamise ülesannet ja vastutab jaotussüsteemi kasutamise eest, tagades selle jaotussüsteemi hooldamise ja vajaduse korral arendamise teatud paikkonnas, ning tagab vajaduse korral maagaasivõrgu ühendamise teiste maagaasivõrkudega ja maagaasivõrgu pikaajalise võime rahuldada mõistlikku nõudlust maagaasi jaotamise järele. Selline üksus on ülioluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punkti kehtestamise eesmärk on võtta üle NIS2-direktiivi I lisa punkti 1 alapunkti d teine taane (*direktiivi 2009/73/EÜ artikli 2 punktis 6 määratletud jaotussüsteemi haldurid*). Direktiivi 2009/73/EÜ artikli 2 punkti 6 kohaselt on jaotussüsteemi haldur „füüsiline või juriidiline isik, kes täidab gaasi jaotamise ülesannet ja vastutab jaotussüsteemi kasutamise eest, tagades selle hoolduse ja vajadusel jaotussüsteemi ehitamise teatud paikkonnas, ning vajadusel gaasivõrgu vastastikuse ühendamise teiste võrkudega, ning kes tagab võrgu pikaajalise võime rahuldada mõistlikku nõudlust gaasi jaotamise järele“. Direktiiv 2009/73/EÜ tunnistati 3. augustil 2024 kehtetuks direktiiviga (EL) 2024/1788. Direktiivi (EL) 2024/1788 artiklit 95 arvestades ning lähtudes selle direktiivi IV lisas esitatud direktiivi 2009/73/EÜ ja direktiivi (EL) 2024/1788 vastavustabelist, on direktiivi 2009/73/EÜ artikli 2 punkti 6 vasteks direktiivi (EL) 2024/1788 artikli 2 punkt 20, mis defineerib selle termini järgmiselt: „füüsiline või juriidiline isik, kes täidab maagaasi jaotamise ülesannet ja vastutab jaotussüsteemi käitamise, selle hoolduse tagamise ja vajaduse korral arendamise eest teatud paikkonnas, ning kohaldataval juhul selle teiste süsteemidega ühendamise eest ning selle eest, et on tagatud süsteemi pikaajaline võime rahuldada mõistlikku nõudlust maagaasi jaotamise järele“. Selle terminiga on seotud ka direktiivi 2009/73/EÜ artikli 2 punkt 5

(*„jaotamine" – maagaasi transportimine kohalike või piirkondlike torustike kaudu tarbijatele, välja arvatud tarnimine*), mille vaste on direktiivi (EL) 2024/1788 artikli 2 punkt 19 (*„jaotamine" – maagaasi transportimine kohalike või piirkondlike torustike kaudu selle edastamiseks tarbijatele, välja arvatud tarnimine*).
166 SE vastavustabeli vaste on siinjuures sama mis eelnõukohase KüTSi § 3 lõike 3 punkti 26 puhul, kuid eeldatavasti on see seotud maagaasiseaduse § 7 lõikega 3: „Gaasi jaotamine käesoleva seaduse tähenduses on gaasi transportimine piirkondlike või jaotustorustike kaudu tarbijapaigaldisteni, kokkulepitud liitumispunktini või liitumispunktist jaotustorustikuni, kaasa arvatud ülekandevõrgu osa, mida kasutatakse gaasi kohalikuks jaotamiseks". Termini „üksus" kohta vt eelnõukohase KüTSi § 2 punkti 36 selgitust. Eelnõu kommenteeritavat punkti sõnastades lähtuti ennekõike direktiivi 2009/73/EÜ sõnastusest (millele NIS2-direktiivis on ka viidatud), mitte direktiivist (EL) 2024/1788, mis erinevad üksteisest selle poolest, et ühes kasutatakse sõna „ehitamine", teises selle asemel „arendamine" (eelnõus kasutatakse viimast). Eeskujuks valitud direktiivi kohta vt ka eelnõukohase KüTSi § 3 lõike 3 punkti 26 selgitust.

Eelnõukohane KüTSi § 3 lõike 3 punkt 41 sätestab üliolulise üksusena üksuse, kes täidab maagaasi ülekandmise ülesannet ja vastutab ülekandesüsteemi käitamise eest, tagades selle ülekandesüsteemi hooldamise ja vajaduse korral arendamise teatud paikkonnas, ning tagab vajaduse korral maagaasivõrgu ühendamise teiste maagaasivõrkudega ja maagaasivõrgu pikaajalise võime rahuldada mõistlikku nõudlust maagaasi ülekandmise järele. Selline üksus on üliolulise üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi I lisa punkti 1 alapunkti d kolmas taane (*direktiivi 2009/73/EÜ artikli 2 punktis 4 määratletud ülekandesüsteemi haldurid*). Direktiivi 2009/73/EÜ artikli 2 punkti 4 kohaselt on ülekandesüsteemi haldur „füüsiline või juriidiline isik, kes täidab ülekande ülesannet ja vastutab ülekandesüsteemi kasutamise eest, tagades selle hoolduse ja vajadusel ülekandesüsteemi ehitamise teatud paikkonnas, ning vajadusel gaasivõrkude vastastikuse ühendamise teiste võrkudega, ning kes tagab võrgu pikaajalise võime rahuldada mõistlikku nõudlust gaasi transportimise järele". Direktiiv 2009/73/EÜ tunnistati 3. augustil 2024 kehtetuks direktiiviga (EL) 2024/1788. Direktiivi (EL) 2024/1788 artiklit 95 arvestades ning lähtudes selle direktiivi IV lisas esitatud direktiivi 2009/73/EÜ ja direktiivi (EL) 2024/1788 vastavustabelist, on direktiivi 2009/73/EÜ artikli 2 punkti 4 vasteks direktiivi (EL) 2024/1788 artikli 2 punkt 18, mis defineerib selle termini kui: „füüsiline või juriidiline isik, kes täidab ülekande ülesannet ja vastutab ülekandesüsteemi käitamise, selle hoolduse tagamise ja vajaduse korral ülekandesüsteemi arendamise eest teatud paikkonnas, ning kohaldataval juhul selle teiste süsteemidega ühendamise eest, ning selle eest, et on tagatud süsteemi pikaajaline võime rahuldada mõistlikku nõudlust maagaasi transportimise järele".
166 SE vastavustabeli vaste on siin sama mis eelnõukohase KüTSi § 3 lõike 3 punkti 26 puhul, kuid eeldatavasti on see seotud maagaasiseaduse § 7 lõikega 2: „Gaasi ülekanne käesoleva seaduse tähenduses on gaasi transportimine ülekandevõrgu kaudu kokkulepitud liitumispunktini või liitumispunktist ülekandevõrguni. Gaasi ülekandeks ei peeta tootmisetapi torustiku ega ülekandevõrgu osa kasutamist gaasi kohalikuks jaotamiseks." Termini „üksus" kohta vt eelnõukohase KüTSi § 2 punkti 36 selgitust. Eelnõu kommenteeritavat punkti sõnastades lähtuti nii direktiivi 2009/73/EÜ (millele NIS2-direktiivis on ka viidatud) kui ka direktiivi (EL) 2024/1788 sõnastusest.

Eelnõukohase KüTSi § 3 lõikega 4 kavandatakse üle võtta NIS2-direktiivi artikli 3 lõige 2. Kõnealuse lõike sõnastamisel lähtuti eeldusest, et KüTSi mõistes on teenuseosutajad kas üliolulised üksused või olulised üksused. Seetõttu on kõnealuse lõike punktides sätestatud need

üksused, kes ei ole üliolulised üksused, sh on need ka õigusselguse huvides eelnõus nimetatud.
Osaliselt on kõnealuses lõikes oluliste üksustena nimetatud sellised üksused, kes on NIS2-direktiivi kohaselt otsesõnu olulised üksused (nt teatud rohkem kui 50 töötajaga ja 10 miljonilise aastase käibe või bilansimahuga üksused). Osaliselt on aga tegemist oluliste üksuste riigisisese määramisega, arvestades NIS2-direktiivi artiklis 2 lõike 2 punktides b–e sätestatud kriteeriume. Need kriteeriumid on järgmised:

> *b) üksus on liikmesriigis sellise teenuse ainuosutaja, mis on kriitilise tähtsusega ühiskondliku või majandustegevuse säilitamiseks;*
> *c) üksuse osutatava teenuse häirel võib olla oluline mõju avalikule turvalisusele, avalikule julgeolekule või rahvatervisele;*
> *d) üksuse osutatava teenuse häire võib tuua kaasa olulise süsteemse riski, eelkõige sektorites, kus sellisel häirel võib olla piiriülene mõju;*
> *e) üksus on kriitilise tähtsusega oma erilise olulisuse tõttu riiklikul või piirkondlikul tasandil konkreetse sektori või teenuseliigi või liikmesriigi muude üksteisest sõltuvate sektorite jaoks.*

Nimetatud NIS2-direktiivi punktid ei täpsusta rohkem, milliseid üksusi on neis mõeldud, vaid igal liikmesriigil on endal võimalus sätestada NIS2-direktiivi ülevõtvas õigusaktis lisaks üksusi, kes vastavad kommenteeritavas lõikes nimetatud kriteeriumitele ning kes on riigisisese seaduse subjektid. Seda on kommenteeritavas lõikes nimetatud subjektide oluliste üksustena sätestamisel tehtud (vt vastavaid selgitusi allpool konkreetsete punktide juures). Samas on loobutud NIS2-direktiivi artikli 2 lõike 2 eraldi ülevõtmisest, st eelnõu uues versioonis ei ole enam kooskõlastusele saadetud eelnõus sisaldunud KüTSi § 1 lõiget 1^4, mis nägi ette vastavad kriteeriumid, vaid eelnõus on juba nendest kriteeriumitest lähtudes sätestatud teatavad üksused üliolulistе ja oluliste üksustena.
Kommenteeritava lõike punktides 1–7 ja 9 nimetatud üksused on olulised üksused sõltumata nende töötajate arvust, käibest ja bilansimahust. Punkti 8 kohaldamisel tuleb aga arvestada ka üksuse töötajate arvu ning käivet või bilansimahtu.
KüTSi § 3 lõike 4 senine sisu (KüTSi reeglite kohaldumine erinevatele avaliku sektori üksustele) on osaliselt kaetud lõikesse 4 lisatavate punktidega (olulised üksused) ning osaliselt ka § 3 lõike 2 punktidega 3 (keskvalitsuse avaliku halduse üksused) ja 4 (kohaliku omavalitsuse avaliku halduse üksused).

Eelnõukohase KüTSi § 3 lõike 4 punktiga 1 sätestatakse olulise üksusena andmekogu vastutav ja volitatud töötleja avaliku teabe seaduse tähenduses. Sellega säilitatakse kehtiv KüTSi § 3 lõike 4 punkt 1. Nimetatud punkt lisati KüTSi 2022. a küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (eelnõu nr 531 SE) vastuvõtmise tulemusel.[49] Selle eelnõu seletuskirja (edaspidi *531 SE seletuskiri*) lk-l 10 selgitati nimetatud sätte lisamist järgmiselt: „Loetelu esimene punkt on [avaliku teabe seaduse] tähenduses andmekogu vastutav ja volitatud töötleja. [Avaliku teabe seaduse] § 43^1 lõikes 1 olevat andmekogu definitsioonis olev lauseosa „mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks“ viitab, et andmekogusid asutatakse ja kasutatakse avalike ülesannete täitmiseks. Seetõttu on kohane hõlmata avalikus sektoris oleva teenuse osutaja nimekirja ka andmekogude vastutavad ja volitatud töötlejad; sh enamik neist on hõlmatud ka muude kavandatava § 3 lõikes 4 olevate punktide sõnastuste tõttu, kuid mitte kõik. Näiteks ei ole muude punktidega hõlmatud Liikluskindlustuse Fond, mis on [avaliku teabe seaduse] mõistes andmekogu vastutav töötleja. Andmekogude vastutavate ja volitatud töötleja hõlmamine avaliku sektori loetelu

[49] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/cd3107f9-b19c-4ed4-b6a7-7379fa3bf6b9/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus/

alla on vajalik ka põhjusel, et eelnõu asendab [avaliku teabe seaduse] alusel kehtestatud ISKE KüTS-i alusel kehtestava [Eesti infoturbestandardiga] ning selleks, et tagada andmekogude küberturvalisus, tuleb seega ka täpsustada KüTS-i kohaldamisala. Ka juba kehtiva õiguse kohaselt oli volitatud töötlejatel kohustus [avaliku teabe seadusest] tulenevalt täita vastutava töötleja juhiseid andmekogu turvalisuse tagamisel. Olenemata sellest, et vastutav töötleja vastutab tema andmekoguga toimuva osas isiklikult, sest vastutust ei ole võimalik edasi anda, ei ole vastutavad töötlejad olnud aktiivsed vastavasisulisi juhiseid jagama. Sellele vaatamata tuleb volitatud töötlejal tagada endast lähtuvalt turvalisus vähemalt samaväärsel tasemel vastutava töötlejaga".
Eeltoodud selgitus viitab ka sellele, et andmekogu all ei mõelda igasugust andmete kogumit vms, vaid sellist, mis on asutatud seaduse alusel, sh seaduses on selle kasutamine (andmekogu eesmärk) kindlaks määratud.
Avaliku teabe seaduse § 43^4 lõikes 1 on andmekogu vastutav töötleja (haldaja) defineeritud kui „riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutusele võtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest."
Sama paragrahvi lõike 2 kohaselt võib andmekogu vastutav töötleja „volitada andmete töötlemise ja andmekogu majutamise teisele riigi- või kohaliku omavalitsuse asutusele, avalik-õiguslikule juriidilisele isikule või hanke- või halduslepingu alusel eraõiguslikule isikule vastutava töötleja poolt ettenähtud ulatuses". Tegemist on siis volitatud töötlejale vastava ülesande volitamisega. Andmekaitse Inspektsiooni andmekogude juhendis[50] on lk-l 13 volitatud töötleja ja tema rolli kohta märgitud: „volitatud töötleja võib olla nii vastutava töötleja kontrolli all tegutsev andmekogu igapäevane haldaja kui ka teenuste osutaja näiteks andmekogu majutaja või arendajana. Sellist volitatud töötleja rolli täidavad paljude andmekogude suhtes IT-asutused nagu RIK ja SMIT. Teenuse osutajaid ei ole vajalik põhimääruses nimepidi loetleda, piisab nende ülesannete nimetamisest". See tähendab et andmekogu volitatud töötleja all avaliku teabe seaduse kontekstis on mõeldud ennekõike volitatud töötlejat, kes majutab konkreetset andmekogu ja vajaduse korral tegeleb selle andmekogu arendamise ja ülalpidamisega. Andmekogu volitatud töötleja all ei ole siinjuures mõeldud näiteks andmeandjat avaliku teabe seaduse tähenduses (vt avaliku teabe seaduse § 43^5 lõige 2) ega ka mitte igasugust isikuandmete volitatud töötlejat isikuandmete kaitse üldmääruse või isikuandmete kaitse seaduse tähenduses.
Kommenteeritav punkt lisatakse KüTSi, arvestades NIS2-direktiivi artikli 2 lõike 2 punktides b, c, d ja e sätestatud kriteeriume.

Eelnõukohase KüTSi § 3 lõike 4 punktiga 2 määratakse oluliseks üksuseks Arenguseire Keskus. Selle punkti eelnõus sätestamisega säilitatakse kehtiv KüTSi § 3 lõike 4 punkt 2.
531 SE seletuskirja lk-l 10 selgitati nimetatud sätte lisamist järgmiselt: „Loetelu teine punkt on Arenguseire Keskus, mis on küll Riigikogu Kantselei struktuuriüksus, kuid arenguseire seaduse § 3 lõike 2 alusel on Keskus oma ülesannete täitmisel iseseisev. Keskuse ülesandeks on ühiskonna pikaajaliste (üle 10-aastase ajahorisondi ulatuvate) arengute tuvastamine, analüüs ja nende põhjal erinevate arengustsenaariumite koostamine koos Eesti ühiskonnale avanevate võimaluste ja ohtude eristamisega, arengustsenaariumite realiseerimise jälgimine ning vajadusel arengustsenaariumite ja nende järelmite korrigeerimine.[51] Eelnõu eesmärk on tagada ka Keskuse tegevuses kasutatavate süsteemide ja andmete turvalisus, mistõttu on õigusselguse huvides eraldi välja toodud ka

[50] Kättesaadav: https://abi.ria.ee/riha/materjalid-riha-kasutajale ja https://abi.ria.ee/__attachments/7243279/AKI_Andmekogude%20juhend.pdf?inst-v=2d62fbb5-f953-41db-a674-fc3dbd1b13b2.
[51] Arenguseire Keskuse tutvustus: https://www.riigikogu.ee/riigikogu/riigikogu-kantselei/juhtkond-ja-osakonnad/.

Arenguseire Keskus kui Riigikogu Kantselei struktuuriüksus. Eelduslikult kohaldatakse küberturvalisuse nõudeid kõikide subjektide kõikidele struktuuriüksustele, kuid see punkt loetelus on loodud õigusselguse tagamise eesmärgil, sest Arenguseire Keskus on oma ülesannete täitmisel iseseisev.“
Kommenteeritav punkt lisatakse KüTSi, arvestades NIS2-direktiivi artikli 2 lõike 2 punktides b ja e sätestatud kriteeriume.

Eelnõukohase KüTSi § 3 lõike 4 punktiga 3 sätestatakse olulise üksusena seaduse alusel asutatud avalik-õiguslikud juriidilised isikud. See on seotud kehtiva KüTSi § 3 lõike 4 punkti 10 säilitamisega.
531 SE seletuskirja lk-del 11–12 selgitati nimetatud sätte lisamist järgmiselt: „Loetelu üheteistkümnes punkt on seaduse alusel loodud avalik-õiguslik juriidiline isik, nt Eesti Haigekassa, Notarite Koda või erinevad ülikoolid.[52] Eranditult kannavad kõik avalik-õiguslikud juriidilised isikud olulist osa avaliku sektori toimimisel, olgu tegemist ühenduse, asutuse või fondiga. Küberturvalisuse nõuded kohaldusid mitmele avalik-õiguslikule juriidilisele isikule ka varasemalt kui andmekogu vastutavale või volitatud töötlejale. Kuivõrd avalik-õiguslikel juriidilistel isikutel on reeglina arvestatav ligipääs erinevatele andmekogudele ning nende osutatavad reguleeritud teenused on ühiskondlikult tähtsad, siis on ka selle eelnõu punkti eesmärk avalikule sektorile mõeldud kohaldamisala täpsustada avalik-õiguslike juriidiliste isikute suhtes. Siinse punkti suhtes on üks erinorm seotud Eesti Rahvusringhäälinguga (vt kehtiva KüTS § 3 lg 1 punkti 10 ning sellega seonduvalt ka [531 SE] § 1 punkti 5 ning § 3 selgitust). Vastav erinorm kehtib kuni 2026. aasta 31. detsembrini.“
Siinkohal vt ka Eesti Rahvusringhäälingu seaduse muudatuse selgitusi.
Kommenteeritav punkt lisatakse KüTSi, arvestades NIS2-direktiivi artikli 2 lõike 2 punktides d ja e sätestatud kriteeriume.

Eelnõukohase KüTSi § 3 lõike 4 punktiga 4 määratakse olulise üksusena kohalike omavalitsuse üksuste liit. Selle eesmärk on säilitada KüTSi § 3 lõike 4 punkt 4.
531 SE seletuskirja lk-l 19 selgitati nimetatud sätte lisamist järgmiselt: „Loetelu neljas punkt on kohaliku omavalitsuse üksuste liit, nt Harjumaa Omavalitsuste Liit, ning kohaliku omavalitsuse üksus ehk vallad ja linnad. Selle ning loetelu neljateistkümnenda punkti eesmärk on täpsustada kohaldamisala kohaliku omavalitsuse üksuse kontekstis, kus sarnaselt riigiasutustega on õigusselguse huvides vajalik määratleda avalik sektor täpsemalt kui juriidilise isiku tasandil.“
Regionaal- ja Põllumajandusministeerium on ette valmistanud kohaliku omavalitsuse korralduse seaduse ja sellega seonduvate seaduste muutmise seaduse (eelnõude infosüsteemi toimik 24-0006),[53] millega sätestatakse kohaliku omavalitsuse korralduse seaduses termini „kohaliku omavalitsuse üksus“ kohta lühend „omavalitsusüksus“ ning samasse seadusesse lisatakse ka 10^1. peatükk nimega „Omavalitsusüksuste liidud“, milles omakorda kasutatakse selle liidu kohta lühendit „omavalitsusüksus“. Kuna terminit „omavalitsusüksus“ kasutatakse selles seaduses termini „kohaliku omavalitsuse üksus“ lühendina ning selle tulem on tähenduselt sama mis kommenteeritavas punktis, siis kõnealuses punktis kasutatud termini „üksus“ all mõeldaksegi selle eelnõu seadusena jõustumise järel kohaliku omavalitsuse korralduse seaduses kasutatud lühendit „omavalitsusüksuste liit“.
Kommenteeritav punkt lisatakse KüTSi, arvestades NIS2-direktiivi artikli 2 lõike 2 punktis e

[52] Algse joonealuse viite sõnastust on muudetud: avalik-õiguslikud juriidilised isikud on leitavad siit: https://www.fin.ee/riigihaldus-ja-avalik-teenistus-kinnisvara/riigihaldus/avaliku-sektori-statistika – vt „Töötajad ja asutused“ sakk „Avaliku sektori asutused“, filtreerides asutuse tüübina „avalik-õiguslikud asutused“.
[53] https://eelnoud.valitsus.ee/main/mount/docList/345b8b87-0431-4aaa-ad59-6f0e7112fd8b

sätestatud kriteeriumi.

Eelnõukohase KüTSi § 3 lõike 4 punktiga 5 sätestatakse olulise üksusena perearstiabi osutaja tervishoiuteenuse korraldamise seaduse tähenduses, kes ei ole elutähtsa teenuse osutaja. KüTSi kehtiva versiooni § 3 lõike 1 punkti 7 kohaselt kuuluvad KüTSi kohaldamisalasse kõik tervishoiuteenuste korraldamise seaduses sätestatud perearstiabi osutajad perearstiabi osutamisel. Algselt anti perearstidele üleminekuks aega *ca* 3,5 aastat: KüTS jõustus mais 2018 ning KüTSi § 29 lõike 3 kohaselt jõustus perearstidega seotud säte 2022. aasta 1. jaanuaril.
Kommenteeritavas punktis on lauseosa „kes ei ole elutähtsa teenuse osutaja“, kuna CER-direktiivi ülevõtmisel on edaspidi osa perearstidest samal ajal ka elutähtsa teenuse osutajad hädaolukorra seaduse tähenduses (kes lisatakse KüTSi subjektiks kavandatava KüTSi § 3 lõike 2 punktiga 2). 426 SE seletuskirjas on märgitud (lk-l 42): „Hinnanguliselt vastab elutähtsa teenuse osutaja kriteeriumidele 60 perearstiabi teenuse osutajat. See tagab igas maakonnas vähemalt kaks elutähtsat teenust osutavat perearstiabi osutajat ning suuremates maakondades elanikkonna arvu järgi rohkem“. Lisaks on sama seletuskirja lk-l 59 märgitud: „Elutähtsa teenuse osutajateks on kavas määrata ka 26 perearstiabi osutajat“; ning lk-del 74–75 on märgitud: „Hinnanguliselt saavad [elutähtsa teenuse osutajateks] kuni 26 perearstiabi osutajat, kes on jaotunud üle Eesti nii, et igas maakonnas oleks vähemalt kaks elutähtsat teenust osutavat perearstiabi osutajat. Eestis on üle 400 isikut, kellel on kehtiv tegevusluba perearstiabi perearsti nimistu alusel osutamiseks. Mõju sihtrühm on väike, kuna moodustab u 5% kõikidest üldarstiabiteenuse osutajatest.“ Sarnased põhimõtted on ka ette nähtud tsiviilkriisi ja riigikaitse seaduses, mis hakkab tulevikus asendama hädaolukorra seadust.
Kehtiva KüTSi § 3 lõike 1 punkti 7 kohaselt kuuluvad KüTSi kohaldamisalasse kõik tervishoiuteenuste korraldamise seaduses nimetatud perearstiabi osutajad perearstiabi osutamisel. Selleks, et eristada neid perearste, kes ei ole edaspidi elutähtsa teenuse osutajad, kuid kes kuuluvad NIS2-direktiivi I lisa punkti 5 esimese taande kohaselt (*Euroopa Parlamendi ja nõukogu direktiivi 2011/24/EL, patsiendiõiguste kohaldamise kohta piiriüleses tervishoius (edaspidi* direktiiv 2011/24/EL*), artikli 3 punktis g määratletud tervishoiuteenuse osutajad*) ka NIS2-direktiivi kohaldamisalasse, on eelnõuga kavandatud lisada KüTSi kommenteeritav punkt. Direktiivi 2011/24/EL artikli 3 punkti g kohaselt on tervishoiuteenuse osutaja „füüsiline või juriidiline isik või muu üksus, kes osutab liikmesriigi territooriumil seaduslikult tervishoiuteenuseid“. Sama artikli punktis a on tervishoiuteenus defineeritud kui „tervishoiuteenused, mida tervishoiutöötajad osutavad patsientidele, et hinnata, säilitada või taastada nende terviseseisundit, sealhulgas ravimite ja meditsiiniseadmete väljakirjutamine, väljastamine ja nendega varustamine“. St üldistatult võib selle punkti alla esmapilgul paigutada erinevaid tervishoiuteenuseid ja nende osutajaid, kuid eelnõu koostajate soov on NIS2-direktiivi võimalikult kitsalt üle võtta, sh ennekõike säilitada kehtiv õigus. Kommenteeritavasse punkti ei ole võimalik lisada kehtiva KüTSi asjakohase punkti lauseosa „perearstiabi osutamisel“, kuna NIS2-direktiiv näeb ette, et sellised üksused hakkavad tervikuna kuuluma KüTSi kohaldamisalasse.
Direktiivi 2011/24/EL artikli 3 punkt g on seotud ka kehtiva KüTSi § 3 lõike 1 punktiga 6 (*tervishoiuteenuste korraldamise seaduses sätestatud haiglavõrku kuuluvate piirkondliku haigla ja keskhaigla pidaja statsionaarse eriarstiabi osutamisel ja kiirabibrigaadi pidaja kiirabi osutamisel*), kuid KüTSi see punkt võetakse üle nii, et selles nimetatud üksustest saavad CER-direktiivi üle võtva seaduse (eelnõu nr 426 SE) vastuvõtmise tulemusena elutähtsa teenuse osutajad. Seetõttu puudub ka vajadus lisada KüTSi nende üksuste kohta kommenteeritava punktiga sarnane säte.
Kommenteeritav punkt lisatakse KüTSi, arvestades NIS2-direktiivi artikli 2 lõike 2 punktides b, c ja e sätestatud kriteeriume.

Eelnõukohase KüTSi § 3 lõike 4 punktiga 6 määratakse oluliseks üksuseks Riigimetsa Majandamise Keskus. Selle eesmärk on seotud kehtiva KüTSi § 3 lõike 4 punkti 9 säilitamisega. 531 SE seletuskirja lk-l 11 selgitati nimetatud sätte lisamist järgmiselt: „Loetelu kümnes punkt on Riigimetsa Majandamise Keskus. Eelnõu koostamise hetkel on Riigimetsa Majandamise Keskus ainus riigitulundusasutus Eestis. Kahjuks aga ei ole eelnõu koostamise hetkel kehtivas õiguses riigitulundusasutuse tähendust määratletud ning puudub ka võimalus Riigimetsa Majandamise Keskust muud moodi määratleda. Kuni 01.01.2010 kehtinud riigivaraseaduse § 6 lõike 1 alusel on riigitulundusasutus riigiasutus, mis võib osutada tasulisi teenuseid ja saada selle eest tulu. Ka eelnõu koostamise hetkel kehtivas riigivaraseaduses on korduvalt riigitulundusasutuse terminit kasutatud, kuid puudub eraldi säte termini määratlemiseks. Kehtiva riigivaraseaduse eelnõu seletuskirja[54] kohaselt ei peetud õigeks sätestada asutuse vorm riigivaraseaduses ning soovitati seda teha Vabariigi Valitsuse seaduses või näiteks sellest asutuse vormist loobuda. Eelnõu koostamise hetkeks kumbagi aga tehtud ei ole. Sellest hoolimata on aga vajalik tagada Riigimetsa Majandamise Keskuse süsteemide turvalisus, kuivõrd tema teenused ning selleks kasutatavad andmed on ühiskonna toimimise seisukohast olulised.“
Kommenteeritav punkt lisatakse KüTSi, arvestades NIS2-direktiivi artikli 2 lõike 2 punktides b ja e sätestatud kriteeriume.

Eelnõukohase KüTSi § 3 lõike 4 punktiga 7 määratakse oluliseks üksuseks selline usaldusteenuse osutaja, kes ei ole kvalifitseeritud usaldusteenuse osutaja. NIS2-direktiivi kohaldamisalasse kuuluvad usaldusteenuse osutajad, kelleks on definitsiooni (vt eelnõukohane KüTSi § 2 punkt 32 ning selles viidatud määruse punkt ja siinse seletuskirja selgitus) kohaselt nii kvalifitseeritud teenuse osutajad (definitsiooni vt eelnõukohasest KüTSi § 2 punktist 16 ning selles viidatud määruse punktist ja siinse seletuskirja selgitusest) kui ka kvalifitseerimata usaldusteenuse osutajad. Kvalifitseeritud usaldusteenuse osutajad on üliolulised üksused ning ülejäänud usaldusteenuse osutajad on olulised üksused.

Eelnõukohane KüTSi § 3 lõike 4 punkt 8 on seotud eelnõukohases KüTSi § 3 lõikes 3 nimetatud tegevusalal tegutsevate üksustega, kes ei ole üliolulised üksused (vt NIS2-direktiivi artikli 3 lõige 2), sest nad ei vasta lõike 3 sissejuhatavas osas nimetatud finants- ja tööjõualastele piirmääradele. Kui üksus tegutseb mõnel lõikes 3 nimetatud tegevusalal, siis kehtivad kõnesolevas punktis nimetatud madalamad piirmäärad töötajate arvule ning käibele või bilansile, millele vastamisel loetakse üksus oluliseks üksuseks KüTSi tähenduses.
Kommenteeritava punkti jõustumise tulemusel kuulub oluliste üksuste hulka üksus, kes vastab kõigile järgmistele tingimustele (arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ):
a) tal on majandusaasta jooksul 50 või rohkem töötajat;
b) tema aastane bilansimaht on üle 10 miljoni euro või tema aastakäive on üle 10 miljoni eurot;
c) ta on nimetatud KüTSi § 3 lõikes 3, st tegemist on vähemalt ühe üksusega selles lõikes viidatud 41 üksuse seas;
d) ta ei ole ülioluline üksus KüTSi § 3 lõike 3 kohaselt.
Kommenteeritava punktiga seosest vt ka eespool esitatud selgitust Euroopa Komisjoni soovituse 2003/361/EÜ rakendamise kohta.

Eelnõukohase KüTSi § 3 lõike 4 punktiga 9 luuakse seos NIS2-direktiivi artikli 3 lõike 1

[54] Riigivaraseaduse eelnõu nr 437 SE seletuskiri lk 14, kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/bd686b3c-a592-2d90-dc53-12d484999745/Riigivaraseadus.

punktiga c ehk kommenteeritava punktiga lisatakse kohaldamisalasse need üldkasutatava elektroonilise side võrgu teenuse osutajad ja üldkasutatava elektroonilise side teenuse osutajad, kes pole üliolulised üksused – viimati nimetatute kohta vt eelnõukohast KüTSi § 3 lõike 2 punkti 9 ja selle selgitust. Siinkohal tuleb ka arvestada asjaoluga, et NIS2-direktiiv näeb ette, et üldkasutatava elektroonilise side võrgu teenuse osutajad ja üldkasutatava elektroonilise side teenuse osutajad kuuluvad NIS2-direktiivi kohaldamisalasse olenemata nende suurusest ehk kõik vastavaid teenuseid osutavad üksused on hõlmatud KüTSiga.
Kõnesoleva punkti jõustumise tulemusel on oluliste üksuste hulka lisatud need üldkasutatava elektroonilise side võrgu teenuse osutajad ja üldkasutatava elektroonilise side teenuse osutajad, kes ei vasta eelnõukohases KüTSi § 3 lõike 2 punktis 9 sätestatud piirmääradele. Sellisel juhul kuuluvad need üksused kõnealuse punkti kohaldamisalasse.

Eelnõukohases KüTSi § 3 lõikes 5 on lisaks lõikele 4 sätestatud veel üks oluliste üksuste loetelu. Ka lõike 5 kohaldamisel tuleb arvestada Euroopa Komisjoni soovituses 2003/361/EÜ ette nähtud piirmääradega. Need piirmäärad on samad mis eelnõukohases KüTS § 3 lõike 4 punktis 8. See tähendab, et kommenteeritava lõike jõustumise tulemusel kuulub oluliste üksuste hulka üksus, kes vastab kõigile järgmistele tingimustele (arvestades keskmise suurusega ettevõtja määratlust Euroopa Komisjoni soovituses 2003/361/EÜ):
a) tal on majandusaasta jooksul 50 või rohkem töötajat ning
b) tema aastane bilansimaht on üle 10 miljoni euro või tema aastakäive on üle 10 miljoni eurot.
Lisaks nendele piirmääradele vastamisele peab üksuse tegevusala olema loetletud kõnealuse lõike (ehk lõike 5) punktides 1–10. St siinkohal ei viidata lõikega 3 reguleeritavatele tegevusaladele, milles tegutsemine toob lõikes 3 nimetatud piirmäärade ületamisel kaasa üksuse lugemise üliolulisek. Lõike 5 kohaldamisel tuleb lähtuda üksnes lõikes 5 nimetatud tegevusvaldkondadest. Ühtlasi tähendab see seda, et nende tegevusvaldkondades saavadki tegutseda üksnes olulised, mitte aga üliolulised üksused.
Kommenteeritava punktiga seoses vt ka eespool esitatud selgitust Euroopa Komisjoni soovituse 2003/361/EÜ rakendamise kohta.

Eelnõukohane KüTSi § 3 lõike 5 punkt 1 sätestab olulise üksusena ettevõtja, kelle põhitegevus on jäätmekäitlus jäätmeseaduse tähenduses, sealhulgas järelevalve jäätmekäitluse üle ja jäätmete kõrvaldamiseks mõeldud jäätmekäitluskoha järelhooldus. Selline ettevõtja on oluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Kommenteeritavale punktile vastab NIS2-direktiivi II lisa punkti 2 esimene taane (*ettevõtjad, kes tegelevad Euroopa Parlamendi ja nõukogu direktiivi 2008/98/EÜ, mis käsitleb jäätmeid ja millega tunnistatakse kehtetuks teatud direktiivid (edaspidi* direktiiv 2008/98/EÜ*), artikli 3 punktis 9 määratletud jäätmekäitlusega, välja arvatud ettevõtjad, kelle põhitegevus ei ole jäätmekäitlus*).
Direktiivi 2008/98/EÜ artikli 3 punkti 9 kohaselt on jäätmekäitlus „jäätmete kogumine, vedu, taaskasutamine (sealhulgas sortimine) ja kõrvaldamine, sealhulgas nende toimingute järelevalve ning jäätmekõrvaldamiskohtade järelhooldus, sealhulgas vahendaja ja edasimüüja tegevus“. Selles definitsioonis on ka mõningaid termineid, mida avavad sama artikli punktid 1, 7, 8, 14, 15 ja 19:
„1) „jäätmed” – mis tahes ained või esemed, mille valdaja ära viskab, kavatseb ära visata või on kohustatud ära viskama;
7) „edasimüüja” – iga ettevõtja, kes tegutseb printsipiaalina jäätmeid ostes ja seejärel müües, kaasa arvatud need edasimüüjad, kes jäätmeid füüsiliselt ei valda;
8) „vahendaja” – iga ettevõtja, kes korraldab teiste nimel jäätmete taaskasutamist või kõrvaldamist, kaasa arvatud need vahendajad, kes jäätmeid füüsiliselt ei valda;
14) „töötlemine” – taaskasutamis- või kõrvaldamistoimingud, kaasaarvatud taaskasutamise või

kõrvaldamise eelne ettevalmistus;
15) „taaskasutamine" – mis tahes toimingud, mille peamiseks tulemuseks on jäätmete kasutamine kasulikul otstarbel selliselt, et nad asendavad teisi materjale, mida muidu oleks kasutatud teatava funktsiooni täitmiseks, või jäätmete ettevalmistamine selle funktsiooni täitmiseks kas tootmises või majanduses laiemalt. [Direktiivi 2008/98/EÜ] II lisas esitatakse taaskasutamistoimingute mitteammendav loetelu;
19) „kõrvaldamine" – mis tahes toiming, mis ei ole taaskasutamine, isegi kui toimingul on teisene tagajärg ainete või energia taasväärtustamise näol. [Direktiivi 2008/98/EÜ] I lisas esitatakse kõrvaldamistoimingute mitteammendav loetelu".
Jäätmeseaduse §-s 13 on jäätmekäitlus defineeritud kui „jäätmete kogumine, vedamine, taaskasutamine, sealhulgas sortimine, ja kõrvaldamine, sealhulgas vahendamine või edasimüümine". Selles definitsioonis loetletud tegevustega seoses on asjakohased sama seaduse § 14 (reguleerib jäätmete kogumist, liigiti kogumist ja vedamist), § 15 (reguleerib jäätmete taaskasutamist ja taaskasutamismooduseid), § 16 (reguleerib jäätmete töötlemist), § 17 (reguleerib jäätmete kõrvaldamist) ning kaudselt ka § 98^7 lõike 2 punktid 4 ja 5 (reguleerivad Keskkonnaametis registreerimist, kui isik korraldab vahendajana jäätmete kõrvaldamist või taaskasutamist teiste nimel või tegutseb jäätmete edasimüüjana).

Eelnõukohase KüTSi § 3 lõike 5 punktiga 2 nimetatakse oluliseks üksuseks ettevõtja, kes toodab aineid Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1907/2006, mis käsitleb kemikaalide registreerimist, hindamist, autoriseerimist ja piiramist (REACH) ning millega asutatakse Euroopa Kemikaaliamet, muudetakse direktiivi 1999/45/EÜ ja tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 793/93 ja komisjoni määrus (EÜ) nr 1488/94 ning samuti nõukogu direktiiv 76/769/EMÜ ja komisjoni direktiivid 91/155/EMÜ, 93/67/EMÜ, 93/105/EÜ ja 2000/21/EÜ (ELT L 396, 30.12.2006, lk 1–850), artikli 3 punkti 9 tähenduses ja turustab aineid või segusid kõnealuse määruse artikli 3 lõike 14 tähenduses, ning ettevõtja, kes toodab ainetest või segudest kõnealuse määruse artikli 3 punktis 3 määratletud tooteid. Selline ettevõtja on oluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi II lisa punkti 3 esimene taane (*ettevõtjad, kes tegelevad Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 1907/2006, mis käsitleb kemikaalide registreerimist, hindamist, autoriseerimist ja piiramist (REACH) ja millega asutatakse Euroopa Kemikaalide Agentuur ning muudetakse direktiivi 1999/45/EÜ ja tunnistatakse kehtetuks nõukogu määrus (EMÜ) nr 793/93, komisjoni määrus (EÜ) nr 1488/94 ning samuti nõukogu direktiiv 76/769/EMÜ ja komisjoni direktiivid 91/155/EMÜ, 93/67/EMÜ, 93/105/EÜ ja 2000/21/EÜ (edaspidi* määrus (EÜ) nr 1907/2006*), artikli 3 punktides 9 ja 14 osutatud ainete valmistamisega ning ainete või segude levitamisega, ning ettevõtjad, kes toodavad ainetest või segudest kõnealuse määruse artikli 3 punktis 3 määratletud tooteid*). Määruse (EÜ) nr 1907/2006 artikli 3 punktides 3, 9 ja 14 on defineeritud järgmised terminid, sh on selle teemaga seotud ka punktides 1 ja 12 sätestatud terminid:
„1. aine — looduslik või tootmismenetluse teel saadud keemiline element või selle ühendid koos püsivuse säilitamiseks vajalike ja tootmismenetlusest johtuvate lisanditega, välja arvatud lahustid, mida on võimalik ainest eraldada, mõjutamata aine püsivust või muutmata selle koostist;
3. toode — ese, millele antakse tootmise käigus teatud kuju, pinnaviimistlus või kujundus, mis määrab tema funktsiooni suuremal määral kui tema keemiline koostis;
9. tootja — ühenduses asutatud füüsiline või juriidiline isik, kes toodab ainet ühenduse piires;
12. turuleviimine — kolmandatele isikutele tasu eest või tasuta tarnimine või kättesaadavaks tegemine. Importi käsitatakse turuleviimisena;
14. levitaja — ühenduses asutatud füüsiline või juriidiline isik, kaasa arvatud jaemüüja, kes üksnes

ladustab ainet ja viib aine turule ainena või segu koostisainena kolmandate isikute jaoks“.
NIS2-direktiiv ei täpsusta seda, mis laadi ainete või toodetega on tegemist, st tegemist on igasuguste keemiliste ainetega, olgu need siis kas tööstuslikud kemikaalid või igapäevakasutuses olevad kemikaalid. Samas võib eeldada, et siinkohal on ainete valmistamise ning ainete või segude levitamise puhul mõeldud neid üksusi, kes peavad end määruse (EÜ) nr 1907/2006 kohaselt registreerima.

Eelnõukohane KüTSi § 3 lõike 5 punkt 3 sätestab olulise üksusena Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002 artikli 3 punktis 2 määratletud toidukäitlemisettevõtja, kes tegeleb hulgimüügi ning tööstusliku tootmise ja töötlemisega. Selline ettevõtja on oluline üksus, kui see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi II lisa i 4 esimene taane (*Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 178/2002, millega sätestatakse toidualaste õigusnormide üldised põhimõtted ja nõuded, asutatakse Euroopa Toiduohutusamet ja kehtestatakse toidu ohutusega seotud menetlused (edaspidi* määrus (EÜ) nr 178/2002*), artikli 3 punktis 2 määratletud toidukäitlemisettevõtjad, kes tegelevad hulgimüügi ning tööstusliku tootmise ja töötlemisega*).
Määruse (EÜ) nr 178/2002 artikli 3 punkti 2 kohaselt on toidukäitlemisettevõtja „avalik või eraõiguslik kasumit taotlev või kasumitaotluseta juriidiline isik, kes on seotud toidu ükskõik millisel tootmis-, töötlemis- või turustusetapil toimuva mis tahes tegevusega“. Selle definitsiooni kohaselt on tegemist ükskõik millise toidu tootmis-, töötlemis- või turustusetapis toimuva mis tahes tegevusega, kuid NIS2-direktiiv näeb ette, et NIS2-direktiivi kohaldamisalasse kuuluvad ainult hulgimüük, tööstuslik tootmine ja töötlemine. Sellest on kommenteeritava punkti sõnastamisel ka lähtutud. Eeldatavasti ei kuulu kommenteeritava punkti kohaldamisalasse näiteks jaemüük – see on sama määruse artikli 3 punkti 7 kohaselt „toidu käitlemine ja/või töötlemine ning toidu hoiustamine müügikohas või tarnimine lõpptarbijale, kaasa arvatud jaotusterminalid, toitlustusettevõtjad, tehasesööklad, asutuste toitlustusettevõtjad, restoranid ja muud samalaadsed toiduteenust pakkuvad ettevõtjad, kauplused, selvehallide jaotuskeskused ja hulgimüügipunktid“. Selles definitsioonis on mainitud ka hulgimüügipunkte, kuid sel asjaolul ei ole siinjuures tähtsust, kuna definitsiooni mõte tundub olevat, et see toit on mõeldud müümiseks lõpptarbijale, kes on sama määruse artikli 3 punkti 18 kohaselt „toidu tarbija, kes ei kasuta kõnealust toitu toidukäitlemistoimingus või sellega seotud tegevuses“.
Kui võrrelda termini „hulgimüük“ tähendust selle termini Eesti õigusaktides sätestatud tähendusega, siis see on müük isikule, kes ei ole tarbija tarbijakaitseseaduse tähenduses. Vt alkoholiseaduse § 3 lõike 1 punkt 4: „Alkoholi käitlemiseks loetakse selle toidugrupi suhtes teostatavad järgmised toimingud: müügiks pakkumine või müük ühelt ettevõtjalt teisele ettevõtjale või muule isikule, kes ei ole tarbija tarbijakaitseseaduse tähenduses (edaspidi hulgimüük)“. Sama lõike punkti 5 kohaselt on jaemüügiks „müügiks pakkumine, müük või mis tahes võlaõigusliku lepingu sõlmimine või mis tahes õiguslikul alusel majandustegevuse raames kättesaadavaks tegemine või üleandmine tarbijale tarbijakaitseseaduse tähenduses (edaspidi jaemüük)“. Turupraktikast lähtudes tuleb lisaks arvestada, et hulgimüügi puhul ei saa tegemist olla ka igasuguse juriidilisele isikule/asutusele suunatud müügiga, vaid eelkõige edasimüügi ja vahendusega tööstus- ja kaubanduslikele tarbijatele, asutustele ning organisatsioonidele.
Tööstusliku tootmise ja töötlemisega soovitakse hõlmata ainult suuremamahulisemat toidutootmist ja -töötlemist – seda tehakse seeläbi, et kommenteeritavas punktis sätestatud üksus peab vastama ka töötajate arvu ja aastase bilansimahu või aastakäibe poolest piirmääradele.
Kommenteeritava punktiga on seotud ka määruse (EÜ) nr 178/2002 artikli 3 punktis 16 defineeritud termin „tootmis- töötlemis- ja turustamisetapid“: „kõik etapid, kaasa arvatud import,

alates toidu esmatootmisest kuni selle hoiustamise, transpordi, müügi või lõpptarbijale tarnimiseni, ning vajaduse korral sööda importimine, tootmine, valmistamine, hoiustamine, transport, turustamine, müük ja tarnimine“.
Kommenteeritavas punktis mainitud tegevused (hulgimüük, tööstuslik tootmine ja töötlemine) on alternatiivid.

Eelnõukohane KüTSi § 3 lõike 5 punkt 4 sätestab olulise üksusena teatavate meditsiiniseadmete tootjad, v.a KüTSi § 3 lõike 3 punktis 6 nimetatud meditsiiniseadme tootjad. Täpsemalt on kõnealuse punktiga hõlmatud Euroopa Parlamendi ja nõukogu määruse (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (ELT L 117, 05.05.2017, lk 1–175), artikli 2 punktis 1 määratletud meditsiiniseadme tootja ning Euroopa Parlamendi ja nõukogu määruse (EL) 2017/746 *in vitro* diagnostikameditsiiniseadmete kohta ning millega tunnistatakse kehtetuks direktiiv 98/79/EÜ ja komisjoni otsus 2010/227/EL (ELT L 117, 05.05.2017, lk 176–332) artikli 2 punktis 2 määratletud *in vitro* diagnostikameditsiiniseadme tootja, välja arvatud kõnesoleva paragrahvi lõike 3 punktis 6 osutatud meditsiiniseadme tootja. Selline üksus on oluline üksus, kui see vastab ka käesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellega võetakse üle NIS2-direktiivi II lisa punkti 5 alapunkti a esimene taane (*Euroopa Parlamendi ja nõukogu määruse (EL) 2017/745, milles käsitletakse meditsiiniseadmeid, millega muudetakse direktiivi 2001/83/EÜ, määrust (EÜ) nr 178/2002 ja määrust (EÜ) nr 1223/2009 ning millega tunnistatakse kehtetuks nõukogu direktiivid 90/385/EMÜ ja 93/42/EMÜ (edaspidi* määrus (EL) 2017/745*), artikli 2 punktis 1 määratletud meditsiiniseadmeid tootvad üksused ning Euroopa Parlamendi ja nõukogu määruse (EL) 2017/746,* in vitro *diagnostikameditsiiniseadmete kohta ning millega tunnistatakse kehtetuks direktiiv 98/79/EÜ ja komisjoni otsus 2010/227/EL (edaspidi* määrus (EL) 2017/746*), artikli 2 punktis 2 määratletud* in vitro *diagnostikameditsiiniseadmeid tootvad üksused, välja arvatud [NIS2-direktiivi] I lisa punkti 5 viiendas taandes osutatud meditsiiniseadmeid tootvad üksused*).
Määruse (EL) 2017/745 artikli 2 punkti 1 kohaselt on meditsiiniseade „mis tahes instrument, aparaat, rakendus, tarkvara, implantaat, reagent, materjal või muu ese, mida võib kasutada eraldi või teistega kombineerituna, mille tootja on ette näinud inimeste puhul kasutamiseks ühel või mitmel järgmisel meditsiinilisel eesmärgil:
– haiguste diagnoosimiseks, ennetamiseks, seireks, prognoosimiseks, raviks või leevendamiseks;
– vigastuse või puude diagnoosimiseks, jälgimiseks, ravimiseks, leevendamiseks või kompenseerimiseks;
– kehaosa või füsioloogilise või patoloogilise protsessi või seisundi uurimiseks, asendamiseks või muutmiseks;
– inimkehast saadud proovide, sealhulgas loovutatud organite, vere ja kudede *in vitro* uurimiseks informatsiooni saamise eesmärgil;
ja mille kavandatud põhitoime inimkehas või -kehale ei ole farmakoloogiline, immunoloogiline või ainevahetuslik mõju avaldamine, kuid mille toimele võib nimetatud mõju kaasa aidata.
Samuti käsitatakse meditsiiniseadmena järgmisi tooteid:
– seadmed rasestumise ärahoidmiseks või soodustamiseks;
– seadmete puhastamiseks, desinfitseerimiseks või steriliseerimiseks ette nähtud tooted, millele on osutatud [määruse 2017/745] artikli 1 lõikes 4 ja käesoleva punkti esimeses lõigus“.
Määruse (EL) 2017/745 artikli 1 lõikes 4 on sätestatud: „[Määruses (EL) 2017/745] osutatakse meditsiiniseadmetele, meditsiiniseadmete abiseadmetele ning [määruse (EL) 2017/745] XVI lisas loetletud, mille suhtes [määrust (EL) 2017/745] lõike 2 alusel kohaldatakse, edaspidi kui

seadmetele“.
Määruse (EL) 2017/746 artikli 2 punktis 2 on *in vitro* diagnostikameditsiiniseade defineeritud kui: „meditsiiniseade, mis on reagent, reagentaine, kalibraator, kontrollaine, testkomplekt, instrument, aparatuur, vahend, tarkvara või süsteem, mida kasutatakse eraldi või teistega kombineerituna ja mille tootja on ette näinud kasutamiseks inimkehast saadud proovide, sealhulgas loovutatud vere ja kudede *in vitro* uurimiseks teabe saamiseks ühe või mitme järgmise nähtuse kohta:
a) füsioloogiline või patoloogiline protsess või seisund;
b) kaasasündinud füüsiline või vaimne puue;
c) eelsoodumus teatava tervisliku seisundi või haiguse tekkeks;
d) ohutuse ja kokkusobivuse kindlaksmääramiseks võimalikud retsipiendid;
e) ravivastuse või reaktsioonide prognoosimine;
f) ravimeetmete kindlaksmääramine või jälgimine.
In vitro diagnostikameditsiiniseadmetena käsitatakse ka proovianumaid“.
Proovianum on defineeritud sama artikli punktis 3 kui „vakumeeritud või vakumeerimata vahend, mille tootja on ette näinud spetsiaalselt inimkehast võetud proovide hoidmiseks ja säilitamiseks *in vitro* diagnostiliste uuringute eesmärgil“.

Eelnõukohase KüTSi § 3 lõike 5 punkti 5 kohaselt on oluline üksus Euroopa Liidu majanduse tegevusalade statistilise klassifikaatori NACE Revision 2 C jao osades 26, 27, 28, 29 ja 30 osutatud majandustegevusega tegelev ettevõtja. Seda eeldusel, et see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga kavandatakse üle võtta NIS2-direktiivi II lisa punkti 5 alapunkti b esimene taane (*ettevõtjad, kes tegelevad NACE Rev. 2 C jao osas 26 osutatud majandustegevusega*), punkti 5 alapunkti c esimene taane (*ettevõtjad, kes tegelevad NACE Rev. 2 C jao osas 27 osutatud majandustegevusega*), punkti 5 alapunkti d esimene taane (*ettevõtjad, kes tegelevad NACE Rev. 2 C jao osas 28 osutatud majandustegevusega*), punkti 5 alapunkti e esimene taane (*ettevõtjad, kes tegelevad NACE Rev. 2 C jao osas 29 osutatud majandustegevusega*) ja punkti 5 alapunkti f esimene taane (*ettevõtjad, kes tegelevad NACE Rev. 2 C jao osas 30 osutatud majandustegevusega*).
Kommenteeritavas punktis olevad ELi NACE Revision 2. klassifikaatori C jao viited on järgmised:
- osa 26: arvutite, elektroonika- ja optikaseadmete tootmine;
- osa 27: elektriseadmete tootmine;
- osa 28: mujal liigitamata masinate ja seadmete tootmine;
- osa 29: mootorsõidukite, haagiste ja poolhaagiste tootmine;
- osa 30: muude transpordivahendite tootmine.

Nagu ka eespool (vt eelnõukohane KüTSi § 3 lg 3 p 7) on ka kõnesoleva punkti puhul viidatud ELi NACE Revision 2. klassifikaatorile, mitte EMTAK 2008 klassifikaatorile. Ilmestamaks erinevusi EMTAK 2008 klassifikaatori ja NACE Revision 2 klassifikaatori vahel olgu toodud mõned näited:
a) NACE Rev. 2 C jao osa 26: 26.11 (pooljuhid on märgitud NACE-s, kuid EMTAKis pole; EMTAKis kuuluvad sellesse ossa ka „nõelhelipeade tootmine“ ja „päikesepaneelide tootmine elektri tootmiseks“; EMTAKis on „kiipkaartide tootmine“, mida pole NACEs); EMTAKi gruppi 262 kuuluvad ka „arvutite komplekteerimine ja montaaž tootja poolt kohapeal“ ning „sularahaautomaatide/kassaautomaatide/pangaautomaatide tootmine“; EMTAKi gruppi 263 kuuluvad ka „kodukeskjaamaseadmete (PBX) tootmine“ ja „WiFi seadmete tootmine“.
b) NACE Rev. 2 C jao osa 27: EMTAKis kuulub klassi 27311 veel „optiliste kiudude, kiukimpude tootmine“ ja „fiiberoptilise kaabli tootmine“; EMTAKi klassi 27321 kuulub ka „koaksiaalkaabli ja koaksiaalsete elektrijuhtmete tootmine“; EMTAKi klassi 27511 kuulub ka „tervisekapslite jaoks aurugeneraatorite tootmine“; EMTAKi klassi 27521 kuuluvad ka „päikesepatareide (paneelide)

tootmine sooja vee tootmiseks“ ja „priimuste tootmine“; EMTAKi klassi 27901 kuuluvad ka „mitteväärismetallist juhtmekanalite ja tarvikute tootmine“ ja „elektriliste välireklaamikastide tootmine“.
1. jaanuaril 2025 hakkas kehtima EMTAK 2025, mis asendab EMTAK 2008 ning selle koostamisel on lähtutud NACE Revision 2.1 klassifikaatorist.[55] Eespool (vt eelnõukohane KüTSi § 3 lg 3 p 7) on selgitatud, miks ei ole võimalik kasutada viidet EMTAK 2025 klassifikaatorile ega ka NACE Revision 2.1 klassifikaatorile ning need selgitused kehtivad ka siin.

Eelnõukohane KüTSi § 3 lõike 5 punkt 6 näeb olulise üksusena ette internetipõhise kauplemiskoha pidaja. Seda eeldusel, et see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi II lisa punkti 6 esimene taane (*internetipõhiste kauplemiskohtade pakkujad*). Termin „internetipõhine kauplemiskoht“ on defineeritud NIS2-direktiivi artikli 6 punktis 28, mis võetakse üle KüTSi § 2 punktiga 13.

Eelnõukohane KüTSi § 3 lõike 5 punkt 7 näeb olulise üksusena ette NIS2-direktiivi II lisa punkti 1 esimesele taande kohaselt (*Euroopa Parlamendi ja nõukogu direktiivi 97/67/EÜ, ühenduse postiteenuste siseturu arengut ja teenuse kvaliteedi parandamist käsitlevate ühiseeskirjade kohta (edaspidi* direktiiv 97/67/EÜ*), artikli 2 punktis 1a määratletud postiteenuste osutajad, sealhulgas kulleriteenuste osutajad*) postiteenuse osutaja, sealhulgas kulleriteenuste osutajad. Direktiivi 97/67/EÜ artikli 2 punktis 1a on postiteenuse osutaja defineeritud kui „ettevõtja, kes osutab ühte või mitut postiteenust“. Sellega on seotud ka sama direktiivi artikli 2 punktis 1 sätestatud termini „postiteenus“ definitsioon: „teenused, mis hõlmavad postisaadetise kogumist, sorteerimist, transporti ja jaotamist“.
NIS2-direktiivi põhjenduses 12 on postiteenuse osutajate, sh kullerpostiteenuse osutajate kohta märgitud järgmist:
(12) [Direktiivis 97/67/EÜ] määratletud postiteenuse osutajate, sealhulgas kullerpostiteenuse osutajate suhtes tuleks kohaldada [NIS2-direktiivi] juhul, kui nad osutavad vähemalt ühe postiteenuseahela etapi teenust, eeskätt kogumis-, sorteerimis- või jaotamisteenust, sealhulgas järeletulemise teenused, võttes arvesse nende võrgu- ja infosüsteemidest sõltuvuse määra. Transporditeenust, mida ei osutata ühegi nimetatud etapi raames, ei peaks käsitama postiteenusena.
Postiseaduse § 2 lõike 1 kohaselt on postiteenuse sisuks „adresseeritud postisaadetise edastamine majandustegevusena“ ning lõike 2 kohaselt on edastamine „protsess, mis hõlmab postisaadetise kogumist, sorteerimist, vedu ja saajale kättetoimetamist“. Postiseaduse § 4 lõige 1 sätestab postisaadetise sisu (sh sama paragrahvi lõiked 2–4 selgitavad seda) ning sama paragrahvi lõige 5 sisustab termini „postiteenus“ (sh sama paragrahvi lõiked 6–11 selgitavad seda). Postiseaduse § 22 lõike 1 kohaselt on postiteenuse osutaja „ettevõtja, kes osutab ühte või või mitut postiteenust“ ning et „ainult postisaadetiste vedu ei ole postiteenuse osutamine“.
NIS2-direktiiv hõlmab ka „kullerteenuste osutajad“, kuid ei täpsusta, keda nende all mõeldakse. Direktiivi 97/67/EÜ põhjendustes 17 ja 18 on kullerposti kohta märgitud:
(17) vähemalt 350 grammi kaaluvad kirjasaadetised moodustavad alla 2 % kirjadest ja alla 3 % avalik-õiguslike ettevõtjate laekumistest; hinna määramise põhimõtted (viiekordne põhihind) võimaldavad paremini vahet teha reserveeritud teenuse ja liberaliseeritud kullerposti teenuse vahel;
(18) silmas pidades asjaolu, et põhiline erinevus kullerposti ja universaalse postiteenuse vahel

[55] https://abiinfo.rik.ee/emtak/emtak2025

seisneb kullerposti teenustega kaasnevas ja klientidele tajutavas lisandväärtuses (olenemata selle vormist), saab tajutava lisaväärtuse kõige tõhusamalt kindlaks määrata nii, et võetakse arvesse lisahinda, mida kliendid on valmis maksma; see ei piira reserveeritud valdkonnas järgitava hinnapiirangu kohaldamist.
Direktiivis 97/67/EÜ esitatud selgituse puhul tuleb arvestada ka asjaoluga, et tegemist on 1997. aastast pärit direktiiviga, mida uuendati viimati 2015. aastal. Postiseaduses on kulleritega seoses nimetatud kullerpostisaadetise edastamist (vt postiseaduse § 4 lg 5 p 4 ja lg 9), kuid ei ole üheselt selge, kas see on sama mis kullerteenuse osutamine NIS2-direktiivi mõttes. Kui see on sama, siis see on juba hõlmatud postiteenuse osutaja terminiga.
Regionaal- ja Põllumajandusministeeriumil on ettevalmistamisel ka postiseaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seadus (eelnõude infosüsteemi toimik 25-0073),[56] mille planeeritav jõustumisaeg on 1. jaanuar 2026. Selle eelnõuga soovitakse muuta postiseaduse § 4 lõiget 9 järgmiselt:
(9) Kullerpostina edastatakse kirisaadetis või postipakk, mis vastab vähemalt neljale järgmisele tingimusele:
1) mis väljastatakse saajale või tema esindajale allkirja vastu või muu saaja tuvastamist võimaldava tunnuse alusel;
2) mis edastatakse kulleriga kiirel ja usaldusväärsel viisil;
3) mille saatjal on võimalus igal ajal saada teavet saadetise asukoha kohta selle teekonnal, sekkuda saadetise kättetoimetamisse ja vajaduse korral korraldada ümber selle edastamine;
4) mis kogutakse saatja elu- või asukohast;
5) mille puhul garanteeritakse kindlaksmääratud kuupäeval kohaletoimetamine;
6) mille kohta saadetakse postisaadetise saatjale kättetoimetamise kinnitus kokkulepitud viisil;
7) mis edastatakse vastavalt individuaalsele kokkuleppele ja kasutaja erinõuetele.

Eelnõukohane KüTSi § 3 lõike 5 punkt 8 näeb olulise üksusena ette sotsiaalmeediaplatvormi pakkuja. Seda eeldusel, et see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi II lisa punkti 6 kolmas taane (*sotsiaalvõrguteenuse platvormide pakkujad*). Termin „sotsiaalmeediaplatvorm“ on defineeritud NIS2-direktiivi artikli 6 punktis 33, mis võetakse üle KüTSi § 2 punktiga 26. Eelnõus on kasutatud NIS2-direktiivi termini asemel terminit „sotsiaalmeediaplatvormi pakkuja“. Selle termini valiku kohta vt selle termini selgitust.

Eelnõukohane KüTSi § 3 lõike 5 punkt 9 näeb olulise üksusena ette teadusasutuse. Seda eeldusel, et see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Sellele punktile vastab NIS2-direktiivi II lisa punkti 7 esimene taane (*teadusasutused*). Termin „teadusasutus“ on defineeritud NIS2-direktiivi artikli 6 punktis 41, mis võetakse üle KüTSi § 2 punktiga 27. Teadusasutusi käsitletakse ka NIS2-direktiivi põhjenduses 36:
(36) Teadusuuringutel on uute toodete ja protsesside väljatöötamisel võtmeroll. Paljusid neist tegevustest viivad ellu üksused, mis jagavad, levitavad või kasutavad oma teadusuuringute tulemusi ärilistel eesmärkidel. Need üksused võivad seega olla olulised osalejad väärtusahelates, mis muudab nende võrgu- ja infosüsteemide turvalisuse siseturu üldise küberturvalisuse lahutamatuks osaks. Teadusorganisatsioone tuleks käsitada nii, et need hõlmavad üksusi, mis pühendavad olulise osa oma tegevusest rakendusuuringutele või tootearendusele Majanduskoostöö ja Arengu Organisatsiooni 2015. aasta Frascati käsiraamatu „Guidelines for

[56] https://eelnoud.valitsus.ee/main/mount/docList/d4bbef7c-a51f-459c-b4f9-1ae428c881aa

Collecting and Reporting Data on Research and Experimental Development, with a view to exploiting their results for commercial purposes, such as the manufacturing and marketing of a product, process or the provision of a service" („Teadus- ja arendustegevuse andmete kogumise ja esitamise suunised, et kasutada nende tulemusi ärilistel eesmärkidel, näiteks toote, protsessi või teenuse tootmiseks või turustamiseks")[57] *tähenduses*.
Eelmainitud Frascati käsiraamatu 2. peatüki punktis 2.9, on „rakendusuuring" (ingl *applied research*) originaalne uuring, mis võetakse ette, et saada uusi teadmisi. See on siiski suunatud ennekõike konkreetse või praktilise eesmärgi saavutamisele või ülesande täitmisele. Eksperimentaalarendus (ingl *experimental development*) on süstemaatiline töö, mis tugineb uuringutest ja praktilisest kogemusest saadud teadmistele ning annab lisateadmisi ning mis on suunatud uute toodete või protsesside tootmisele või olemasolevate toodete või protsesside täiustamisele. Samas NIS2-direktiiv kitsendab seda definitsiooni, lisades tingimuse, et teadustegevusi tuleb ellu viia eesmärgiga kasutada nende tulemusi ärilistel eesmärkidel, näiteks toote või protsessi tootmiseks või arendamiseks, teenuse osutamiseks või turustamiseks.

Eelnõukohane KüTSi § 3 lõike 5 punkt 10 näeb olulise üksusena ette veebipõhise otsingumootori pakkuja. Seda eeldusel, et see vastab ka kõnesoleva lõike sissejuhatavas osas nimetatud piirmääradele.
Selle punktiga võetakse üle NIS2-direktiivi II lisa punkti 6 teine taane (*internetipõhiste otsingumootorite pakkujad*). Termin „internetipõhine otsingumootor" on defineeritud NIS2-direktiivi artikli 6 punktis 29, mis võetakse üle KüTSi § 2 punkti 33 muudatusega, kasutades terminit „veebipõhine otsingumootor". Põhjust, miks kommenteeritavas punktis kasutatakse terminit „veebipõhise", mitte „internetipõhise", on selgitatud KüTSi § 2 punkti 33 juures.

Eelnõukohase KüTSi § 3 lõikega 6 kavandatakse üle võtta NIS2-direktiivi artikli 2 lõike 1 teine lõik. Euroopa Komisjoni soovituse 2003/361/EÜ lisa artikli 3 lõige 4 kehtestab üldreegli, mille kohaselt ei ole ettevõtja väike- ega keskmise suurusega, kui 25% või rohkemat tema kapitalist või hääleõigusest kontrollivad otseselt või kaudselt, ühiselt või üksikult, üks või mitu avaliku sektori organisatsiooni (ingl *controlling public body*). Vt selle kohta ka nimetatud soovituse põhjendus 13: *(13) Vältimaks kunstlikku vahetegemist liikmesriigi erinevate avalik-õiguslike asutuste vahel ja arvestades vajadust õiguskindluse järele, peetakse vajalikuks kinnitada, et VKE ei ole ettevõte, mille kapitalist või hääleõigustest 25% või enam kontrollib avalik-õiguslik asutus*.
NIS2-direktiivi artikli 2 lõike 1 teine lõik täpsustab, et viidatud soovituse artikli 3 lõiget 4 ei arvestata NIS2-direktiivi puhul. Seetõttu tuleb KüTSi lisada sama nõue. Eeltoodu tõttu on eelnõu kohaselt võimalik mõnda üksust pidada väike- või keskmise suurusega ettevõtjaks, kui seda kontrollib (osaliselt) avaliku sektori organisatsioon, aga ainult siis, kui kommenteeritava paragrahvi lõike 2 punktis 9, lõike 3 sissejuhatavas osas, lõike 4 punktis 8 ja lõike 5 sissejuhatavas osas nimetatud tingimused (töötajate arv ja finantsnäitajad) on täidetud. NIS2-direktiiv ei näe ette nõudeid, kuidas tehakse kindlaks töötajate arv ja finantsnäitajad avaliku sektori organisatsioonide puhul. Need kuuluvad NIS2-direktiivi artikli 2 lõike 2 punkti f kohaselt NIS2-direktiivi kohaldamisalasse, olenemata üksuse suurusest. Soovitus 2003/361/EÜ ei ole mõeldud reguleerima seda, kuidas toimida kontrolli omavate avaliku sektori organisatsioonidega, ega sisalda selgeid reegleid selle kohta. Selle soovituse reeglite järgimine kontrolli omavate avaliku sektori organisatsioonide puhul (tuvastamaks nende seost partner- ja sidusettevõtjatega väike- või keskmise suurusega ettevõtjate puhul) tekitaks Euroopa Liidu liikmesriikide seas killustatust ja õiguslikku segadust. Seetõttu ei tule eraldiseisva kontrolli omava avaliku sektori üksuse töötajate

[57] https://www.oecd.org/en/publications/frascati-manual-2015_9789264239012-en.html

arvu ja finantsnäitajaid arvesse võtta, kui selgitatakse kommenteeritava lõike kohaselt välja väike- või keskmise suurusega ettevõtjate töötajate arvu ja finantsnäitajaid.
Vt lisaks kommenteeritava paragrahvi käsitluse alguses esitatud selgitusi soovituse 2003/361/EÜ kohta.

Eelnõukohane KüTSi § 3 lõige 7. Pärast eelnõu kooskõlastamist on lisatud eelnõusse lisareegel üksuse töötajate arvu, aastakäibe ja aastabilansimahu arvestamise kohta partner- ja sidusettevõtjate puhul.
Sellise reegli loomise võimalusele viitab NIS2-direktiivi põhjendus 16, mis on sõnastatud järgmiselt:
(16) Vältimaks seda, et üksusi, millel on partnerettevõtjad või mis on sidusettevõtjad, peetaks elutähtsateks[58] või olulisteks üksusteks, kui see oleks ebaproportsionaalne, on liikmesriikidel võimalik soovituse 2003/361/EÜ lisa artikli 6 lõike 2 kohaldamisel võtta arvesse üksuse oma partneritest või sidusettevõtjatest sõltumatuse määra. Eelkõige on liikmesriikidel võimalik võtta arvesse asjaolu, et üksus on oma partner- või sidusettevõtjatest sõltumatu teenuste osutamisel kasutatavate võrgu- ja infosüsteemide osas, ja teenuste osas, mida üksus osutab. /.../.
Arvestades eelnõu koostamisel aluseks võetud üldpõhimõtet, et riigisiseselt ei sätestatae NIS2-direktiivis ette nähtud miinimumnõuetest rangemaid nõudeid , on lõikesse 7 lisatud NIS2-direktiivi põhjenduses 16 sätestatud võimalus jätta partner- ja sidusettevõtjate töötajate arv ning käive- või bilansimaht arvestamata. Seeläbi on võimalik KüTSi kohaldamisalast välja jätta sellised üksused, kes vastaks töötajate arvu ning käibe- või bilansimahu poolest nõuetele just seetõttu, et partner- ja sidusettevõtja vastavad näitajad lisanduvad (st üksuse enda näitajate järgi piirmäärasid ei ületataks). Selline lahendus on nendele ettevõtjatele võrreldes kooskõlastamisele saadetud eelnõuga oluliselt soodsam.
Kommenteeritavas lõikes ette nähtud välistuse rakendamine on võimalik, kui asjaomasel partner- või sidusettevõtjal on otsustav mõju enda infotehnoloogiasüsteemide toimimise üle. Teisisõnu, kui nad on enda IT-lahenduste korraldamisel sõltumatud. Selline sõltumatus infotehnoloogiasüsteemide toimimise üle otsustamisel on olemas eelkõige siis, kui partner- ja sidusettevõtja saab omal vastutusel teha põhilisi otsuseid infotehnoloogiasüsteemide, selle komponentide ja protsesside üle. Kui partner- või sidusettevõtja on selliste otsuste tegemisel vaba, siis ei arvestata tema töötajate arvu, käivet ega bilansimahtu üksuse töötajate arvu ning käibe- või bilansinäitajate kindlakstegemisel. Kõnealuse välistuse kohaldamine ei tule aga kõne alla juhul, kui IT-lahendused on ette nähtud terves kontsernis ühetaoliselt, näiteks otsustab kõik IT-süsteemidega seotud küsimused emaettevõtja.

Eelnõukohase KüTSi §-ga 3[1] kavandatakse sätestada teenuseosutajate ja domeeninimede registreerimise teenuse osutaja kohustus teatada teatavad andmed, mille põhjal Riigi Infosüsteemi Amet koostab vastavate üksuste nimekirja.

Eelnõukohase KüTSi § 3[1] lõike 1 eesmärk on võtta üle NIS2-direktiivi artikli 3 lõike 4 esimene lõik. Selles on sätestatud teave, mida teenuseosutaja ja domeeninimede registreerimise teenuseid osutav üksus peab Riigi Infosüsteemi Ametile esitama. Siinjuures on ka asjakohane NIS2-direktiivi põhjendus 18:
(18) Selleks et tagada selge ülevaade [NIS2-direktiivi] kohaldamisalasse kuuluvatest üksustest, peaksid liikmesriigid koostama elutähtsate[59] ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste loetelu. Selleks peaksid liikmesriigid nõudma, et

[58] Eelnõus "ülioluliseks üksuseks".
[59] Eelnõus „ülioluliste üksuste".

üksused esitaksid pädevatele asutustele vähemalt järgmise teabe: nimi, aadress ja ajakohastatud kontaktandmed, sealhulgas üksuse e-posti aadressid, IP-vahemikud ja telefoninumbrid ning, kui see on kohaldatav, lisades osutatud asjaomane sektor ja allsektor ning, kui see on kohaldatav, selliste liikmesriikide loetelu, kus nad [NIS2-direktiivi] kohaldamisalasse kuuluvaid teenuseid osutavad. Selleks peaks komisjon Euroopa Liidu Küberturvalisuse Ameti (ENISA) abiga kehtestama põhjendamatu viivituseta teabe esitamise kohustusega seotud suunised ja vormid. Elutähtsate[60] ja oluliste üksuste ning domeeninimede registreerimise teenuseid osutavate üksuste loetelu koostamise ja ajakohastamise hõlbustamiseks peaks liikmesriikidel olema võimalik luua riiklikud mehhanismid, mis võimaldavad üksustel end ise registreerida. Kui registrid on riigi tasandil olemas, saavad liikmesriigid otsustada asjakohaste mehhanismide üle, mis võimaldavad [NIS2-direktiivi] kohaldamisalasse kuuluvaid üksusi kindlaks määrata.
Võrreldes ülevõetava NIS2-direktiivi vastava lõikega on eelnõukohasesse KüTSi § 3^1 lõike 1 punkti 1 lisatud andmeväljana ka „registrikood", kuna see aitab paremini eristada üksusi, ennekõike olukorras, kus üksus vahetab näiteks oma nime. Nimevahetusega ei kaasne üldjuhul registrikoodi muutumist – see toimub pigem ennekõike juriidilise isiku ühinemise või jagunemise käigus. Seetõttu on registrikood eeldatavasti püsivamat laadi tunnus kui üksuse nimi.
Kommenteeritava lõike punktides 3 ja 4 nimetatud teave tuleb esitada siis, kui see on asjakohane ehk seda ei pea kõik üksused esitama. Näiteks on punktiga 4 seotud teave vajalik mh ka selleks, et selgitada välja, kas ning mil määral on konkreetse teema käsitlemine või probleemi lahendamine Riigi Infosüsteemi Ameti või mõne muu liikmesriigi pädeva asutuse ülesanne.

Eelnõukohase KüTSi § 3^1 lõike 2 kohaselt koostab Riigi Infosüsteemi Amet iga kahe aasta järel teenuseosutajate ja domeeninimede registreerimise teenuse osutajate nimekirja. Sisu poolest vastab vaadeldav säte NIS2-direktiivi artikli 3 lõikele 3. Sarnane säte on kehtivas KüTSi § 3 lõikes 3. Seega ei ole tegemist Riigi Infosüsteemi Ametile pandava uue ülesandega. Vt ka eelnõuga kavandatavat KüTSi § 20 lõiget 1.

Eelnõukohane KüTSi § 3^1 lõige 3. Eelneva lõikega 2 on asjakohane koos vaadelda ka lõiget 3, mis sätestab, et lõikes 2 nimetatud teave on asutusesiseseks kasutamiseks mõeldud teave avaliku teabe seaduse tähenduses, Kommenteeritav lõige aitab tagada teenuseosutajate ja domeeninimede registreerimise teenuse osutajate nimekirja kui tundliku andmekogumi konfidentsiaalsust. Näiteks on selle nimekirja hulgas ka kõik hädaolukorra seaduse tähenduses elutähtsa teenuse osutajad ning need üksused kantakse tsiviiltoetuse registrisse (vt hädaolukorra seaduse § 38 lg 1^1 lause 1). Riigikaitseseaduse § 82^{14} lõike 1 kohaselt on tsiviiltoetuse register „andmekogu, milles peetakse arvestust riigikaitseks, vastuvõtva riigi toetuse osutamiseks, tsiviil-sõjaliseks koostööks, kõrgendatud kaitsevalmiduse, hädaolukorra, sõjaseisukorra ja muude sündmuste lahendamiseks vajalike vahendite ja nende kasutamiseks vajalike andmete, elutähtsa teenuse osutajate, riigikaitselisi ameti- ja töökohti omavate tööandjate, asja sundkasutusse võtmise ning asja sundvõõrandamise üle". Arvestades tsiviiltoetuse registri pidamise eesmärki, on selles sisalduvate andmete kogum vähemalt asutusesiseseks kasutamiseks mõeldud teave (vt näiteks avaliku teabe seaduse § 35 lg 1 p 3^1, 5, 6, 6^2 või 18^1). Sellele viitab ka tsiviiltoetuse registri põhimääruse[61] § 34 lõige 1, mis sätestab, et „Register on piiratud juurdepääsuga ja registriandmed on ette nähtud ainult ametialaseks kasutamiseks". Seega ei peaks teadmisvajaduseta isik mõnel muul moel (sh kõnealuses paragrahvis ette nähtud nimekirja kasutades) teada saama teavet, mis on kantud tsiviiltoetuse registrisse. Samas ei ole kõnealuses paragrahvis ette nähtud nimekirja kaitsmiseks muud sobivamat juurdepääsupiirangu alust. Seetõttu on selle nimekirja käsitamine asutusesiseseks

[60] Eelnõus „ülioluliste üksuste".
[61] https://www.riigiteataja.ee/akt/129102024008

kasutamiseks mõeldud teabena vajalik, et kaitsta selles nimekirjas olevat koondteavet ning seeläbi ka selles nimekirjas olevaid üksusi. Näiteks selleks, et pahatahtlikel isikutel oleks keerukam mõjutada ühiskonna toimimise seisukohast vajalike üksuste kasutatavaid võrgu- ja infosüsteeme ning seeläbi teenuseid, mis neid süsteeme kasutavad. See omakorda aitab tagada laiapindse riigikaitse eesmärke,[62] sealhulgas ühiskonna toimimist. Kommenteeritava lausega tekitatava juurdepääsupiirangu aluse kehtestamine lähtub seetõttu ka ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsiooni[63] artikli 3 lõike 1 esimese lõigu punktides a („tagada riigi julgeolek ja riigikaitse ning kaitsta rahvusvahelisi suhteid“) ja b („tagada avalik julgeolek“) sätestatud võimalustest piirata juurdepääsu ametlikele dokumentidele.

Eelnõukohase KüTSi § 3[1] lõikega 4 on kavas üle võtta NIS2-direktiivi artikli 3 lõike 4 teine lõik, st sätestatakse kohustus teavitada viivitamata ja igal juhul kahe nädala jooksul alates muudatuse kuupäevast lõike 1 kohaselt esitatud teabe muudatustest.

Eelnõukohase KüTSi § 3[1] lõigete 5–8 eesmärk on võtta üle NIS2-direktiivi artikli 3 lõige 5. Siinkohal vt ka eelnõuga kavandatavat KüTSi § 20 lõiget 2, samuti ka NIS2-direktiivi põhjendust 19:
(19) Liikmesriigid peaksid esitama komisjonile vähemalt igasse lisades osutatud sektorisse ja allsektorisse kuuluvate elutähtsate[64] ja oluliste üksuste arvu, samuti asjakohase teabe kindlaks määratud üksuste arvu kohta ja selle kohta, millise [NIS2-direktiivi] sätte põhjal need üksused kindlaks määrati ning millist liiki teenust nad osutavad. Liikmesriike julgustatakse vahetama komisjoniga teavet elutähtsate[65] ja oluliste üksuste kohta ning ulatusliku küberturbeintsidendi korral asjakohast teavet (näiteks asjaomase üksuse nimi).
Lõiked 5–8 ei hõlma domeeninimede registreerimise teenuse osutajaid – sellega seoses vt ka eelnõukohase KüTSi § 2 punkti 4 selgitust.

Eelnõukohane KüTSi § 3[1] lõige 9 on seotud NIS2-direktiivi artikli 3 lõike 4 kolmanda lõiguga. Selles lõigus viidatud Euroopa Komisjoni suunised ja vormid on esitatud komisjoni 14. septembri 2023. aasta teatises „Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 3 lõike 4 kohaldamise kohta 2023/C 324/02“.[66]

KüTSi §-i 4 tehtavad muudatused ja täiendused on seotud NIS2-direktiivi artikli 26 lõike 1 punkti b ja lõigete 2–4, aga ka artikli 27, ennekõike selle lõigete 2–5 ülevõtmisega. Termini „digitaalse teenuse osutaja“ tähenduse kohta vt eelnõukohane KüTSi § 2 punkt 2 ning selle selgitused. Termini „digitaalse teenuse osutaja esindaja“ tähenduse kohta vt eelnõukohane KüTSi § 2 punkt 3 ning selle selgitused. NIS2-direktiivi artikli 26 lõike 1 punkt b näeb ette, et digitaalse teenuse osutaja loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on tema peamine tegevuskoht Euroopa Liidus. Seega saab ainult jurisdiktsioonikohane liikmesriik nõuda digitaalse teenuse osutajalt kõnesolevas lõikes nimetatud andmeid. Sama põhimõte kehtib ka juhul, kui tuleb koostada teenuseosutajate ja domeeninimede registreerimise teenuse osutajate nimekiri.

Eelnõukohase KüTSi § 4 lõike 1 punktidega kavandatakse üle võtta NIS2-direktiivi artikli 27

[62] https://kaitseministeerium.ee/et/eesmargid-tegevused/laiapindne-riigikaitse
[63] https://www.riigiteataja.ee/akt/216092020001
[64] Eelnõus „ülioluliste üksuste“.
[65] Eelnõus „ülioluliste üksuste“.
[66] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0914%2801%29&qid=1728044123374

lõige 2. Nii nagu eelnõukohases KüTSi § 3^1 lõike 1 punktis 1, on ka KüTSi § 4 lõike 1 punkti 1 lisatud andmeväljana „registrikood“, kuna see aitab paremini eristada digitaalse teenuse osutajaid, ennekõike olukorras, kus digitaalse teenuse osutaja vahetab näiteks enda nime. Nimevahetusega ei kaasne üldjuhul registrikoodi muutumist – see toimub pigem ennekõike juriidilise isiku ühinemise või jagunemise käigus.

Eelnõukohaste KüTSi § 4 lõigetega 2–4 on kavas üle võtta NIS2-direktiivi artikli 26 lõiked 2–3, mis näevad ette konkreetses järjekorras tegevused, mille tulemusena selgitatakse välja digitaalse teenuse osutaja peamine tegevuskoht.
Digitaalse teenuse osutajad on selle riigi jurisdiktsiooni all, kus on nende peamine tegevuskoht Euroopa Liidus. NIS2-direktiivi põhjenduse 114 kohaselt on ainult ühel liikmesriigil vastav jurisdiktsioon nende üksuste puhul (tingimusel, et osutatakse ainult digitaalse teenuse osutajale omast teenust, mitte muid teenuseid, mis on NIS2-direktiivi, st KüTSi kohaldamisalas). Peamise tegevuskohana tuleks käsitada liikmesriiki, kus tehakse valdav osa otsustest küberturvalisuse riskijuhtimismeetmete kohta.
Ehk kui digitaalse teenuse osutaja peamine tegevuskoht on kommenteeritava paragrahvi lõike 2 kohaselt Eesti kui „Euroopa Liidu liikmesriik, kus turvameetmeid käsitlevad otsused valdavalt tehakse“, siis puudub vajadus peamise tegevuskoha väljaselgitamiseks lõigete 3 või 4 alusel. Kuid kui lõikes 2 sätestatud kriteerium ei ole asjakohane (nt võetakse turvameetmeid käsitlevad otsused vastu Ühendkuningriigis või Ameerika Ühendriikides), siis tuleb vaadata, kas tegemist on lõikes 3 kirjeldatud olukorraga; kui seegi ei ole asjakohane, siis kohaldub lõige 4.
Kui digitaalse teenuse osutaja leiab, et tema suhtes kohaldatakse järelevalve käigus õigustamatult mõne liikmesriigi õigusnormi, siis peab sellel üksusel olema võimalus selle liikmesriigi pädeva asutuse järelevalvemeedet vaidlustada. Mainitud järelevalvemeedet võidi kohaldada, kuna ühe liikmesriigi pädev asutus leidis, et tal on järelevalvepädevus olemas, kuid tegelikkuses ei pruukinud tal seda olla. Seetõttu tuleks ebaselguse vältimiseks kasutada nii NIS2-direktiivi artikli 27 lõike 1 alusel koostatud üksuste registrit kui ka NIS2-direktiivi artiklis 37 (eelnõukohases KüTSi §-s 17^3) sätestatud vastastikuse abi sätteid.

Eelnõukohase KüTSi § 4 lõike 5 mõte on sätestada erand sama paragrahvi lõigetest 2-4. Kommenteeritava lõikega kavandatakse üle võtta NIS2-direktiivi artikli 26 lõike 3 kolmas lause *(Kõnealust üksust loetakse selle liikmesriigi jurisdiktsiooni alla kuuluvaks, kus on esindaja tegevuskoht või kus ta on asutatud.).*

Eelnõukohase KüTSi § 4 lõikega 6 on kavas üle võtta NIS2-direktiivi artikli 27 lõige 3 (*Liikmesriigid tagavad, et lõikes 1 osutatud üksused teavitavad pädevat asutust viivitamata lõike 2 kohaselt esitatud teabe muutumisest, tehes seda igal juhul hiljemalt kolme kuu jooksul alates muudatuse kuupäevast.*) ning **KüTSi § 4 lõikega 7** NIS2-direktiivi artikli 27 lõige 4 (*Lõigetes 2 ja 3 osutatud teabe, välja arvatud lõike 2 punktis f osutatud teave, kättesaamisel edastab asjaomase liikmesriigi ühte kontaktpunkt selle põhjendamatu viivituseta ENISA-le.*). Sellega on seotud ka NIS2-direktiivi põhjendus 117:
(117) Selleks et tagada selge ülevaade domeeninimede süsteemi teenuse osutajatest, tippdomeeninimede registritest ja domeeninimede registreerimise teenuseid osutavatest üksustest[67], pilvandmetöötlusteenuse osutajatest, andmekeskusteenuse osutajatest, sisulevivõrgu

[67] Eelnõus „domeeninimede registreerimise teenuse osutajatest“.

pakkujatest[68], hallatud teenuse osutajatest[69] ja turbetarnijatest[70] ning internetipõhiste kauplemiskohtade[71], internetipõhiste otsingumootorite[72] ja sotsiaalvõrguteenuse platvormi pakkujatest[73], kes osutavad kogu liidus teenuseid, mille suhtes kohaldatakse [NIS2-direktiivi], peaks ENISA looma ja haldama selliste üksuste registrit, tuginedes liikmesriikidelt saadud teabele, mida saadakse, kui see on kohaldatav, riiklike mehhanismide kaudu, mis on loodud, et üksused saaksid end registreerida. Ühtsed kontaktpunktid peaksid edastama ENISA-le teabe ja kõik selle muudatused. Tagamaks, et kõnealusesse registrisse kantav teave on täpne ja täielik, võivad liikmesriigid esitada ENISA-le oma riiklikes registrites kõnealuste üksuste kohta olemasoleva teabe. ENISA ja liikmesriigid peaksid võtma meetmeid, et hõlbustada selliste registrite koostalitlusvõimet, tagades samal ajal konfidentsiaalse või salastatud teabe kaitse. ENISA peaks kehtestama asjakohased teabe klassifitseerimise ja haldamise protokollid, et tagada avalikustatud teabe turvalisus ja konfidentsiaalsus ning piirata juurdepääs sellisele teabele ning selle talletamine ja edastamine sihtkasutajatega.

Eelnõukohane KüTSi § 4 lõige 8 on seotud NIS2-direktiivi artikli 27 lõikega 1, mille kohaselt loob Euroopa Liidu Küberturvalisuse Amet tema esitatud teabe põhjal digitaalse teenuse osutajate registri ja haldab seda. NIS2-direktiivi artikli 27 lõike 1 teise lause kohaselt võimaldab Euroopa Liidu Küberturvalisuse Amet taotluse korral juurdepääsu NIS2-direktiivi kohastele pädevatele asutustele. Seetõttu tuleb tekitada ka vastava taotluse esitamise volitus Riigi Infosüsteemi Ametile. Kommenteeritava lõikega ei ole võimalik anda sarnast taotluse esitamise õigust KüTSi § 14 lõikes 5 nimetatud järelevalveasutustele, kuna nimetatud asutused ei tee riiklikku järelevalvet digitaalse teenuse osutajate üle.

Eelnõukohane KüTSi § 4 lõige 9 on seotud NIS2-direktiivi artikli 27 lõikega 5. Selles viidatud Euroopa Komisjoni suunised ja vormid on esitatud komisjoni 14.09.2023. a teatises „Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 3 lõike 4 kohaldamise kohta 2023/C 324/02“.[74]

Eelnõukohane KüTSi § 4 lõige 10 on seotud NIS2-direktiivi artikli 26 lõike 3 esimese ja teise lause ülevõtmisega. Need kaks lauset on järgmised: „Kui lõike 1 punktis b osutatud üksuse tegevuskoht ei ole liidus või ta ei ole seal asutatud, kuid ta pakub liidus oma teenuseid, määrab ta endale liidus esindaja. Esindaja tegevuskoht peab olema ühes nendest liikmesriikidest, kus teenuseid osutatakse, või ta peab olema seal asutatud.“ Lauseosa „lõike 1 punktis b osutatud üksuse“ all on mõeldud eelnõu kontekstis digitaalse teenuse osutajat ehk neidsamu üksusi, kelle suhtes kasutatakse eelnõus digitaalse teenuse osutaja mõistet.
Kommenteeritava lõikega on seotud ka NIS2-direktiivi põhjendus 116:
(116) Kui domeeninimede süsteemi teenuse osutaja, tippdomeeninimede register, domeeninimede registreerimise teenuseid osutav üksus[75], pilvandmetöötlusteenuse osutaja, andmekeskusteenuse

[68] Eelnõus „sisulevivõrguteenuse osutajatest“.
[69] Eelnõus „haldusteenuse osutajatest“.
[70] Eelnõus „infoturbeteenuse osutajatest“.
[71] Eelnõus „internetipõhise kauplemiskoha pidajatest“.
[72] Eelnõus „veebipõhiste otsingumootorite pakkujatest“.
[73] Eelnõus „sotsiaalmeediaplatvormi pakkujatest“.
[74] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0914%2801%29&qid=1728044123374
[75] Eelnõus „domeeninimede registreerimise teenuse osutaja“.

osutaja, sisulevivõrgu pakkuja[76], hallatud teenuse osutaja[77] või turbetarnija[78] või internetipõhiste kauplemiskohtade[79], internetipõhiste otsingumootorite[80] või sotsiaalvõrguteenuse platvormi pakkuja[81], kes ei ole asutatud liidus, osutab teenuseid liidus, peaks ta määrama endale liidus esindaja. Otsustamaks, kas kõnealune üksus pakub teenuseid liidu piires, tuleks kindlaks teha, kas üksus kavatseb osutada teenuseid ühes või mitmes liikmesriigis asuvatele isikutele. Seda, et liidus pääseb juurde üksuse või vahendaja veebisaidile, e-posti aadressile või muudele kontaktandmetele, või seda, et kasutatakse keelt, mida kasutatakse üldiselt kolmandas riigis, kus üksus on asutatud, tuleks pidada sellise kavatsuse kindlakstegemiseks ebapiisavaks. Samal ajal võivad asjaolud, nagu ühes või mitmes liikmesriigis üldiselt kasutatava keele või vääringu kasutamine, millega kaasneb võimalus tellida teenuseid selles keeles, või liidus paiknevate klientide või kasutajate mainimine, viidata sellele, et üksus kavatseb pakkuda teenuseid liidus. Esindaja peaks tegutsema üksuse nimel ning pädevatel asutustel või CSIRTil peaks olema võimalik esindajaga ühendust võtta. Esindaja tuleks määrata sõnaselgelt üksuse kirjaliku volitusega täitma [NIS2-direktiivis] sätestatud kohustusi, sealhulgas intsidentidest teatamise kohustust.

Eelnõukohaste KüTSi § 4 lõigete 11–12 eesmärk on üle võtta NIS2-direktiivi artikli 26 lõike 3 neljas lause (*Kui käesoleva lõike kohast esindajat liidus määratud ei ole, võib üksuse vastu, kes rikub [NIS2-direktiivi], võtta õiguslikke meetmeid iga liikmesriik, kus üksus teenuseid osutab*.) ja artikli 26 lõige 4 (*Esindaja määramine lõike 1 punktis b osutatud üksuse poolt ei piira õiguslike meetmete võtmist üksuse enda vastu.*). Need sätted tagavad, et digitaalse teenuse osutajal ei ole võimalik talle NIS2-direktiiviga seatud kohustustest esindaja määramisega (ega ka määramata jätmisega) kõrvale hoida ega kohustusi või vastutust esindajale delegeerida. Lõige 12 annab selguse, kas ja kes võib konkreetse teenuse osutaja suhtes võtta õiguslikke meetmeid, kui digitaalse teenuse osutaja ei ole endale esindajat määranud. Digitaalse teenuse osutaja esindaja kohta vt ka kavandatavat KüTSi § 2 punkti 2.

Eelnõukohane KüTSi § 4[1] on oma sisult uus paragrahv, mille eesmärk on tagada seaduse jõustumise järel selle subjektiks saavatele teenuseosutajatele sujuv üleminekuaeg alustamaks nõuete täitmist. Tegemist ei ole rakendussättega, vaid materiaalõigusliku sättega, kuna see hakkab reguleerima selliseid olukordi, kus üksus saavutab seaduse subjektile (teenuseosutajale või domeeninime registreerimise teenuse osutajale) vastavad tunnused kas a) vahetult seadusemuudatuse jõustumise mõjul, ilma et asjaomane subjekt oleks varem KüTSi kohaldamisalasse kuulunud, või b) pärast seadusemuudatuse jõustumist. See hõlmab kahte liiki olukordi – teenuseosutaja võib saada KüTSi subjektiks a) kas vahetult uute KüTSi reeglite jõustumise mõjul (nt tegemist on sellise subjektiga, kes kehtiva KüTSi kohaldamisalas ei ole, aga pärast seadusemuudatuse jõustumist on) või b) millalgi tulevikus, ka nt mitme aasta pärast (nt kui aasta pärast seaduse muudatuse jõustumist asutatakse uus ühing, kes hakkab tegutsema eelnõukohases KüTSi §-s 3 nimetatud valdkonnas ning kelle töötajate arv ja käive vastavad asjakohastele tunnustele, kui see on subjektiks saamise puhul ette nähtud). Praegustele eelnõukohastele KüTSi subjektidele kohalduvate nõuete täitmise aega reguleerivate sätete ehk üleminekusätete (rakendussätete) kohta vt eelnõukohase KüTSi § 28[1] selgitusi.
Kavandatav säte on üles ehitatud nii, et lõiked 1 ja 2 reguleerivad teenuseosutaja, domeenimede

[76] Eelnõus „sisulevivõrguteenuse osutaja“.
[77] Eelnõus „haldusteenuse osutaja“.
[78] Eelnõus „infoturbeteenuse osutaja“.
[79] Eelnõus „internetipõhise kauplemiskoha pidaja“.
[80] Eelnõus „veebipõhise otsingumootori pakkuja“.
[81] Eelnõus „sotsiaalmeediaplatvormi pakkuja“.

registreerimise teenuse osutaja ja digitaalse teenuse osutaja teavitamiskohustuse tekkimist Riigi Infosüsteemi Ameti ees, samuti digitaalse teenuse osutaja esindaja määramise kohustust. Need kohustused tuleb täita kolme kuu jooksul pärast seda, kui isik täidab KüTSi subjektsuse tunnused. Lõiked 3 ja 4 näevad ette üleüldise üleminekuaja teenuseosutajatele (sh digitaalse teenuse osutajatele) ja elutähtsa teenuse osutajatele. KüTSi nõuded tuleb esimesel korral täita kolme aasta jooksul alates teenuseosutaja (sh digitaalse teenuse osutaja) tunnustele vastavuse tekkimisest ja elutähtsa üksuse puhul hädaolukorra seaduse (või tulevikus tsiviilkriisi ja riigikaitse seaduse) kohaselt määratud tähtaja jooksul. Lõikes 5 täpsustatakse selguse huvides, et seda lõiget ei kohaldata KüTSi §-s 28^1 sätestatud juhul ehk nendele teenuseosutajatele, kes on juba kehtiva KüTSi subjektid ja kes saavad üleminekuaja eelnõukohases KüTSi §-s 28^1 sätestatu järgi.
Domeeninimede registreerimise teenuse osutaja puhul tuleb arvestada asjaoluga, et neile üksustele kohaldub ainult osa NIS2-direktiivi ja seeläbi ka ainult osa KüTSi nõudeid (vt eelnõukohase KüTSi § 2 p 4 selgitust). Samuti tuleb arvestada asjaoluga, et see üksus on üks nendest, mille suhtes kasutatakse terminit digitaalse teenuse osutaja (vt eelnõukohast KüTSi § 2 p 2).

Eelnõukohane KüTSi § 4^1 lõige 1. Teenuseosutaja ja domeeninimede registreerimise teenuse osutaja täidab eelnõu kohaselt KüTSi § 3^1 lõikes 1 sätestatava kohustuse kolme kuu jooksul alates teenuseosutaja või domeeninimede registreerimise teenuse osutaja tunnustele vastavuse tekkimisest. KüTSi § 3^1 lõikes 1 on kavas eelnõuga sätestada, millise teabe need üksused peavad Riigi Infosüsteemi Ametile esitama. Kommenteeritavas lõikes on neile selleks antud tähtaeg – kolm kuud alates teenuseosutaja või domeeninimede registreerimise teenuse osutaja tunnustele vastavuse tekkimisest. Selliselt on Riigi Infosüsteemi Ametil omakorda võimalik koostada eelnõukohases KüTSi § 3^1 lõikes 2 sätestatav nimekiri kõigist teenuseosutajatest ja domeeninimede registreerimise teenuse osutajatest.

Eelnõukohane KüTSi § 4^1 lõige 2. Digitaalse teenuse osutaja täidab eelnõu kohaselt KüTSi § 4 lõigetes 1 ja 10 sätestatavad kohustused kolme kuu jooksul alates digitaalse teenuse osutaja tunnustele vastavuse tekkimisest. Eelnõuga nähakse KüTSi § 4 lõikes 1 ette digitaalse teenuse osutaja kohustus esitada Riigi Infosüsteemi Ametile andmeid. Eelnõu kohaselt on kavas sätestada KüTSi § 4 lõikes 10 digitaalse teenuse osutaja kohustus määrata teatud juhtudel digitaalse teenuse osutaja esindaja, sealhulgas teha esindaja kontaktandmed püsivalt avalikult kättesaadavaks. Kommenteeritavas lõikes määratakse selleks tähtaeg – kolm kuud alates sellest, kui üksus hakkab vastama digitaalse teenuse osutaja tunnustele KüTSi tähenduses. Tähtaja määramisel on võetud eeskuju NIS2-direktiivi artikli 27 lõikest 3, mis võetakse üle eelnõukohase KüTSi § 4 lõikega 6. See sätestab digitaalse teenuse osutajale kohustuse teavitada eelnõukohases KüTSi § 4 lõikes 1 ette nähtud andmete muudatustest viivitamata, kuid hiljemalt kolm kuud pärast muudatuse kuupäeva. Edastatava teabe hulgas on ka teave digitaalse teenuse osutaja esindaja kontaktandmete kohta ehk need kohustused on omavahel seotud: kui on kohustus esindaja määrata ja seda pole tehtud, siis pole ka võimalik esitada esindaja kontaktandmeid. NIS2-direktiiv ei määra, mis tähtaja jooksul peab digitaalse teenuse osutaja enda esindaja määrama (vt NIS2-direktiivi artikli 26 lõiget 3, mis on kavas üle võtta eelnõukohase KüTSi § 4 lõikega 10), kuid kuna eelnõukohases KüTSi § 4 lõikes 1 oleva teabe uuendamine peab toimuma kolme kuu jooksul alates vastava muudatuse tegemisest, siis on siin kommenteeritavas lõikes lähtutud samast tähtajast.

Eelnõukohane KüTSi § 4^1 lõige 3. Kui eelnõu kohaselt näevad lõiked 1 ja 2 ette kohustuse esitada Riigi Infosüsteemi Ametile teavet kolme kuu jooksul alates eelnõukohase KüTSi tähenduses teenuseosutaja, domeeninimede registreerimise teenuse osutaja või digitaalse teenuse osutaja tunnustele vastavuse tekkimisest, siis lõige 3 sätestab uutele KüTSi subjektidele

(teenuseosutajatele ja domeeninimede registreerimise teenuse osutajatele) aja, mille jooksul peavad nad enda tegevuse KüTSi muude nõuetega kooskõlla viima ja neid järgima hakkama. Selleks on neil aega kolm aastat alates KüTSi subjektiks saamisest (teisisõnu hiljemalt kaks aastat ja üheksa kuud alates lõigetes 1 ja 2 sätestatud teavitamisest, kui seda tehakse viimasel päeval). Sätte eesmärk on anda uutele KüTSi subjektidele piisav aeg enda tegevus KüTSi reeglitega kooskõlla viia ning neid rakendada.
Eraldi väärib märkimist, et säte kohaldub eelnõu järgi teenuseosutajatele, sh digitaalse teenuse osutajatele. Digitaalse teenuse osutajate hulgas on ka domeeninimede registreerimise teenuse osutajad (vt eelnõus KüTSi § 2 p 2), kuid neile üksustele kohalduvad ainult mõned eelnõukohased KüTSi nõuded:

a) lähtudes NIS2-direktiivi artikli 3 lõigete 3–5 ülevõtmisest eelnõukohase KüTSi §-ga 3^1 – selle paragrahvi kontekstis tuleneb siin sätestatud esmase kohustuse (kontakt- jms andmete edastamise kohustus) esmakordne täitmine eelnõukohasest KüTSi § 4^1 lõikest 1;
b) lähtudes NIS2-direktiivi artiklite 26 ja 27 ülevõtmisest eelnõukohase KüTSi §-ga 4 – selle paragrahvi kontekstis tuleneb siin sätestatud esmaste kohustuste (kontakt- jms andmete edastamise kohustus, esindaja määramise kohustus) esmakordne täitmine eelnõukohasest KüTSi § 4^1 lõikest 2;
c) lähtudes NIS2-direktiivi artiklist 28, mille võttis üle Eesti Interneti SA nõukogu (vt seletuskirjale lisatud vastavustabeli selgitusi) – nende nõuete puhul puudub vajadus tekitada materiaalõiguslik säte, kuna see on seotud Eesti Interneti SAga sõlmitava .ee-domeenide akrediteeritud registripidaja teenuse osutamise lepinguga[82] ning selle täitmisega.

Kuna NIS2-direktiiv domeeninimede registreerimise teenuse osutajale muid nõudeid ei kehtesta ning nende kohustuste esmakordse täitmise tähtaeg tuleneb kommenteeritava paragrahvi lõigetest 1 ja 2, siis tulenevad nende edaspidise täitmise tähtajad kommenteeritava lõike teises lauses viidatud õigusnormidest. Seetõttu siin kommenteeritav lõige (kohustus täita muud KüTSi nõuded kolme aasta jooksul alates KüTSi subjekti tunnusele vastavuse tekkimisest) domeeninimede registreerimise teenuse osutajatele praktikas kohalduma ei hakka.

Eelnõukohane KüTSi § 4^1 lõige 4. Seda lõiget on kavas kohaldada elutähtsa teenuse osutajatele. Nemad peavad esimesel korral rakendama KüTSi eelnõu kohaseid nõudeid hädaolukorra seaduse § 38 lõike 1^3 punktis 3 sätestatud korras määratud tähtajal. Elutähtsa teenuse osutaja on eelnõu kohaselt KüTSi mõttes ülioluline üksus, kuid ta määratakse elutähtsa teenuse osutajaks hädaolukorra seaduse § 38 alusel haldusaktiga. Seetõttu on ka neile KüTSi reeglite kohaldamine seotud nende elutähtsa teenuse osutajaks määramisega hädaolukorra seaduse tähenduses. Hädaolukorra seaduse muudatusi on põhjalikumalt selgitatud hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu nr 426 SE seletuskirjas.[142]
Hädaolukorra seaduse § 38 lõike 1^3 kohaselt antakse selles haldusaktis, millega isik elutähtsa teenuse osutajaks määratakse, tähtaeg hädaolukorra seaduses ja muudes õigusaktides elutähtsa teenuse toimepidevuse tagamiseks sätestatud nõuete täitmiseks. Eelnõukohase KüTSi nõudeid võib pidada „muudes õigusaktides elutähtsa teenuse toimepidevuse tagamiseks sätestatud nõueteks“. Seetõttu on ka KüTSi kohaldamine elutähtsa teenuse osutajatele seotud hädaolukorra seaduse alusel haldusaktis määratava tähtajaga. Erandiks on üksnes kommenteeritava paragrahvi lõigetes 1 ja 2 sätestatavad kohustused. Need tuleb ka elutähtsa teenuse osutajal täita lõigetes 1 ja 2 sätestataval tähtajal ehk eelnõu kohaselt kolme kuu jooksul pärast seda, kui ta nendes lõigetes viidatud üksuse tunnused täidab.

[82] https://www.internet.ee/registripidaja/kuidas-saada-ee-akrediteeritud-registripidajaks

Nagu ka kõik teised kommenteeritava paragrahvi lõiked, hakkab ka see lõige kohalduma üksnes sellistele elutähtsa teenuse osutajatele, kes saavad elutähtsa teenuse osutajaks pärast kõnealuse eelnõuga kavandatava seaduse jõustumist. Nende puhul saab lähtuda üksnes hädaolukorra seaduse § 38 lõike 1^3 punktis 3 sätestatud tähtajast. Sellistele elutähtsa teenuse osutajatele, kes on juba praegu (st enne kavandatava seaduse jõustumist) elutähtsa teenuse osutajad või on selleks hädaolukorra seaduse § 38 lõike 1^3 alusel määratud enne kõnealusest eelnõust tulenevate muudatuste jõustumist, tuleb kohaldada eelnõukohase KüTSi § 28^1 lõigetes 3 ja 4 sätestatut.

Eelnõukohane KüTSi § 4^1 lõige 5. Kommenteeritav lõige on selgitava ja täpsustava iseloomuga, et tuua üheselt esile eelnõuga kavandatava KüTSi § 4^1 ja § 28^1 omavaheline seos. Paragrahvis 4^1 sätestatut ei kohaldata sellistele teenuseosutajatele, kellele eelnõu järgi kohaldatakse KüTSi §-s 28^1 sätestatut.

Eelnõukohase KüTSi § 5 pealkiri. KüTSi kehtivas versioonis on paragrahvi pealkiri „§ 5. Ühtne kontaktpunkt ja pädev asutus“, kuid seda pealkirja ei ole võimalik edaspidi kasutada, kuna praegu on KüTSi § 5 sisu seotud ennekõike Riigi Infosüsteemi Ametiga, kuid eelnõuga on kavas luua õigusnorme, mis on seotud ka muude valitsusasutustega. Paragrahvi kavandatavas uues pealkirjas ei tähista sõnapaar „pädevad asutused“ neid asutusi ainult NIS2-direktiivi artikli 8 lõike 1 tähenduses, vaid siin on mõeldud ka muid asjakohaseid valitsusasutusi.

Eelnõukohase KüTSi § 5 lõike 1 muudatusega kavandatakse anda Vabariigi Valitsusele volitus võtta vastu NIS2-direktiivi artiklis 7 nimetatud küberturvalisuse strateegia, mis võib olla muu õigusakti alusel koostatava dokumendi osa. Praktikas kuulub see digiühiskonna arengukava koosseisu, mille võtab vastu Vabariigi Valitsus.
Küberturvalisuse strateegia ületab seda koostava ministeeriumi pädevusvaldkondi, mistõttu on Vabariigi Valitsuse seaduse § 57 lõiget 3 arvestades antud küberturvalisuse strateegia vastuvõtmise kohustuse kehtestamise volitus Vabariigi Valitsusele.
Kommenteeritava lõikega antakse küberturvalisuse valdkonna eest vastutavale ministrile ülesanne koordineerida küberturvalisuse strateegia koostamist.

Eelnõukohase KüTSi § 5 lõike 2 kohaselt sätestab küberturvalisuse valdkonna eest vastutav minister määrusega riiklikku küberturvalisuse strateegiat puudutavad üksikasjad. Tegemist on volitusnormiga, mille eesmärk on vältida seaduse põhiteksti koormamist üksnes haldusesiseste protsesside ja nõuetega. Seetõttu võetaksegi valdav osa NIS2-direktiivi artiklis 7 sätestatust (sh **s**trateegia koostamise ulatus, tingimused ja elluviimise kord, mis hõlmavad ka uuendamise ja tulemushindamise korda**)** üle rakendusaktiga.
Vabariigi Valitsuse seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu nr 505 SE kohase seadusega liikusid 01.01.2025 Majandus- ja Kommunikatsiooniministeeriumist Justiits- ja Digiministeeriumisse digiühiskonna poliitika, avalike e-teenuste, digiarengu ja küberturvalisuse, riigi infosüsteemide, kesksete võrgu- ja infosüsteemide ning side ja telekommunikatsiooniga seotud ülesanded. Samuti liikusid Majandus- ja Kommunikatsiooniministeeriumi alt Justiits- ja Digiministeeriumi valitsemisalasse Riigi Infosüsteemi Amet, Riigi Info- ja Kommunikatsioonitehnoloogia Keskus, Riigi Infokommunikatsiooni Sihtasutus ning Eesti Interneti Sihtasutus.
Kommenteeritava lõikega on seotud ka NIS2-direktiivi põhjendused 48–57, 60 ja 97:
(48) Küberturvalisuse kõrge taseme saavutamiseks ja säilitamiseks peaksid [NIS2-direktiiviga] nõutavad riiklikud küberturvalisuse strateegiad koosnema sidusatest raamistikest, milles on esitatud strateegilised eesmärgid ja prioriteedid küberturvalisuse valdkonnas ning nende

saavutamiseks vajalik juhtimine. Need strateegiad võivad koosneda ühest või mitmest seadusandlikust või muust kui seadusandlikust aktist.
(49) Võrgu- ja infosüsteemide taristu, riistvara, tarkvara ja veebipõhiste rakenduste turvalisuse ning selliste ettevõtjate või lõppkasutajate andmete kaitsmiseks, millest üksused sõltuvad, luuakse alus küberhügieeni poliitikameetmetega. Küberhügieeni poliitikameetmed, mis koosnevad ühistest alustavadest, sealhulgas tarkvara ja riistvara uuendamine, salasõnade muutmine, uute paigalduste haldamine, administraatori õigustega juurdepääsukontode piiramine ja andmete varundamine, võimaldavad luua intsidentide või küberohtude puhuks valmisoleku ning üldise turvalisuse ja julgeoleku ennetava raamistiku. Liikmesriikide küberhügieeni poliitikameetmeid peaks jälgima ja analüüsima ENISA.
(50) Küberturvalisuse alane teadlikkus ja küberhügieen on liidu küberturvalisuse taseme tõstmiseks üliolulised, eelkõige seetõttu, et ühendatud seadmete arv kasvab pidevalt ja neid võetakse küberrünnete puhul üha enam sihtmärgiks. Tuleks teha pingutusi, et suurendada üldist teadlikkust selliste seadmetega seotud riskidest, samal ajal kui liidu tasandil tehtavad hindamised võiksid aidata tagada ühtse arusaama sellistest riskidest siseturul.
(51) Liikmesriigid peaksid ergutama uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamist, mis võiks parandada küberrünnete avastamist ja ennetamist ning ressursse küberrünnete vastu paremini suunata. Seepärast peaksid liikmesriigid sellise tehnoloogia kasutamise hõlbustamiseks soodustama oma riiklikes küberturvalisuse strateegiates teadus- ja arendustegevust, eelkõige seoses küberturvalisuse automatiseeritud või poolautomaatsete vahenditega, ning, kui see on kohane, jagama sellise tehnoloogia kasutajate koolitamiseks ja tehnoloogia täiustamiseks vajalikke andmeid. Uuendusliku tehnoloogia, sealhulgas tehisintellekti kasutamine peaks olema kooskõlas liidu andmekaitseõigusega, sealhulgas andmekaitsepõhimõtetega, nagu andmete täpsus, võimalikult väheste andmete kogumine, õiglus ja läbipaistvus ning andmeturve, näiteks tipptasemel krüpteerimine. Määruses (EL) 2016/679 sätestatud lõimitud ja vaikimisi andmekaitse nõuetest tuleb täielikult kinni pidada.
(52)Tänu avatud lähtekoodiga küberturbevahenditele ja -rakendustele võib tõusta avatuse tase ja need võivad mõjuda soodsalt tööstusinnovatsiooni tõhususele. Avatud standardid soodustavad turbevahendite koostalitlusvõimet, mis on kasulik tööstusvaldkonna sidusrühmade turvalisuse seisukohast. Avatud lähtekoodiga küberturbevahendid ja -rakendused võivad võimendada laiemat arendajate kogukonda, võimaldades tarnijate mitmekesistamist. Avatud lähtekoodiga võib kaasneda küberturvalisusega seotud vahendite kontrolliprotsessi suurem läbipaistvus ning kogukonna juhitav nõrkuste tuvastamise protsess. Seetõttu peaks liikmesriikidel olema võimalik edendada avatud lähtekoodiga tarkvara ja avatud standardite kasutuselevõttu, järgides poliitikat, mis on seotud avatud andmete ja avatud lähtekoodi kasutamisega läbipaistvusel põhineva turvalisuse osana. Avatud lähtekoodiga küberturbevahendite kasutuselevõttu ja kestlikku kasutamist edendavad tegevuskavad, on eriti olulised väikeste ja keskmise suurusega ettevõtjate jaoks, kellel on märkimisväärsed rakenduskulud, mida saaks vähendada, kui vajadust spetsiifiliste rakenduste või vahendite järele vähendataks.
(53) Kommunaalettevõtted on üha enam ühendatud linnade digivõrkudega, et parandada linnatranspordivõrke, ajakohastada veevarustust ja jäätmekäitlust ning suurendada valgustuse ja hoonete kütmise tõhusust. Need digitaliseeritud kommunaalettevõtted on küberrünnete vastu vähe kaitstud ja edukas küberrünne võib kodanikke nende ettevõtete omavahelise seotuse tõttu ulatuslikult kahjustada. Liikmesriigid peaksid oma riikliku küberturvalisuse strateegia raames välja töötama poliitika, milles käsitletakse selliste ühendatud või arukate linnade arendamist ja nende võimalikku mõju ühiskonnale.
(54) Viimastel aastatel on liit seisnud silmitsi lunavararünnete hüppelise kasvuga, mille puhul pahavara krüpteerib andmeid ja süsteeme ning nõuab vabastamiseks lunaraha maksmist.

Lunavararünnete sagenemist ja tõsidust võivad mõjutada mitmed tegurid, nagu erinevad ründemustrid, nagu lunavara kui teenusega seotud kuritegelikud ärimudelid ja krüptoraha, lunaraha nõudmised ja tarneahela rünnete sagenemine. Liikmesriigid peaksid oma riikliku küberturvalisuse strateegia raames välja töötama poliitika, milles käsitletakse lunavararünnete sagenemist.

(55) Sobiva raamistiku kõigi sidusrühmade vahel teadmiste vahetamiseks, parimate tavade jagamiseks ja vastastikuse mõistmise ühise taseme loomiseks võib pakkuda küberturvalisuse valdkonna avaliku ja erasektori partnerlus. Liikmesriigid peaksid edendama poliitikat, millega toetatakse küberturvalisuse valdkonna avaliku ja erasektori partnerluse loomist. Niisuguses poliitikas tuleks muu hulgas täpsustada, millised on avaliku ja erasektori partnerluse ulatus ja kaasatud sidusrühmad, juhtimismudel, olemasolevad rahastamisvõimalused ja osalevate sidusrühmade koostoime. Avaliku ja erasektori partnerluse raames saab võimendavalt kasutada erasektori üksuste eksperditeadmisi, et abistada pädevaid asutusi tänapäevaste teenuste ja protsesside arendamisel, sealhulgas teabevahetus, varajane hoiatamine, küberohtude ja intsidentidega seotud õppused, kriisiohje ning vastupanuvõime kavandamine.

(56) Liikmesriigid peaksid oma riiklikes küberturvalisuse strateegiates käsitlema väikeste ja keskmise suurusega ettevõtjate küberturvalisuse vajadusi. Liidus on väikeste ja keskmise suurusega ettevõtjate osakaal tööstus- ja äriturul suur ning neil on sageli raske kohaneda uute äritavadega üha rohkem ühendatud maailmas ja digitaalses keskkonnas, kus töötajad on kodutööl ja äritegevus toimub järjest rohkem interneti kaudu. Mõnedel väikestel ja keskmise suurusega ettevõtjatel on küberturvalisusega seoses sellised probleemid nagu vähene küberteadlikkus, kaugtöösüsteemide IT-turvalisuse puudumine, küberturvalisuse tagamiseks kasutatavate lahenduste suured kulud ja kõrgem ohutase, näiteks lunavaraga seoses, mille lahendamiseks nad peaksid saama suuniseid ja tuge. Väikestest ja keskmise suurusega ettevõtjatest on üha enam saamas tarneahela rünnete sihtmärk, sest nende küberturvalisuse riskijuhtimismeetmed ja ründehaldamine ei ole nii ranged ning asjaolu tõttu, et neil on piiratud turberessursid. Sellised tarneahela ründed ei mõjuta üksnes väikeseid ja keskmise suurusega ettevõtjaid ja nende tegevust, vaid võivad avaldada astmelist mõju ka üksustele, kellele nad tarnivad, põhjustades ulatuslikuma ründe. Liikmesriigid peaksid oma riiklike küberturvalisuse strateegiate kaudu aitama väikestel ja keskmise suurusega ettevõtjatel tarneahelates esinevaid probleeme lahendada. Liikmesriikidel peaks olema väikeste ja keskmise suurusega ettevõtjate jaoks riiklikul või piirkondlikul tasandil kontaktpunkt, mis kas annab väikestele ja keskmise suurusega ettevõtjatele suuniseid ja abi või suunab nad küberturvalisuse küsimustes suuniste ja abi saamiseks asjakohaste asutuste juurde. Liikmesriike julgustatakse osutama ka selliseid teenuseid nagu veebisaidi konfigureerimine ja logimise võimaldamine mikroettevõtjatele ja väikestele ettevõtjatele, kellel see võimekus puudub.

(57) Liikmesriigid peaksid oma riiklikes küberturvalisuse strateegiates laiema kaitsestrateegia osana võtma kasutusele aktiivse küberkaitse edendamise poliitika. Selle asemel et tegutseda reageerivalt, tähendab aktiivne küberkaitse võrguturbe rikkumise aktiivset ennetamist, avastamist, seiret, analüüsimist ja tagajärgede leevendamist, milleks kasutatakse nii ohvri võrgus kui ka sellest väljaspool olevaid võimalusi. See võiks hõlmata liikmesriike, kes pakuvad teatavatele üksustele tasuta teenuseid või vahendeid, sealhulgas iseteeninduskontrolle, avastamisvahendeid ja kõrvaldamisteenuseid. Võime ohuteavet ja -analüüse, kübertegevuse hoiatusi ja reageerimismeetmeid kiiresti ja automaatselt jagada ning mõista on ülioluline, et teha ühtseid pingutusi võrgu- ja infosüsteemide vastu suunatud rünnete tulemuslikuks ennetamiseks, avastamiseks ja vastumeetmete võtmiseks. Aktiivne küberkaitse põhineb kaitsestrateegial, millega välistatakse ründemeetmed.

(60) Liikmesriigid peaksid võtma koostöös ENISAga meetmeid, et nõrkuste[83] koordineeritud avalikustamist hõlbustada, kehtestades selleks asjakohase riikliku poliitika. Oma riikliku poliitika raames peaksid liikmesriigid kooskõlas oma õigusega püüdma võimalikult suures ulatuses lahendada probleeme, millega puutuvad kokku nõrkuste[84] valdkonnas uuringuid läbi viivad isikud, sealhulgas probleeme, mis on seotud nende võimaliku kriminaalvastutusega. Võttes arvesse, et mõnes liikmesriigis võib nõrkuste valdkonnas uuringuid läbi viivate füüsiliste ja juriidiliste isikute suhtes kohaldada kriminaal- ja tsiviilvastutust, soovitatakse liikmesriikidel võtta vastu suunised, mis käsitlevad infoturbeuurijate nende tegevuse eest vastutusele võtmisest loobumist ja tsiviilvastutusest vabastamist.

(97) Siseturg sõltub interneti toimimisest rohkem kui kunagi varem. Peaaegu kõigi elutähtsate[85] ja oluliste üksuste teenused sõltuvad interneti kaudu pakutavatest teenustest. Et tagada elutähtsate[86] ja oluliste üksuste pakutavate teenuste sujuv osutamine, on oluline, et kõikidel üldkasutatavate elektroonilise side võrkude pakkujatel[87] oleksid asjakohased küberturvalisuse riskijuhtimismeetmed ja et nendega seotud olulistest intsidentidest teataataks. Liikmesriigid peaksid tagama üldkasutatavate elektroonilise side võrkude turvalisuse säilimise ning oma eluliste julgeolekuhuvide kaitse sabotaaži ja spionaaži eest. Kuna rahvusvaheline ühenduvus edendab ja kiirendab liidu ja selle majanduse konkurentsipõhist digitaliseerimist, tuleks merealuseid sidekaableid mõjutavatest intsidentidest teavitada CSIRTi või, kui see on kohaldatav, pädevat asutust. Kui see on asjakohane, tuleks merealuste sidekaablite küberturvalisust riiklikus küberturvalisuse strateegias arvesse võtta ning see peaks hõlmama võimalike küberturvalisuse riskide kaardistamist ja leevendusmeetmeid, et tagada nende kaitse kõrgeimal tasemel.

Lisaks eeltoodule on kommenteeritava lõikega seotud ka komisjoni suunised NIS2-direktiivi artikli 4 lõigete 1 ja 2 kohaldamise kohta (2023/C 328/02).[88] Need suunised on seotud ennekõike eelnõukohase KüTSi § 1 lõike 4 (*lex specialis* võrreldes KüTSi nõuetega, nt DORA määrus) rakendamisega, kuid selles on ka esitatud selgitused riikliku küberturvalisuse strateegia kontekstis (peatükk III. Samaväärsuse tagajärjed, alapeatükk III. 2. Riiklik küberturvalisuse strateegia; suunise punktid 30–32):

30. Vastavalt [NIS2-direktiivi] artikli 7 lõikele 1 peab iga liikmesriik võtma vastu riikliku küberturvalisuse strateegia. Riiklik küberturvalisuse strateegia on liikmesriigi ühtne raamistik, mis näeb ette küberturvalisuse valdkonna strateegilised eesmärgid ja prioriteedid ning nende eesmärkide ja prioriteetide saavutamiseks vajaliku juhtimise kõnealuses liikmesriigis (vt [NIS2-direktiivi] artikli 6 punkt 4). Küberturvalisuse strateegia peab muu hulgas sisaldama eesmärke ja prioriteete, mis hõlmavad eelkõige direktiivi (EL) 2022/2555 I ja II lisas osutatud sektoreid. Lisaks peab see strateegia sisaldama juhtimisraamistikku nende eesmärkide ja prioriteetide, kaasa arvatud [NIS2-direktiivi] artikli 7 lõikes 2 osutatud poliitikameetmete saavutamiseks.

31. Peale selle on [NIS2-direktiivi] artikli 7 lõike 1 punktis c sätestatud, et riiklik küberturvalisuse strateegia peab sisaldama juhtimisraamistikku, milles selgitatakse asjaomaste sidusrühmade riikliku tasandi rolle ja kohustusi, mis toetavad [NIS2-direktiivi] kohaste pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide vahelist koostööd ja koordineerimist riiklikul tasandil, samuti nende organite ja valdkondlike liidu õigusaktide kohaste pädevate asutuste vahelist koordineerimist ja

[83] Eelnõus „turvahaavatavuste“.
[84] Eelnõus „turvahaavatavuste“.
[85] Eelnõus „ülioluliste üksuste“.
[86] Eelnõus „ülioluliste üksuste“.
[87] Eelnõus „üldkasutatava elektroonilise side võrgu teenuse osutajatel“.
[88] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0918%2801%29&qid=1751186614700

koostööd.
32. Seega ei puuduta [NIS2-direktiivi] artikli 7 kohane küberturvalisuse strateegia vastuvõtmise nõue küberturvalisuse nõudeid, mis on elutähtsate[89] ja oluliste üksuste suhtes kehtestatud vastavalt nimetatud direktiivi artiklitele 21 ja 23, ega selle direktiivi artikli 4 lõigete 1 ja 2 nõuete kohaselt VII peatükis sätestatud järelevalve- ja täitmise tagamise sätteid. Artikli 7 asjaomaseid sätteid tuleks kohaldada ka edaspidi nende sektorite, allsektorite ja üksuste liikide suhtes, mille jaoks on olemas valdkondlikud liidu õigusaktid [NIS2-direktiivi] artikli 4 tähenduses.
Sama suunise liites on DORA määruse selgituste punktis 2 eelviimane lause: *Liikmesriigid peaksid jätkuvalt kaasama finantssektori oma küberturvalisuse strateegiatesse.*

Eelnõukohane KüTSi § 5 lõige 3 on seotud NIS2-direktiivi artikli 14 lõike 3 esimese lausega (*Koostöörühma moodustavad liikmesriikide, komisjoni ja ENISA esindajad.*) ning artikli 16 lõike 2 ülevõtmisega. Kommenteeritava lõikega on kavas anda asjaomased volitused nii Justiits- ja Digiministeeriumile kui ka Riigi Infosüsteemi Ametile, kuna Vabariigi Valitsuse seaduse § 44 lõike 1 kohaselt on riiki volitatud esindama valitsusasutus või muu riigiasutus seadusest, oma põhimäärusest ja teistest õigusaktidest tulenevate ülesannete täitmisel.

Eelnõukohane KüTSi § 5 lõige 4 on seotud NIS2-direktiivi artikli 8 lõigete 1 ja 3, artikli 9 lõike 1, artikli 10 lõike 1, artikli 12 lõike 1 ning artikli 15 ülevõtmisega. Kommenteeritava lõikega on seotud ka NIS2-direktiivi põhjendused 38–40 ja 68–73. Lõikega on kavas anda Riigi Infosüsteemi Ametile nende artiklite alusel asjaomaseid ülesandeid.
(38) Arvestades liikmesriikide juhtimisstruktuuride erinevusi ning selleks, et kaitsta juba kehtivat valdkondlikku korda või liidu reguleerivaid ja järelevalveasutusi, peaks liikmesriikidel olema võimalik määrata küberturvalisuse ja [NIS2-direktiivi] kohaste järelevalveülesannete eest vastutavaks vähemalt ühe riikliku pädeva asutuse või see asutada.
(39) Et hõlbustada ametiasutuste piiriülest koostööd ja suhtlust ning [NIS2-direktiivi] tõhusalt rakendada, on vaja, et iga liikmesriik määraks ühtse kontaktpunkti, kes vastutab võrgu- ja infosüsteemide turvalisuse küsimuste koordineerimise ning liidu tasandil tehtava piiriülese koostöö eest.
(40) Ühtsed kontaktpunktid peaksid tagama tõhusa piiriülese koostöö teiste liikmesriikide asjaomaste asutustega ning asjakohasel juhul komisjoni ja ENISAga. Seepärast tuleks ühtsetele kontaktpunktidele teha ülesandeks edastada CSIRTi või pädeva asutuse taotlusel teated piiriülese mõjuga oluliste intsidentide kohta teiste mõjutatud liikmesriikide ühtsetele kontaktpunktidele. Riiklikul tasandil peaksid ühtsed kontaktpunktid võimaldama sujuvat valdkondadevahelist koostööd teiste pädevate asutustega. Ühtsed kontaktpunktid võiksid olla ka määruse (EL) 2022/2554 kohaste pädevate asutuste edastatava, finantssektori ettevõtjatega seotud intsidente käsitleva asjakohase teabe adressaadid ning, kui see on asjakohane, peaks neil olema võimalik edastada kõnealune teave CSIRTidele või [NIS2-direktiivi] kohastele pädevatele asutustele.
(68) Liikmesriigid peaksid aitama kaasa komisjoni soovituses (EL) 2017/1584 ette nähtud küberturvalisuse kriisidele reageerimise ELi raamistiku loomisele olemasolevate koostöövõrgustike, eelkõige Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule (EU-CyCLONe), CSIRTide võrgustiku ja koostöörühma tegevuse kaudu. EU-CyCLONe ja CSIRTide võrgustik peaksid tegema koostööd menetluskorra alusel, milles määratakse kindlaks kõnealuse koostöö üksikasjad, ning vältima ülesannete dubleerimist. EU-CyCLONe menetluskorras tuleks täpsustada võrgustiku toimimist puudutav kord, muu hulgas rollid, koostööviisid, teiste asjaomaste osalejatega suhtlemine, teabevahetuse vormid ja kommunikatsioonivahendid. Liidu tasandi

[89] Eelnõus „üliloluliste üksuste“.

kriisiohje puhul peaksid asjaomased pooled lähtuma nõukogu rakendusotsuses (EL) 2018/1993 sätestatud kriisidele poliitilist reageerimist käsitlevast ELi integreeritud korrast (edaspidi „IPCRi kord“). Komisjon peaks selleks rakendama üldise kiirhoiatussüsteemi ARGUS kõrgetasemelise valdkondadevahelise kriisikoordineerimise menetlusprotsessi. Kui kriisil on oluline välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, tuleks käivitada Euroopa välisteenistuse kriisidele reageerimise mehhanism.

(69) Soovituse (EL) 2017/1584 lisa kohaselt tuleks ulatusliku küberturbeintsidendina mõista intsidenti, mille põhjustatud häired on niivõrd laialdased, et ühe liikmesriigi suutlikkusest nendega toimetulekuks ei piisa, või millel on märkimisväärne mõju vähemalt kahele liikmesriigile. Olenevalt nende põhjusest ja mõjust võivad ulatuslikud küberturbeintsidendid eskaleeruda ning muutuda täieulatuslikuks kriisiks, mis takistab siseturu tõrgeteta toimimist või kujutab endast mitme liikmesriigi või kogu liidu üksustele või kodanikele tõsist avaliku julgeoleku- või turvalisusriski. Võttes arvesse selliste intsidentide ulatuslikku haaret ja (enamikul juhtudel) piiriülest laadi, peaksid liikmesriigid ning asjaomased liidu institutsioonid, organid ja asutused tegema koostööd nii tehnilisel, operatiiv- kui ka poliitilisel tasandil, et reageerimist liidu ulatuses nõuetekohaselt koordineerida.

(70) Liidu tasandi ulatuslike küberturbeintsidentide ja kriiside puhul tuleb kiire ja tõhusa reageerimise tagamiseks võtta koordineeritud meetmeid, kuna sektorite ja liikmesriikide omavaheline sõltuvus on väga suur. Kübervastupidavusvõimeliste võrgu- ja infosüsteemide olemasolu ning andmete kättesaadavus, konfidentsiaalsus ja terviklus on väga olulised liidu julgeoleku ning liidu kodanike, ettevõtjate ja institutsioonide kaitsmiseks intsidentide ja küberohtude eest ning samuti selleks, et suurendada üksikisikute ja organisatsioonide usaldust liidu võimekuse vastu edendada ja kaitsta üleilmset, avatud, vaba, stabiilset ja turvalist küberruumi, mis põhineb inimõigustel, põhivabadustel, demokraatial ja õigusriigil.

(71) EU-CyCLONe peaks ulatuslike küberturbeintsidentide ja kriiside korral toimima vahendajana tehnilise ja poliitilise tasandi vahel ning tõhustama operatiivtasandi koostööd ja toetama otsuste tegemist poliitilisel tasandil. Võttes arvesse komisjoni pädevust kriisiohje valdkonnas, peaks EU-CyCLONe koostöös komisjoniga tuginema CSIRTide võrgustiku järeldustele ja kasutama oma võimekust, et koostada ulatuslike küberturbeintsidentide ja kriiside mõjuanalüüs.

(72) Küberründed on oma olemuselt piiriülesed ning oluline intsident võib häirida ja kahjustada elutähtsaid teabetaristuid, millest sõltub siseturu sujuv toimimine. Kõigi asjaomaste osalejate rolli käsitletakse soovituses (EL) 2017/1584. Lisaks vastutab komisjon Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL loodud liidu elanikkonnakaitse mehhanismi raames üldiste valmisolekumeetmete eest, mis hõlmavad hädaolukordadele reageerimise koordineerimiskeskuse ning ühise hädaolukordade side- ja infosüsteemi haldamist, olukorrateadlikkuse ja analüüsivõime säilitamist ja edasiarendamist ning liikmesriigi või kolmanda riigi abitaotluse korral eksperdirühmade mobiliseerimise ja lähetamise võimekuse loomist ja haldamist. Komisjon vastutab ka rakendusotsuse (EL) 2018/1993 kohase IPCRi korra analüüsiaruannete esitamise eest, muu hulgas seoses küberturvalisuse olukorrateadlikkuse ja valmisolekuga, samuti olukorrateadlikkuse ja kriisidele reageerimisega põllumajanduse, ebasoodsate ilmastikutingimuste, konfliktide kaardistamise ja prognooside, loodusõnnetuste varajase hoiatamise süsteemide, tervisealaste hädaolukordade, nakkushaiguste seire, taimetervise, keemiliste ainetega seotud juhtumite, toidu- ja söödaohutuse, loomatervise, rände, tolli, tuumaavariide ja kiirguslike avariiolukordade ning energeetika valdkonnas.

(73) Kui see on asjakohane, võib liit kooskõlas ELi toimimise lepingu artikliga 218 sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldab neil osaleda ja korraldada osalust mõningates koostöörühma, CSIRTide võrgustiku ning EU-CyCLONe tegevuses. Selliste lepingutega tuleks tagada liidu huvid ja piisaval tasemel

andmekaitse. See ei tohiks välistada liikmesriikide õigust teha nõrkuste haldamisel ja küberturvalisuse riskijuhtimisel koostööd kolmandate riikidega, hõlbustades liidu õiguse kohast teatamist ja üldist teabevahetust.

Eelnõukohane KüTSi § 5 lõige 5 on seotud NIS2-direktiivi artikli 8 lõike 3 ülevõtmisega, et täpsustada kehtiva õiguse (vt eelnõus KüTSi § 14 lõiget 5) olukorda. Selle tulemusena on selge, kuidas suhestub julgeolekuasutus NIS2-direktiivi ning selle rakendamisega. Eelnõu kohaselt annab julgeolekuasutus vajalikku infot Riigi Infosüsteemi Ametile (vt eelnõus KüTSi § 17^4), et viimane saaks enda ülesandeid täita nii riigisiseselt kui ka riigiväliste koostööpartnerite suhtes.

Eelnõukohase KüTSi § 5^2 lisamine on seotud Euroopa Komisjoni 11. märtsi 2024. a delegeeritud määruse (EL) 2024/1366 rakendamisega ehk selle artiklite 4 ja 39–41 sätete täpsustamisega Eestis.

Eelnõukohane KüTSi § 5^2 lõige 1 on seotud delegeeritud määruse artikli 4 lõikega 1, mille sisu on järgmine:
1. Niipea kui võimalik ja hiljemalt 13. detsember 2024 määrab iga liikmesriik ühe riikliku või reguleeriva asutuse, kes vastutab talle [delegeeritud määrusega (EL) 2024/1366] antud ülesannete täitmise eest (edaspidi „pädev asutus“). Kuni [delegeeritud määrusest (EL) 2024/1366] tulenevate ülesannete täitmiseks pole pädevat asutust määratud, täidab [delegeeritud määruse (EL) 2024/1366] kohaseid pädeva asutuse ülesandeid liikmesriigi poolt direktiivi (EL) 2019/944 artikli 57 lõike 1 kohaselt määratud reguleeriv asutus.
Direktiivi (EL) 2019/944 artikli 57 lõike 1 kohaselt määratud reguleeriv asutus Eestis on Konkurentsiamet, kellel praegu puudub küberturvalisuse tagamise kontrolliga seotud kompetents, mistõttu on kasulikum, et niisuguse ülesande täitmiseks pädeva asutuse (kelleks saab loogilis-praktilistel kaalutlustel olla eelkõige Riigi Infosüsteemi Amet) nimetab käskkirjaga riikliku küberturvalisuse valdkonna eest vastutav minister.

Eelnõukohane KüTSi § 5^2 lõige 2 on seotud delegeeritud määruse (EL) 2024/1366 artikli 4 lõikes 3 nimetatud võimalusega ülesandeid, v.a sama määruse artiklis 5 loetletud ülesanded, teisele riigi ametiasutusele edasi delegeerida.
Kommenteeritud paragrahvi lõigetega on seotud ka delegeeritud määruse (EL) 2024/1366 artikkel 5, mille sisu on järgmine:
Artikkel 5. Asjaomaste asutuste ja organite koostöö riigi tasandil
Pädevad asutused tagavad asjakohase koostöö küberturvalisuse eest vastutavate pädevate asutuste, küberkriiside ohjamise asutuste, riikide reguleerivate asutuste, riskivalmiduse eest vastutavate pädevate asutuste ja CSIRTide vahel ning koordineerivad seda koostööd, et täita käesolevas määruses sätestatud asjakohaseid kohustusi. Pädevad asutused koordineerivad oma tegevust ka teiste liikmesriikide määratud organite või asutustega, et tagada tõhusad menetlused ning vältida ülesannete ja kohustuste dubleerimist. Pädevatel asutustel peab olema võimalik anda asjaomastele riikide reguleerivatele asutustele korraldus küsida ACERilt arvamust vastavalt artikli 8 lõikele 3.
ACER on lühend, mis eesti keeles tähendab Euroopa Liidu energeetikasektorit reguleerivate asutuste koostöö ametit.

Eelnõukohane KüTSi § 5^2 lõige 3 on seotud delegeeritud määruse (EL) 2024/1366 artikli 39 lõikes 1, artikli 40 lõikes 4 ning artikli 41 lõigetes 1 ja 2 sätestatud ülesannetega, et tekitada volitus need ülesanded vajaduse korral edasi volitada määruse (EL) 2019/943 artikli 35 kohaselt asutatud piirkondlikule koordineerimiskeskusele. Kommenteeritava lõikega ei ole kavas sätestada kohustus

need ülesanded edasi volitada, vaid võimalus, et Vabariigi Valitsus sellise volituse annab.
Kommenteeritava lõikega seotud asjakohased sätted on:
a) delegeeritud määruse (EL) 2024/1366 artikli 39 lõiked 1 ja 4:
Artikkel 39. Küberrünnete avastamine ja nendega seotud teabe käsitlemine
1. Ülisuure ja suure mõjuga üksused arendavad asjaomase pädeva asutuse, ENTSO-E ja Euroopa Liidu jaotusvõrguettevõtjate üksuse toetusel välja vajaliku võime kindlakstehtud küberrünnete käsitlemiseks. Ülisuure ja suure mõjuga üksusi võib toetada nende liikmesriigis kindlaks määratud CSIRT osana CSIRTidele [NIS2-direktiivi] artikli 11 lõike 5 punktiga a antud ülesandest. Ülisuure ja suure mõjuga üksused rakendavad tõhusaid protsesse, et teha kindlaks ja liigitada küberründeid ning reageerida rünnetele, mis mõjutavad või võivad mõjutada piiriüleseid elektrivooge, et minimeerida nende küberrünnete mõju.
4. Liikmesriigid võivad lõikes 1 osutatud ülesanded delegeerida ka määruse (EL) 2019/943 artikli 37 lõike 2 kohastele piirkondlikele koordineerimiskeskustele.
ENTSO-E on lühend, mis eesti keeles tähendab Euroopa elektri põhivõrguettevõtjate võrgustikku.
b) delegeeritud määruse artikli 40 lõiked 4 ja 5:
Artikkel 40. Kriisiohje
4. Ülisuure ja suure mõjuga üksused arendavad ja hoiavad oma käsutuses suutlikkust, sisesuuniseid, valmisolekukavasid ja töötajaid, et osaleda piiriüleste kriiside avastamises ja leevendamises. Üheaegsest elektrikriisist mõjutatud ülisuure või suure mõjuga üksus uurib koos oma pädeva asutusega sellise kriisi algpõhjust, et teha kindlaks, kuivõrd on kriis seotud küberründega.
5. Liikmesriigid võivad lõikes 4 sätestatud ülesanded delegeerida ka määruse (EL) 2019/943 artikli 37 lõike 2 kohastele piirkondlikele koordineerimiskeskustele.
c) delegeeritud määruse artikli 41 lõiked 1, 2 ja 4:
Artikkel 41. Küberkriisi ohjamise ja kriisile reageerimise kavad
1. 24 kuu jooksul pärast seda, kui ACERile on teatavaks tehtud kogu liitu hõlmav riskihindamisaruanne, töötab ACER tihedas koostöös ENISA, ENTSO-E, Euroopa Liidu jaotusvõrguettevõtjate üksuse, küberturvalisuse eest vastutavate pädevate asutuste, pädevate asutuste, ohuvalmiduse eest vastutavate pädevate asutuste, riikide reguleerivate asutuste ning võrgu- ja infoturbe riiklike küberkriisi ohjamise asutustega elektrisektori jaoks välja liidu tasandi küberkriisi ohjamise ja kriisile reageerimise kava.
2. 12 kuu jooksul pärast seda, kui ACER on lõike 1 kohaselt elektrisektori jaoks välja töötanud liidu tasandi küberkriisi ohjamise ja kriisile reageerimise kava, koostab iga pädev asutus piiriüleste elektrivoogude teemalise küberkriisi ohjamise ja kriisile reageerimise riikliku kava, milles võetakse arvesse liidu tasandi küberkriisi ohjamise kava ja määruse (EL) 2019/941 artikli 10 kohaselt kehtestatud riiklikku ohuvalmiduskava. See kava peab olema kooskõlas [NIS2-direktiivi] artikli 9 lõike 4 kohase riikliku ulatuslike küberturbeintsidentide ja kriiside lahendamise kavaga. Pädev asutus kooskõlastab oma tegevuse ülisuure ja suure mõjuga üksustega ning oma liikmesriigi ohuvalmiduse eest vastutava pädeva asutusega.
4. Liikmesriigid võivad lõigetes 1 ja 2 loetletud ülesanded delegeerida ka määruse (EL) 2019/943 artikli 37 lõike 2 kohastele piirkondlikele koordineerimiskeskustele.
d) määruse (EL) 2019/943 artikkel 35:
Artikkel 35. Piirkondlike koordineerimiskeskuste loomine ja missioon
1. Hiljemalt 5. juuliks 2020 esitavad kõik süsteemikäitamispiirkonna põhivõrguettevõtjad asjaomastele reguleerivatele asutustele ettepaneku piirkondlike koordineerimiskeskuste loomise kohta kooskõlas käesolevas peatükis sätestatud kriteeriumidega.
Süsteemikäitamispiirkonna reguleerivad asutused vaatavad ettepaneku läbi ja kiidavad selle heaks.

Ettepanek peab sisaldama vähemalt järgmisi elemente:
a) liikmesriik, kus on piirkondlike koordineerimiskeskuste ja osalevate põhivõrguettevõtjate asukoht;
b) ühendatud ülekandesüsteemi tõhusa, turvalise ja töökindla toimimise tagamiseks vajalik organisatsiooniline, rahaline ja töökorraldus;
c) piirkondlike koordineerimiskeskuste töölerakendamise kava;
d) piirkondlike koordineerimiskeskuste põhikirjad ja töökorrad;
e) koostöömenetluste kirjeldus kooskõlas artikliga 38;
f) piirkondlike koordineerimiskeskuste vastutuse korra kirjeldus kooskõlas artikliga 47;
g) kui kahte piirkondlikku koordineerimiskeskust hallatakse artikli 36 lõike 2 kohaselt rotatsiooni korras, siis piirkondlike koordineerimiskeskuste üheselt mõistetavate kohustuste ja nende ülesannete täitmise tagamiseks ette nähtud korra kirjeldus.
2. Pärast seda, kui reguleerivad asutused on lõikes 1 osutatud ettepaneku heaks kiitnud, asendavad piirkondlikud koordineerimiskeskused määruse (EÜ) nr 714/2009 artikli 18 lõike 5 alusel vastu võetud süsteemi käidueeskirjade kohaselt loodud piirkondlikud talitluskindluse koordinaatorid ning alustavad tööd hiljemalt 1. juulil 2022.
3. Piirkondlikud koordineerimiskeskused luuakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2017/1132 II lisas osutatud õiguslikus vormis.
4. Piirkondlikud koordineerimiskeskused tegutsevad liidu õiguse kohaseid ülesandeid täites sõltumatult riikide individuaalsetest huvidest ja põhivõrguettevõtjate huvidest.
5. Piirkondlikud koordineerimiskeskused täiendavad põhivõrguettevõtjate rolli, täites piirkondliku tähtsusega ülesandeid, mis on neile antud kooskõlas artikliga 37. Põhivõrguettevõtjad vastutavad võimsusvoogude juhtimise eest ning turvalise, töökindla ja tõhusa elektrisüsteemi tagamise eest kooskõlas direktiivi (EL) 2019/944 artikli 40 lõike 1 punktiga d.“
e) määruse (EL) 2019/943 artikkel 37 lõige 2:
Artikkel 37. Piirkondlike koordineerimiskeskuste ülesanded
2. Komisjoni või liikmesriikide ettepanekul avaldab direktiivi (EL) 2019/944 artikli 68 kohaselt loodud komitee arvamuse piirkondlikele koordineerimiskeskustele uute nõustamisülesannete andmise kohta. Kui komitee avaldab uute nõustamisülesannete andmise kohta positiivse arvamuse, täidavad piirkondlikud koordineerimiskeskused neid ülesandeid ENTSO-E poolt välja töötatud ja ACERi poolt artiklis 27 sätestatud menetluse kohaselt heaks kiidetud ettepaneku alusel.
Balti riikides on piirkondlikuks koordineerimiskeskuseks Baltic RCC, mis loodi 2022. aastal.[90]

Eelnõukohase KüTSi §-ga 6, kuid ka teiste sätetega seoses on kavas teha seaduses tehniline muudatus, mille kohaselt asendatakse sõnad “teenuse osutaja” grammatikanõuetega kooskõla saavutamiseks liitsõnaga “teenuseosutaja”. Täpsemalt puudutab see muudatus KüTSi § 6 punkte 1–3, § 7 lõiget 3, § 8 pealkirja, lõiget 1^1, lõike 2 punkti 3 ja lõiget 6 ning § 16 lõiget 2. Ülejäänud KüTSi sätete puhul on eelnõuga selline muudatus kavas konkreetse sätte muutmise käigus.

Eelnõukohase KüTSi §-ga 6^1 on kavas võtta üle NIS2-direktiivi artikkel 20. See on ka seotud NIS2-direktiivi põhjendusega 137:
(137) [NIS2-direktiivi] eesmärk peaks olema tagada kõrgel tasemel vastutus küberturvalisuse riskijuhtimismeetmete rakendamise ja teatamiskohustuse täitmise eest elutähtsate[91] ja oluliste üksuste tasandil. Seepärast peaksid elutähtsate[92] ja oluliste üksuste juhtorganid kiitma

[90] https://majandus.postimees.ee/7435802/balti-elektrisusteemi-koordineerimiskeskus-alustab-tood-sel-suvel-tallinnas ja https://baltic-rcc.eu/about.
[91] Eelnõus „ülioluliste üksuste“.
[92] Eelnõus „ülioluliste üksuste“.

küberturvalisuse riskijuhtimismeetmed heaks ja jälgima nende rakendamist.
NIS2-direktiivi artiklis 20 kasutatakse sõna „juhtorganid“, kuid ei täpsustata, mida või keda selle all mõeldakse. Juhtorganitel on administratiivsed ja järelevalvefunktsioonid ning nende pädevus ja struktuur võib liikmesriikides erineda. Euroopa Komisjon on selles kontekstis toonud paralleeli Euroopa Parlamendi ja nõukogu direktiiviga 2013/36/EL, mis käsitleb krediidiasutuste tegevuse alustamise tingimusi ning krediidiasutuste ja investeerimisühingute usaldatavusnõuete täitmise järelevalvet, millega muudetakse direktiivi 2002/87/EÜ ning millega tunnistatakse kehtetuks direktiivid 2006/48/EÜ ja 2006/49/EÜ.[93] Selle direktiivi põhjenduses 56 on selgitatud:
(35) Juhtorganit tuleks käsitada sellise organina, millel on nii otsuste elluviimise kui ka järelevalve funktsioon. Juhtorganite pädevus ja struktuur on liikmesriigiti erinev. Liikmesriikides, kus juhtorganitel on ühetasandiline struktuur, on juhtorganil tavaliselt juhtimise ja järelevalve ülesanded. Kahetasandilise struktuuriga liikmesriikides täidab juhtorgani järelevalvefunktsiooni eraldi järelevalvenõukogu, millel ei ole otsuste elluviimise funktsiooni, ja otsuste elluviimise funktsiooni täidab eraldi juhatus, mis vastutab ettevõtja igapäevase juhtimise eest. Sellest tulenevalt määratakse juhtorgani eri harudele eri ülesanded.
Seega on võimalik, et mõnes liikmesriigis on näiteks kaheastmeline süsteem, kus ühel juhtorgani tasandil toimub järelevalvefunktsiooni täitmine, kuid ilma administratiivse rollita, ning teine on administratiivse rolliga juhtorgan, kelle ülesanne on ettevõtja igapäevane majandamine – nii on see näiteks aktsiaseltsi ja osaühingu puhul ka Eestis (viimase puhul võib olla juhtimine korraldatud ka üheastmeliselt ehk on üksnes juhatus, ilma nõukoguta).
Eelnõu esialgses versioonis oli viidatud „juhtorganile“ nii, nagu see on NIS2-direktiivi artiklis 20 ette nähtud. Seda ei peetud aga piisavalt täpseks. Ühtlasi ei ole Eesti õiguse järgi võimalik vastutusele võtta juhtorganit, vaid üksust ja/või selle juhtorgani liiget. Seetõttu on eelnõu pärast kooskõlastamist muudetud. Eelnõu kohaselt pannakse NIS2-direktiivi artiklis 20 ette nähtud kohustused üksuse juhatuse liikmele. Juhatus esindab ja juhib ühingut. Küberturvalisuse nõuete täitmine kuulub üksuse üldiste juhtimisülesannete täitmise juurde. Juhatus on olemas nii aktsiaseltsil kui ka osaühingul, nõukogu peab seadusjärgselt olema üksnes aktsiaseltsil. Nendeks olukordadeks, kus üksusel ei ole enda juriidilise vormi tõttu juhatust, on eelnõukohases lõikes 4 nähtud ette erireegel.

Eelnõukohane KüTSi § 6[1] lõige 1. Euroopa Komisjon on eelnõu koostajatele NIS2-direktiivi kohta antud selgitustes kinnitanud, et kui liikmesriigi õigus võimaldab juhtorganites määrata konkreetsed ülesanded juhtorgani konkreetsele liikmele, siis on ka NIS2-direktiivi artiklis 20 olevad kohustused võimalik määrata konkreetsele juhtorgani liikmele. Sellest lähtudes nähakse kommenteeritava paragrahvi lõikes 1 eelnõuga ette, et teenuseosutaja määrab vähemalt ühe juhatuse liikme, kes kiidab heaks turvameetmed, jälgib nende rakendamist ja vastutab selle eest. Selle eesmärk on tagada täpsem rollide jaotus üksuse juhatuses ja tagada seeläbi ka praktikas küberturvalisuse nõuete parem järgimine. Riigi Infosüsteemi Ameti taotlusel on üksusel kohustus ametile esitada ka selle juhatuse liikme kontaktid. See juhatuse liige on näiteks ka ameti kontaktisik, kui amet teeb küberturvalisuse nõuete täitmise üle järelevalvet. Mõistagi ei kohaldata vastutava juhatuse liikme määramise kohustust sellisele üksusele, kellel ongi ainult üks juhatuse liige. Sellisel juhul kohaldatakse kõnealuses sättes ette nähtavaid kohustusi üksuse ainsale juhatuse liikmele. Kui üksuse juhtorgan peaks mingil põhjusel delegeerima kommenteeritava paragrahviga ette nähtavad kohustused muule isikule kui juhatuse liikmele, poleks see NIS2-direktiivi artikliga 20 ja kommenteeritava paragrahviga kooskõlas. Seetõttu ei ole võimalik niisugusel juhul kohustust delegeerida. Kommenteeritava paragrahvi lõikega 1 on kavas võtta üle NIS2-direktiivi artikli 20

[93] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32013L0036&qid=1748076190666

lõige 1, konkreetsemalt selle esimene tekstilõik. Juhatuse liige kiidab heaks turvameetmed, jälgib nende rakendamist ja vastutab selle eest. Turvameetmete all on mõeldud eelnõukohase KüTSi § 7 ning selle alusel kehtestatud määrustes ette nähtud turvameetmeid. Tuleb arvestada asjaoluga, et küberturvalisusega tegelemine ei ole ühekordne projekt, vaid see on järjepidev tegevus, mistõttu on vaja sätestada, et teenuseosutaja juhatuse liige tegeleb lisaks turvameetmete heakskiitmisele ka nende rakendamise jälgimisega.
NIS2-direktiivi artikli 20 lõige 1 viitab vastutusele turvameetmete rakendamise eest. Eelnõu esialgses versioonis oli vastutus nähtud ette eelnõukohases KüTSi §-s 18^4 väärteokaristusena. Pärast kooskõlastamist on jäetud esialgu kavandatud KüTSi § 18^4 eelnõust välja, et järgida NIS2-direktiivi võimalikult minimaalse ülevõtmise põhimõtet. Nimelt ei pea direktiivikohane vastutus tähendama ilmtingimata riigisiseses õiguses karistusõiguslikku vastutust (nii nagu see oli esialgses eelnõus ette nähtud), vaid see võib seisneda ka tsiviilõiguslikus vastutuses hüvitada kahju, mis on tekkinud turvameetmete järgimata jätmise (juhatuse liikme seadusest tulenevate kohustuste rikkumise) tõttu. See on teenuseosutajale kindlasti leebem variant võrreldes tema suhtes algatatava riikliku süüteomenetlusega. Tsiviilõigusliku vastutuse reeglid on riigisiseses õiguses juba olemas ja neid ei pea direktiivi ülevõtmiseks eraldi sätestama. Näiteks juhul, kui kõnealune üksus on osaühing, vastutab juhatuse liige üksusele tekitatud kahju eest äriseadustiku §-s 187 ette nähtud juhatuse liikme vastutuse reeglite kohaselt. Kui üksus on aktsiaselts, kohaldub äriseadustiku § 315. Juhul kui kõnealune üksus on riigi- või kohaliku omavalitsuse asutus (kellele kohaldatakse juhatuse liikme kohta sätestatut kõnealuse paragrahvi lõike 4 kohaselt), saab üksusele tekitatud kahju hüvitamisel lähtuda avaliku teenistuse seaduse §-s 80 sätestatust.

Eelnõukohase KüTSi § 6^1 lõikega 2 on kavas võtta üle NIS2-direktiivi artikli 20 lõige 2. Lõikes teenuseosutaja juhatuse liikmele ette nähtavad koolitused võiksid hõlmata küberturvalisusega seotud riske ja ohtusid, levinumaid rünnakutüüpe ja riskide haldamist.
Koolituse läbija ehk teenuseosutaja juhatuse liige:
1) mõistab Euroopa Liidu ja riiklikku küberjulgeolekut korraldavaid regulatsioone ning nende mõju organisatsiooni (äri)tegevusele ja riiklikule küberjulgeolekule, sh juhtide kohustusi ja vastutust;
2) saab regulaarseid küberülevaateid, tunneb levinumaid küberohte (nt õngitsus, lunavara, andmepüügi- ja teenustõkestusrünnakud), nende realiseerumise tõenäosust ja mõju enda organisatsiooni (äri)tegevusele;
3) tunneb küberturvalisuse valdkonnas olevate riskide juhtimise põhimõtteid, sh teeb otsuseid, seab prioriteete ja võimaldab ressursse enda organisatsiooni riskide leevendamise meetmete rakendamiseks ja kaitseks;
4) mõistab kriisiohjamise ja küberintsidentidele reageerimise protsessi olulisust ning vajadust eelnevalt välja töötatud ja testitud toimepidevus- ja kriisiplaanide järele.
NIS2-direktiivi kõnealune artikkel ei määra, mis on selliste koolituste tegemise intervall. Eelnõu kooskõlastamise käigus saabus selle kohta väga erinevat tagasisidet, alates sellest, et koolitused võiksid toimuda vähemalt kord kümne aasta jooksul, kuni selleni, et need peaksid toimuma vähemalt kord aastas. Arvestades KüTSi subjektide väga laia ja ka eriilmelist ringi, ei ole võimalik määrata sellist intervalli, mis sobiks kõigile. Pärast kooskõlastamist on seetõttu otsustatud jätta koolituste intervall seaduse tasandil reguleerimata. Koolitusi peab eelnõu kohaselt läbima regulaarselt, kuid seadusega ei kirjutata ette, kas seda tuleks teha iga aasta, iga kahe või iga viie aasta tagant. Selle määrab iga üksus ise vastavalt enda profiilile.

Eelnõukohane KüTSi § 6^1 lõige 3 on seotud lõikes 1 ette nähtava reegliga, mille järgi peab üksus määrama vähemalt ühe konkreetse juhatuse liikme, kes tegeleb turvameetmete heakskiidu ja nende

rakendamise jälgimisega ja ka vastutab selle eest. Lõikega 3 on kavas reguleerida olukorda, kus üksus ei ole turvanõuete eest vastutavat juhatuse liiget määranud ja kõnealuses paragrahvis sätestatavad reeglid kohalduvad kõigile juhatuse liikmetele. Sellist tagajärge on üksusel võimalik vältida, kui ta määrab ühe vastutava juhatuse liikme, nii nagu eelnõuga lõikes 1 ette nähakse.

Eelnõukohase KüTSi § 6[1] lõikega 4 on kavas reguleerida olukorda, kus konkreetsel üksusel ei ole tema juriidilise vormi või struktuuri tõttu juhatuse liiget. Regulatsioon on vajalik, sest eelnõu uues versioonis ei räägita enam juhtorgani liikmest, vaid juhatuse liikmest. Kõigil üksustel, kellele KüTSi kohaldatakse, ei pruugi aga juhatust ega juhatuse liikmeid olla. Seetõttu nähakse eelnõukohases lõikes 4 ette, et samas paragrahvis juhatuse liikme kohta käivat kohaldatakse ka muule isikule, kes on seaduse, põhimääruse või muu õigusakti kohaselt määratud asjaomase teenuseosutaja juures juhtimisülesandeid täitma. Näiteks kui tegemist on mõne ameti või inspektsiooniga, võib selleks isikuks olla peadirektor. Eraldi tuuakse välja, et füüsilisest isikust ettevõtja ehk FIE puhul kohaldub juhatuse liikme kohta sätestatu talle endale, sest FIE-l ei ole juhatust, tema ise täidabki kõiki selliseid juhtimisülesandeid, mida näiteks äriühingus täidab juhatuse liige. Seetõttu peab FIE füüsilise isikuna ka ise tagama küberturvalisuse nõuete täitmise, eeldusel et konkreetne FIE on KüTSi tähenduses teenuseosutaja.

Eelnõukohaste KüTSi § 7 muudatustega ja KüTSi § 7 lõike 5 alusel kehtestatud määrust muutes on kavas võtta üle NIS2-direktiivi artikkel 21. Pärast eelnõu kooskõlastamist on otsustatud viia osa seni eelnõu paragrahvi 7 kavandatud tehnilisemast regulatsioonist KüTSi § 7 lõike 5 alusel kehtestatud määrusesse. Eelnõus on lähtutud loogikast, et KüTSi §-s 7 jäetakse alles teenuseosutaja võrgu- ja infosüsteemi turvameetmetele ette nähtud üldised nõuded. Täpsemad nõuded selle kohta, mil moel eri subjektide kategooriatesse kuuluvad teenuseosutajad turvameetmeid rakendama peavad, nähakse ette KüTSi § 7 lõike 5 alusel kehtestatud määruses. Nimelt on eelnõu kooskõlastusringi ja sellele eelnenud arutelude tulemusel otsustatud, et mitte kõik KüTSi subjektid ei pea järgima Eesti infoturbestandardi või selle alternatiiviks oleva rahvusvahelise standardi ISO/IEC 27001 nõudeid ega allu selle kohustuse täitmisel välise auditeerimise nõudele,[94] vaid teatud subjektide suhtes kehtivad alalised ja esmased turvameetmete nõuded, võimaldades turvameetmete rakendamise täpse viisi valida teenuseosutajal endal. Eelnõukohases lõikes 1 nähakse ette üldine kohustus alaliselt turvameetmeid rakendada ja selle eesmärgid. Eelnõukohases lõikes 2 nähakse ette, mida tuleb turvameetmete rakendamisel arvestada. Kehtiva KüTSi § 7 lõiget 3 ei ole kavas muuta. Samuti ei ole kavas muuta lõikes 5 sätestatud volitusnormi. NIS2-direktiivi artikli 21 lõikes 2 on sätestatud täpsemad alalised reeglid selle kohta, mida peavad turvameetmed hõlmama – need nähakse eelnõu järgi ette lõike 5 alusel kehtestatava määruse muudatusega. Eelnõu kohaselt saab KüTSi § 7 uued lõiked 6 ja 7. Lõikes 6 täpsustatakse lõikes 5 ette nähtud volitusnormi. Lõikega 7 võetakse üle NIS2-direktiivi artikli 21 lõige 5.
Kommenteeritavas paragrahvis ja selle alusel antud määruste muudatusega määratakse eelnõu kohaselt kindlaks need tegevused ja asjaolud, mida teenuseosutaja peab turvameetme rakendamisel tegema või arvestama. Turvameetmete definitsiooni kohta vt KüTSi § 2 punkti 30.
Kommenteeritava paragrahvi ja selle alusel antavate määrustega on seotud ennekõike NIS2-direktiivi põhjendused 77–86 ja 88–91 ning konkreetsemate üksuste (näiteks usaldusteenuse osutajad, sh kvalifitseeritud usaldusteenuse osutajad, üldkasutatava elektroonilise side võrgu teenuse osutaja ja üldkasutatava elektroonilise side teenuse osutaja) puhul ka põhjendused 93–100:

[94] Vt eelnõude infosüsteemi toimikut 25-0715 Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmine – https://eelnoud.valitsus.ee/main/mount/docList/7d3ea848-35b2-47d8-8eb8-fa2f735c3da6.

(77) Vastutus võrgu- ja infosüsteemi turvalisuse tagamise eest lasub suurel määral elutähtsatel[95] *ja olulistel üksustel. Tuleks edendada ja arendada riskijuhtimiskultuuri, mis hõlmab riskihindamisi ja riskile vastavate küberturvalisuse riskijuhtimismeetmete rakendamist.*
(78) Küberturvalisuse riskijuhtimismeetmetes peaks võtma arvesse, mil määral elutähtis[96] *või oluline üksus võrgu- ja infosüsteemidest sõltub, ning hõlmama meetmeid intsidendiriskide tuvastamiseks, vältimiseks, avastamiseks, neile reageerimiseks ja neist taastumiseks ning nende mõju leevendamiseks. Võrgu- ja infosüsteemide turvalisus peaks hõlmama salvestatavate, edastatavate ja töödeldavate andmete turvalisust. Küberturvalisuse riskijuhtimismeetmetega tuleks tagada süsteemne analüüs, milles võetakse arvesse inimtegurit, et saada võrgu- ja infosüsteemi turvalisusest terviklik pilt.*
(79) Kuna võrgu- ja infosüsteemide turvalisust ähvardavatel ohtudel võib olla erinev põhjus, peaksid küberturvalisuse riskijuhtimismeetmed tuginema kõiki ohte hõlmavale käsitusele, mille eesmärk on kaitsta võrgu- ja infosüsteeme ja nende füüsilist keskkonda selliste olukordade eest nagu vargus, tulekahju, üleujutus, telekommunikatsiooni- või elektrikatkestus või loata füüsiline juurdepääs elutähtsa või olulise üksuse teabe- ja teabetöötlusrajatistele ning nende kahjustamine ja häirimine, mis võib ohustada võrgu- ja infosüsteemides salvestatud, edastatud või töödeldud andmete või nende süsteemide pakutavate või nende kaudu juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust. Seepärast peaksid küberturvalisuse riskijuhtimismeetmed käsitlema ka võrgu- ja infosüsteemide füüsilist turvalisust ja keskkonnaohutust, hõlmates selliste süsteemide kaitsmist süsteemirikete, inimliku eksimuse, pahatahtliku tegevuse või loodusnähtuste eest kooskõlas Euroopa ja rahvusvaheliselt tunnustatud standarditega, näiteks ISO/IEC 27000 seeria standarditega. Sellega seoses peaksid elutähtsad[97] *ja olulised üksused oma küberturvalisuse riskijuhtimismeetmete osana käsitlema ka personali turvalisust ja kehtestama asjakohased juurdepääsukontrolli põhimõtted. Need meetmed peaksid olema kooskõlas [CER-direktiiviga]*.
(80) Selleks et tõendada vastavust küberturvalisuse riskijuhtimismeetmetele ja kui puuduvad Euroopa Parlamendi ja nõukogu määrusele (EL) 2019/881 vastavad asjakohased Euroopa küberturvalisuse sertifitseerimise kavad, peaksid liikmesriigid konsulteerides koostöörühma ja Euroopa küberturvalisuse sertifitseerimise rühmaga edendama asjaomaste Euroopa ja rahvusvaheliste standardite kasutamist elutähtsate[98] *ja oluliste üksuste poolt, või liikmesriigid võivad üksustelt nõuda, et nad kasutaksid sertifitseeritud IKT-tooteid, IKT-teenuseid ja IKT-protsesse.*
(81) Et vältida elutähtsatele[99] *ja olulistele üksustele ebaproportsionaalse finants- ja halduskoormuse panemist, peaksid küberturvalisuse riskijuhtimismeetmed olema proportsionaalsed asjaomase võrgu- ja infosüsteemi puhul esineva riski tasemega ning lähtuma selliste meetmete tehnilisest tasemest ning, kui see on kohaldatav, Euroopa ja rahvusvahelistest standarditest ning nende rakendamise kuludest.*
(82) Küberturvalisuse riskijuhtimismeetmed peaksid olema proportsionaalsed elutähtsa[100] *või olulise üksuse riskidele avatuse määraga ning intsidendi ühiskondliku ja majandusliku mõjuga. Elutähtsatele*[101] *ja olulistele üksustele kohandatud küberturvalisuse riskijuhtimismeetmete*

[95] Eelnõus „üliolulistel üksustel“.
[96] Eelnõus „üliloluline üksus“.
[97] Eelnõus „üliolulised üksused“.
[98] Eelnõus „üliloluliste üksuste“.
[99] Eelnõus „üliolulistele üksustele“.
[100] Eelnõus „üliolulise üksuse“.
[101] Eelnõus „üliolulistele üksustele“.

kehtestamisel tuleks igakülgselt arvesse võtta elutähtsate[102] ja oluliste üksuste erinevat avatust riskidele, näiteks üksuse kriitilisuse määra, riske, sealhulgas ühiskondlikke riske, millega ta kokku puutub, üksuse suurust, intsidentide esinemise tõenäosust ja nende tõsidust, sealhulgas nende ühiskondlikku ja majanduslikku mõju.

(83) Elutähtsad[103] ja olulised üksused peaksid tagama oma tegevuses kasutatavate võrgu- ja infosüsteemide turvalisuse. Nende puhul on eelkõige tegemist privaatsete võrgu- ja infosüsteemidega, mida haldavad kas elutähtsa[104] või olulise üksuse enda IT-töötajad või mille turvalisusega seotud teenused ostetakse sisse. [NIS2-direktiivis] sätestatud küberturvalisuse riskijuhtimismeetmeid ning teatamiskohustust tuleks kohaldada asjaomaste elutähtsate[105] ja oluliste üksuste suhtes olenemata sellest, kas kõnealused üksused hooldavad oma võrgu- ja infosüsteeme ise või tellivad selleks hooldusteenuse väljast.

(84) Võttes arvesse nende piiriülest olemust, tuleks domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate[106], hallatud teenuse osutajate[107], turbetarnijate[108], internetipõhise kauplemiskohtade[109], internetipõhiste otsingumootorite[110], sotsiaalvõrguteenuse platvormi pakkujate[111] ja usaldusteenuse osutajate suhtes kohaldada liidu tasandil suuremat ühtlustamist. Seetõttu tuleks küberturvalisuse riskijuhtimismeetmete rakendamise hõlbustamiseks seoses kõnealuste üksustega võtta vastu rakendusakt.

(85) Eriti oluline on tegeleda riskidega, mis tulenevad üksuse tarneahelast ja suhetest tema tarnijatega, näiteks andmete talletamise ja töötlemise teenuse osutajate või turbeteenuse osutajate ja sisutoimetajatega, kui võtta arvesse selliste intsidentide esinemise sagedust, mille puhul üksused on langenud võrgu- ja infosüsteemi vastu suunatud küberrünnete ohvriks ning kurjategijad on suutnud kahjustada üksuse võrgu- ja infosüsteemide turvalisust, kasutades ära kolmandate isikute tooteid ja teenuseid mõjutavaid nõrkusi. Seepärast peaksid elutähtsad[112] ja olulised üksused hindama ja arvesse võtma toodete ja teenuste üldist kvaliteeti ja vastupidavust, nendesse integreeritud küberturvalisuse riskijuhtimismeetmeid, samuti oma tarnijate ja teenuseosutajate[113] küberturvalisuse tavasid, sealhulgas nende turvalise arenduse menetlusi. Elutähtsaid[114] ja olulisi üksusi tuleks eelkõige julgustada lisama küberturvalisuse riskijuhtimismeetmeid oma otseste tarnijate ja teenuseosutajatega sõlmitavatesse lepingutesse. Kõnealused üksused võiksid võtta arvesse ka riske, mis tulenevad muu tasandi tarnijatest ja teenuseosutajatest.

(86) Teenuseosutajate seas on intsidentide ennetamisel, tuvastamisel, lahendamisel ja neist taastumisel üksuste jaoks eriti oluline tugiroll turbetarnijatel[115] sellistes teenusevaldkondades

---

[102] Eelnõus „üliolulise üksuste“.
[103] Eelnõus „üliolulised üksused“.
[104] Eelnõus „üliolulise üksuse“.
[105] Eelnõus „üliolulise üksuste“.
[106] Eelnõus „sisulevivõrguteenuse osutajate“.
[107] Eelnõus „haldusteenuse osutajate“.
[108] Eelnõus „infoturbeteenuse osutajate“.
[109] Eelnõus „internetipõhiste kauplemiskohtade pidajate“.
[110] Eelnõus „veebipõhise otsingumootori pakkujate“.
[111] Eelnõus „sotsiaalmeediaplatvormi pakkujate“.
[112] Eelnõus „üliolulised üksused“.
[113] Siin ei ole pigem mõeldud eelnõuga KüTSi § 3 lõikes 1 sõnastatavat terminit „teenuseosutaja“, vaid neid üksusi, kes KüTSi kohaldamisalas olevale üksusel teenust osutavad või pakuvad. Samas võivad sellisteks üksusteks olla ka nt eelnõukohased haldusteenuse osutajad või infoturbeteenuse osutajad. Siinne märkus kohaldub ka siinse tekstilõigu kahe järgmise lause kohta.
[114] Eelnõus „üliolulisi üksusi“.
[115] Eelnõus „infoturbeteenuse osutajatel“.

nagu intsidentide lahendamine, läbistustestimine, turvaaudit ja konsultatsioonid. Turbetarnijad[116] on aga olnud ka ise küberrünnete sihtmärgiks ja kuna nad on üksuste tegevusse tihedalt lõimitud, kaasneb nendega eriline risk. Seega peaksid elutähtsad[117] ja olulised üksused olema turbetarnija[118] valimisel iseäranis hoolikad.

(88) Elutähtsad[119] ja olulised üksused peaksid tähelepanu pöörama ka sellistele riskidele, mis tulenevad nende suhtlemisest ja suhetest teiste sidusrühmadega laiemas ökosüsteemis, et muu hulgas tõkestada tööstusspionaaži ja kaitsta ärisaladusi. Täpsemalt peaksid üksused võtma asjakohaseid meetmeid tagamaks, et nende koostöö akadeemiliste ja teadusasutustega toimub kooskõlas nende küberturvalisuse poliitikaga ning et selles koostöös järgitakse teabele turvalise juurdepääsu ja selle levitamisega seotud üldisi häid tavasid ja eelkõige intellektuaalomandi kaitsega seotud tavasid. Võttes arvesse andmete olulisust ja väärtust elutähtsate[120] ja oluliste üksuste tegevuse jaoks, peaksid kõnealused üksused kolmandate isikute poolt osutatavatele andmete teisendamise ja analüüsi teenustele tuginedes võtma kõik asjakohased küberturvalisuse riskijuhtimismeetmed.

(89) Elutähtsad[121] ja olulised üksused peaksid kasutusele võtma mitmesugused küberhügieeni põhitavad, näiteks usaldamatuse põhimõtte, tarkvarauuendused, seadme konfiguratsiooni, võrgu segmenteerimise, identiteedi ja juurdepääsu halduse ning kasutajateadlikkuse, ning pakkuma oma töötajatele koolitusi ning suurendama teadlikkust küberohtude, andmepüügi ja inimestega manipuleerimise meetodite kohta. Lisaks peaksid kõnealused üksused hindama oma küberturvalisuse võimekust ning püüdma võtta asjakohasel juhul kasutusele küberturvalisust suurendavad tehnoloogiad, näiteks tehisintellekti või masinõppesüsteemid, et suurendada oma võimekust ning võrgu- ja infosüsteemide turvalisust.

(90) Et käsitleda põhjalikumalt peamisi tarneahelariske ning aidata asjakohaselt juhtida [NIS2-direktiivi] kohaldamisalasse kuuluvates sektorites tegutsevatel elutähtsatel[122] ja olulistel üksustel tarneahela ja tarnijatega seotud riske, peaks koostöörühm tegema koostöös komisjoni ja ENISAga ning asjakohasel juhul pärast asjakohaste sidusrühmadega, sealhulgas tööstusega konsulteerimist koordineeritud kriitilise tähtsusega tarneahelate turberiski hindamise (nagu tehti 5G-võrkude kohta vastavalt soovitusele (EL) 2019/534 (5G-võrkude küberturvalisuse kohta)), eesmärgiga määrata iga sektori jaoks kindlaks kriitilise tähtsusega IKT-teenused, IKT-süsteemid või IKT-tooted, asjaomased ohud ja nõrkused. Sellise turberiski koordineeritud hindamise käigus tuleks kindlaks teha meetmed, leevenduskavad ja parimad tavad, millega võidelda kriitilise tähtsusega sõltuvuse vastu, potentsiaalsete nõrkade lülide, ohtude, nõrkuste[123] ja muude riskide vastu, mis on seotud tarneahelaga, ning uurida, kuidas saaks elutähtsaid[124] ja olulisi üksusi julgustada neid ulatuslikumalt kasutusele võtma. Võimalikud muud kui tehnilised riskitegurid, nagu kolmanda riigi lubamatu mõju tarnijatele ja teenuseosutajatele, eelkõige alternatiivsete juhtimismudelite puhul, hõlmavad varjatud nõrkusi[125] või tagauksi ja võimalikke süsteemseid tarnehäireid, eriti tehnoloogilise kinnistumise või teenuseosutajast sõltuvuse korral.

(91) Kriitilise tähtsusega tarneahela turberiskide koordineeritud hindamisel tuleks asjaomase

---

[116] Eelnõus „infoturbeteenuse osutajad“.
[117] Eelnõus „üliolulised üksused“.
[118] Eelnõus „infoturbeteenuse osutaja“.
[119] Eelnõus „üliolulised üksused“.
[120] Eelnõus „ülioluliste üksuste“.
[121] Eelnõus „üliolulised üksused“.
[122] Eelnõus „üliolulistel üksustel“.
[123] Eelnõus „turvahaavatavuste“.
[124] Eelnõus „üliolulisi üksusi“.
[125] Eelnõus „turvahaavatavusi“.

sektori omadusi silmas pidades võtta arvesse nii tehnilisi kui ka asjakohasel juhul muid kui tehnilisi tegureid, sealhulgas neid, mis on kindlaks määratud soovituses (EL) 2019/534, 5G-võrkude küberturvalisusega seotud ELi koordineeritud riskihindamist käsitlevas aruandes ja koostöörühma kokkulepitud ELi 5G-küberturvalisuse meetmepaketis. Et teha kindlaks tarneahelad, mille suhtes peaks kohaldama turberiski koordineeritud hindamist, tuleks arvesse võtta järgmisi kriteeriume: i) kui suurel määral elutähtsad[126] ja olulised üksused kindlaid kriitilise tähtsusega IKT-teenuseid, IKT-süsteeme või IKT-tooteid kasutavad ning nendele tuginevad; ii) kindlate kriitilise tähtsusega IKT-teenuste, IKT-süsteemide või IKT-toodete asjakohasus kriitilise tähtsusega või tundlike funktsioonide (sealhulgas isikuandmete töötlemine) täitmisel; iii) alternatiivsete IKT-teenuste, IKT-süsteemide või IKT-toodete kättesaadavus; iv) IKT-teenuste, IKT-süsteemide või IKT-toodete tarneahela kui terviku vastupidavusvõime kogu nende olelusringi jooksul häirivate sündmuste korral või v) kui tegemist on kujunemisjärgus IKT-teenuste, IKT-süsteemide või IKT-toodetega, siis nende potentsiaalne tulevane tähtsus üksuste tegevuse jaoks. Lisaks tuleks erilist tähelepanu pöörata IKT-teenustele, IKT-süsteemidele või IKT-toodetele, mille suhtes kehtivad kolmandatest riikidest tingitud erinõuded.

Eelnõukohase KüTSi § 7 lõikega 1 on kavas võtta üle NIS2-direktiivi artikli 21 lõike 1 esimene tekstilõik, samal ajal säilitades muudetava lõike 1 olemuse ja sisu eelnõu kohaselt sätestatavas sõnastuses.

Kommentaaris mainitud artikli olemust selgitab ka NIS2-direktiivi artikli 4 kontekstis asjaomane komisjoni suunis.[127] NIS2-direktiivi artikli 21 lõike 1 esimese tekstilõigu kohaselt tagavad liikmesriigid, et elutähtsad (eelnõus üliolulised) ja olulised üksused võtavad asjakohased ja proportsionaalsed tehnilised, tegevuslikud ja korralduslikud meetmed, et juhtida riske, mis ohustavad nende üksuste tegevuses või teenuste osutamisel kasutatavate võrgu- ja infosüsteemide turvalisust. Meetmed peaksid olema riskipõhised ja nendega peaks saama intsidentide mõju ennetada või minimeerida. NIS2-direktiivi artikli 21 lõike 1 teises tekstilõigus on täpsustatud, kuidas tuleks hinnata selliste meetmete proportsionaalsust (vt ka NIS2-direktiivi põhjendusi 78, 81 ja 82 ning eespool kommenteeritava paragrahvi sissejuhatuses olevaid selgitusi). NIS2-direktiivi artikli 21 lõikes 1 sätestatud kohustus, mille kohaselt peavad elutähtsad (eelnõus üliolulised) ja olulised üksused võtma asjakohaseid ja proportsionaalseid küberturvalisuse riskijuhtimismeetmeid, kehtib kõigi asjaomase üksuse tegevuste ja teenuste suhtes ega puuduta üksnes konkreetseid infotehnoloogia varasid või elutähtsaid teenuseid, mida üksus osutab.[128]

NIS2-direktiivi artikli 6 punktis 2 sätestatud võrgu- ja infosüsteemide turvalisuse definitsioonis viidatakse infosüsteemide võimele panna teatava kindlusega vastu mis tahes sündmusele, mis võiks kahjustada salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust. Asjaolu, et definitsioonis kasutatakse selliseid mõisteid nagu „kättesaadavus“, „autentsus“, „terviklus“ ja „konfidentsiaalsus“, viitab kõigile neljale võrgu- ja infosüsteemide turvalisusega seotud kaitse-eesmärgile. NIS2-direktiivi artikli 6 punktis 1 defineeritud „võrgu- ja infosüsteem“ hõlmab elektroonilise side võrke; seadmeid või omavahel ühendatud või seotud seadmete rühmi, millest vähemalt ühes toimub mõne programmi kohaselt digiandmete automaatne töötlemine, ja digiandmeid, mida salvestatakse, töödeldakse, saadakse päringutega või edastatakse

[126] Eelnõus „üliolulised üksused“.

[127] Komisjoni teatis „Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 4 lõigete 1 ja 2 kohaldamise kohta“ 2023/C 328/02: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0918%2801%29&qid=1751961587504.

[128] *Op cit*, p 7.

selliste elektroonilise side võrkude või seadmete kaudu nende töö, kasutamise, kaitsmise või hooldamise jaoks. Sellest tulenevalt peaksid turvameetmed hõlmama ka üksuse tegevuses kasutatavat riistvara, püsivara ja tarkvara.[129]

Eelnõukohase KüTSi § 7 lõikega 2 on kavas võtta üle NIS2-direktiivi artikli 21 lõike 1 teine tekstilõik ja lõike 2 sissejuhatav osa. Tegemist on asjaoludega, millega tuleb teenuse osutajal turvameetmete rakendamisel arvestada.
Kõiki ohte hõlmavat lähenemisviisi selgitab NIS2-direktiivi artikli 4 kontekstis nii vastav komisjoni suunis kui ka direktiivi põhjendus 79 (vt eespool). Selles suunises on märgitud, et nõutavad küberturvalisuse riskijuhtimismeetmed tuginevad kõiki ohte hõlmavale lähenemisviisile. Võrgu- ja infosüsteemide turvalisust ähvardavad ohud võivad olla pärit eri allikatest ja seepärast võib mis tahes liiki sündmus avaldada üksuse võrgu- ja infosüsteemile negatiivset mõju ja tõenäoliselt põhjustada intsidendi. Seepärast ei peaks üksuse võetavad küberturvalisuse riskijuhtimismeetmed kaitsma mitte ainult üksuse võrgu- ja infosüsteeme, vaid ka nende süsteemide füüsilist keskkonda igasuguste sündmuste eest, nagu sabotaaž, vargus, tulekahju, üleujutus, side- või elektrikatkestus või loata füüsiline juurdepääs, mis võiksid kahjustada salvestatud, edastatud või töödeldud andmete või võrgu- ja infosüsteemide pakutavate või nende kaudu juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust. Sellest tulenevalt peaksid küberturvalisuse riskijuhtimismeetmed käsitlema ka võrgu- ja infosüsteemide füüsilist ja keskkonnaalast turvalisust seoses süsteemirikete, inimlike eksimuste, kuritahtlike tegude või loodusnähtustega.[130]
Kommenteeritavas lõikes sätestatavaid punkte selgitavad ka siinse paragrahvi selgituse sissejuhatavas osas märgitud muud NIS2-direktiivi põhjendused, mida siin ei korrata.

Eelnõukohase KüTSi § 7 lõikega 6 on kavas täpsustada lõikes 5 sätestatavat volitusnormi. Nimelt nähakse ette, et määruses võib täpsustada alalisi asjakohaseid ja proportsionaalseid tehnilisi, tegevuslikke ning korralduslikke turvameetmeid ning nende rakendamise nõudeid ja tingimusi. Selline täpsustamine on vajalik, et NIS2-direktiivi artikli 21 lõikes 2 sätestatud nõuded saaks näha ette just määruses. Määruses täpsustatavad turvameetmed on seotud eelnõukohase KüTSi § 7 lõikes 1 ette nähtud alaliste turvameetmete täpsustamisega.

Eelnõukohane KüTSi § 7 lõige 7 on mõeldud NIS2-direktiivi artikli 21 lõike 5 rakendamiseks ehk kommenteeritava lõikega tekitatakse selgus, millised teenuseosutajad hakkavad lähtuma turvameetmete rakendamisel NIS2-direktiivi artikli 21 lõike 5 alusel Euroopa Komisjoni rakendusaktist ja seal sätestatud nõuetest.
Euroopa Komisjon on kehtestanud rakendusaktiga erinõuded järgmiste teenuseosutajate suhtes (esitatud on eelnõus kasutatavad terminid): domeeninimede süsteemi teenuse osutajad, tippdomeeninimede registrid, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrguteenuse osutajad, haldusteenuse osutajad, infoturbeteenuse osutajad, internetipõhise kauplemiskoha pidajad, veebipõhise otsingumootori pakkujad, sotsiaalmeediaplatvormi pakkujad ja usaldusteenuse osutajad.
Selle rakendusakti pealkiri on „Euroopa 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, turbetarnijate ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite, sotsiaalvõrguteenuse platvormide ja

[129] *Op cit*, p 8.
[130] *Op cit*, p 9.

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.“[131]
Euroopa Liidu Küberturvalisuse Amet on seoses selle rakendusaktiga andnud neile üksustele ka suunised rakendusakti nõuete täitmiseks.[132]
Siin kommenteeritava lõike eesmärk on tekitada selgus, et kui tegemist on eelviidatud rakendusmääruses nimetatud üksusega, kohaldatakse talle rakendusmääruse nõudeid kogu tema tegevuse puhul – tingimusel, et selle üksuse tegevus ongi ainult seotud rakendusaktis nimetatud teenustega.
Kui üksus osutab nii rakendusaktis nimetatud kui ka muid teenuseid (nt üldkasutatava elektroonilise side võrgu teenus), kohaldatakse turvameetmete kontekstis rakendusaktis nimetatud teenustele rakendusakti nõudeid ning ülejäänud teenustele kommenteeritavas paragrahvis ja selle alusel kehtestatud nõudeid.
Üksus, kes osutab rakendusaktis nimetatud teenust või teenuseid, võib enda vastavust rakendusakti nõuetele tõendada, kasutades lisaks asjaomastele Euroopa ja rahvusvahelistele standarditele liikmesriikide siseriikliku õigusega ettenähtud raamistikke, juhiseid või muid mehhanisme (vt rakendusmääruse (EL) 2024/2690 põhjenduse 7 neljandat lauset).
NIS2-direktiivi artikli 25 lõige 1 sätestab: *[NIS2-direktiivi artikli] 21 lõigete 1 ja 2 ühtse kohaldamise edendamiseks toetavad liikmesriigid võrgu- ja infosüsteemide turvalisust käsitlevate Euroopa ja rahvusvaheliste standardite ja tehniliste spetsifikatsioonide rakendamist, ilma et nad seejuures nõuaksid või diskrimineerivalt soosiksid konkreetset tüüpi tehnoloogia kasutamist*.
Euroopa Komisjoni selgituste kohaselt võivad liikmesriigid viidatud lõike rakendamiseks ergutada Euroopa standardi, rahvusvahelise standardi või muude tehniliste nõuete kasutamist, mis on sätestatud liikmesriigi tugiraamistikus, soovitustes või muudes mehhanismides. Seega oleneb liikmesriigi õigusega antavatest tingimustest see, kuidas ja mil määral saab tõendada nende abil rakendusmääruses (EL) 2024/2690 ette nähtud nõuete täitmist. Siin kõne all oleva eelnõu kohaselt ei sätestata, et rakendusmääruses (EL) 2024/2690 ette nähtud nõuete täitmiseks tuleb kasutada Eesti infoturbestandardit või rahvusvahelist standardit ISO/IEC 27001, kuid see siiski ei tähenda, et teenuseosutaja ei võiks seda ise vabatahtlikult teha (kui rakendusmäärus (EL) 2024/2690 ei näe ette konkreetse standardi rakendamist).

KüTSi § 8 lõike 1 eelnõukohane muudatus on seotud i) erisuse sätestamisega julgeolekuasutuste kontekstis ehk NIS2-direktiivi artikli 8 lõike 1 ülevõtmisega (vt eelnõus KüTSi § 5 lõiget 9) ja ii) NIS2-direktiivi artikli 23 lõike 4 punktis a sätestatud kohustuse ülevõtmisega. Kui kehtiva KüTSi kohaselt on teenuseosutajal kohustus Riigi Infosüsteemi Ametit teavitada 24 tundi pärast olulise mõjuga küberintsidendist teada saamist, siis NIS2-direktiiv näeb ette esmase teate (*varajane hoiatus*) esitamise kohustuse 24 tunni jooksul, millele järgneb enne lõppraportit 72 tunni möödumisel esitatav täiendatud teade ja Riigi Infosüsteemi Ameti taotlusel ka vaheraport. Kuna üks intsidendist teatamise neljaosalisest mehhanismist on Eesti õigusest praegu puudu, tulebki paragrahvi 8 muuta läbivalt.

---

[131] Rakendusakt jõustus 7. novembril 2024 ja on kättesaadav https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1730728447038; lisainfo leitav: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en ja https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=PI_COM:Ares(2024)4640447&qid=1728309190768.

[132] Lisainfo https://www.enisa.europa.eu/news/supporting-nis2-implementation-through-actionable-guidance ja https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

KüTSi § 8 lõike 2 punktide 1 ja 4 eelnõukohane muudatus on tehniline, kuna edaspidi on kavas võrgu- ja infosüsteemi riskianalüüsi tegemise nõue sätestada KüTSi § 7 lõike 1 punktis 1, mitte sama paragrahvi lõike 2 punktis 1. Muudatust tegemata oleks kõnealuse lõike punktides 1 ja 4 viide valele õigusnormile.

Eelnõukohase KüTSi § 8 lõike 2 punkti 5 muutmisega on kavas teha seaduses tehniline muudatus, mille kohaselt asendatakse sõnad "teenuse osutaja" grammatikanõuetega kooskõla saavutamiseks liitsõnaga "teenuseosutaja". Ülejäänud KüTSi sätete puhul on eelnõuga selline muudatus kavas konkreetse sätte muutmise käigus.

Eelnõukohase KüTSi § 8 lõike 2 punktiga 6 ehk lisanduva punktiga on kavas luua selgem seos ja määratlus, et ka NIS2-direktiivi artikli 23 lõike 11 alusel vastu võetud Euroopa Komisjoni rakendusaktis määratletud oluline intsident on olukord, millest tuleb KüTSi § 8 kohaselt Riigi Infosüsteemi Ametit teavitada, kuna tegemist on olulise mõjuga küberintsidendiga.
Euroopa Komisjon on kehtestanud rakendusaktiga erinõuded järgmiste teenuseosutajate suhtes (esitatud on eelnõus kasutatavad terminid): domeeninimede süsteemi teenuse osutajad, tippdomeeninimede registrid, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrguteenuse osutajad, haldusteenuse osutajad, infoturbeteenuse osutajad, internetipõhise kauplemiskoha pidajad, veebipõhise otsingumootori pakkujad, sotsiaalmeediaplatvormi pakkujad ja usaldusteenuse osutajad.
Selle rakendusakti pealkiri on „Euroopa 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, 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".[133]
Avalikule kooskõlastusringile saadetud eelnõu versioonis oli kasutatud sõnastust „oluline küberintsident", kuid eelnõu teksti ülevaatamise käigus jõuti järelduseni, et tuleb kasutada sõnastust „oluline intsident", kuna sama sõnastust on kasutatud NIS2-direktiivis ja selle artikli 23 lõike 5 alusel antud rakendusaktis. Ka eelnõus on KüTSi § 8 lõike 2 punkti 6 tekst sama sõnastusega, et tekiks selgem arusaam – rakendusaktis olev „oluline intsident" on see olukord, mille puhul on tegemist KüTSi mõttes „olulise mõjuga küberintsidendiga", millest tuleb pädevat asutust teavitada.
Kui jätta kommenteeritav punkt lisamata, siis ei oleks üheselt selge, kuidas hakkaks KüTSis sätestatud olulise mõjuga küberintsidendist teatamine suhestuma nende olukordadega, mis on kindlaks määratud vastavas rakendusaktis.

KüTSi § 8 lõige 4 tunnistatakse eelnõu kohaselt kehtetuks, kuna küberintsidendist vabatahtliku teatamise temaatika on eelnõuga kavandatud paragrahvi 8^1.

Eelnõukohase KüTSi § 8 lõikega 4^1 on kavas võtta üle NIS2-direktiivi artikli 23 lõike 4 punkt a

[133] Rakendusakt jõustus 7. novembril 2024 ja on kättesaadav https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1730728447038. Lisainfo: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en ja https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=PI_COM:Ares(2024)4640447&qid=1728309190768.

ehk määrata kindlaks need asjaolud, mida olulise mõjuga küberintsidendi kohta esmases teates esitada tuleb – tingimusel, et selline teave on esmase teate esitamise ajal olemas, sest praktikas võib esineda ka olukord, et mingi asjaolu ei ole veel teada (nt intsidendi piiriülene mõju või hinnang olulise mõjuga küberintsidendi tõsidus ja mõju vms). Seetõttu on sättes ka sõnad „esitatakse võimaluse korral".

NIS2-direktiivi artikli 23 lõige 4 näeb laiemalt ette nelja laadi teavitamist, millest lähtudes kohendatakse eelnõuga paragrahvis 8 läbivalt ka intsidendist teatamise siseriiklikku korraldust. Direktiivi kohaselt jagunevad teavitamised järgmiselt: varajane hoiatus, intsidenditeade, vahearuanne ja lõpparuanne. Vastavaid teavitusi ja küberintsidendist teatamise temaatikat käsitlevad ka NIS2-direktiivi põhjendused 101–107:

(101) [NIS2-direktiivis] sätestatakse olulistest intsidentidest teatamisele mitmeetapiline lähenemisviis, et saavutada õige tasakaal kahe ülesande vahel: ühelt poolt kiire teatamine, mis aitab vähendada oluliste intsidentide võimalikku levikut ja võimaldab elutähtsatel[134] ja olulistel üksustel abi otsida, ning teiselt poolt põhjalik aruandlus, mis võimaldab saada üksikutest intsidentidest väärtuslikke õppetunde ja suurendada aja jooksul üksikute ettevõtete ja tervete sektorite vastupanuvõimet küberohtude suhtes. Sellega seoses peaks [NIS2-direktiiv] hõlmama teatamist sellistest intsidentidest, mis asjaomase üksuse esialgse hinnangu kohaselt võivad põhjustada asjaomase üksuse teenustele tõsiseid tegevushäireid või kõnealusele üksusele rahalist kahju või mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset varalist või mittevaralist kahju. Esialgses hinnangus tuleks muu hulgas arvesse võtta mõjutatud võrgu- ja infosüsteeme ning eelkõige nende tähtsust üksuse teenuste osutamisel, küberohu tõsidust ja tehnilisi omadusi ning kõiki ärakasutamist võimaldavaid nõrkusi[135], samuti üksuse kogemusi sarnaste intsidentidega. Sellised näitajad nagu teenuse toimimise mõjutamise ulatus, intsidendi kestus või mõjutatud teenusekasutajate arv võivad mängida olulist rolli selle kindlakstegemisel, kas teenuse tegevushäire on tõsine.

(102) Elutähtsatelt[136] ja olulistelt üksustelt, kes saavad olulisest intsidendist teadlikuks, tuleks nõuda, et nad esitaksid varajase hoiatuse põhjendamatu viivituseta ja igal juhul 24 tunni jooksul. Sellele varajasele hoiatusele peaks järgnema intsidenditeade. Asjaomased üksused peaksid esitama intsidenditeate põhjendamatu viivituseta ja igal juhul 72 tunni jooksul pärast olulisest intsidendist teadlikuks saamist, et eelkõige ajakohastada varajase hoiatuse kaudu esitatud teavet ning anda esialgne hinnang olulisele intsidendile, muu hulgas selle tõsidusele ja mõjule ning, kui need on kättesaadavad, ka turvarikke indikaatoritele[137]. Lõpparuanne tuleks esitada ühe kuu jooksul pärast intsidenditeadet. Varajane hoiatus peaks sisaldama üksnes teavet, mis on vajalik CSIRTi või, kui see on kohaldatav, pädeva asutuse olulisest intsidendist teavitamiseks ja võimaldama asjaomasel üksusel vajaduse korral abi otsida. Selline varajane hoiatus, kui see on kohaldatav, peaks näitama, kas on kahtlus, et olulise intsidendi põhjuseks on ebaseaduslik või pahatahtlik tegevus, ning kas sellel on tõenäoliselt piiriülene mõju. Liikmesriigid peaksid tagama, et kohustus esitada kõnealune varajane hoiatus või sellele järgnev intsidenditeade ei suuna teavitava üksuse ressursse kõrvale intsidentide käsitlemisega seotud tegevusest, mis tuleks prioriseerida, et vältida olukorda, kus intsidentidest teatamise kohustus kas suunab vahendeid oluliste intsidentide lahendamiselt kõrvale või kahjustab muul viisil üksuse sellealaseid pingutusi. Kui intsident jätkub lõpparuande esitamise ajal, peaksid liikmesriigid tagama, et asjaomased üksused esitavad sel ajal vahearuande ja ühe kuu jooksul pärast olulise intsidendi nendepoolset

[134] Eelnõus „üliolulistel üksustel".
[135] Eelnõus „turvahaavatavusi".
[136] Eelnõus „üliolulistelt üksustelt".
[137] Eelnõus „turvarikkemärkidele".

käsitlemist lõpparuande.
(103) Kui see on kohaldatav, peaksid elutähtsad[138] ja olulised üksused teavitama oma teenuste kasutajaid viivitamata meetmetest või parandusmeetmetest, mida nad saavad olulisest küberohust tulenevate riskide vähendamiseks võtta. Kui see on kohane ja eelkõige juhul, kui oluline küberoht tõenäoliselt realiseerub, peaksid kõnealused üksused teavitama ohust ka oma teenuste kasutajaid. Nõue teavitada teenuste kasutajaid olulistest küberohtudest tuleks täita nii hästi kui võimalik, kuid see ei vabasta kõnealuseid üksusi kohustusest võtta oma kulul viivitamata sobivaid meetmeid, et selliseid võimalikke ohte ennetada või need kõrvaldada ning taastada teenuse turvalisuse tavapärane tase. Selline teave oluliste küberohtude kohta tuleks edastada kasutajatele tasuta ja selle sõnastus peaks olema kergesti mõistetav.
(104) Üldkasutatavate elektroonilise side võrkude pakkujad[139] või üldkasutatavate elektroonilise side teenuste osutajad peaksid rakendama sisseprojekteeritud ja vaiketurvet ning teavitama teenuse kasutajaid olulistest küberohtudest ning meetmetest, mida viimased saavad oma seadmete ja side turvalisuse kaitseks võtta, kasutades näiteks teatavat liiki tarkvara või krüpteerimistehnoloogiaid.
(105) Küberohte ennetav lähenemisviis on küberturvalisuse riskijuhtimise oluline osa, mis peaks võimaldama pädevatel asutustel tulemuslikult vältida küberohtude muutumist intsidentideks, mis võivad põhjustada märkimisväärset varalist või mittevaralist kahju. Seetõttu on küberohtudest teatamine esmatähtis. Seepärast julgustatakse üksusi küberohtudest vabatahtlikult teatama.
(106) [NIS2-direktiivi] alusel nõutava teabe esitamise lihtsustamiseks ja üksuste halduskoormuse vähendamiseks peaksid liikmesriigid asjakohase teabe esitamiseks ette nägema tehnilised vahendid, nagu ühtne kontaktpunkt, automatiseeritud süsteemid, veebipõhised vormid, kasutajasõbralikud liidesed, teatevormid, spetsiaalsed platvormid, mida üksused saavad kasutada, olenemata sellest, kas nad kuuluvad [NIS2-direktiivi] kohaldamisalasse. [NIS2-direktiivi] rakendamist toetavad liidu rahalised vahendid, eelkõige Euroopa Parlamendi ja nõukogu määrusega (EL) 2021/694 loodud programmi „Digitaalne Euroopa" raames, võiksid hõlmata toetust ühtsetele kontaktpunktidele. Üksused on sageli ka olukorras, kus konkreetsest intsidendist tuleb eri õigusaktides sätestatud teatamiskohustuse tõttu teavitada eri asutusi. Sellised olukorrad tekitavad lisakoormust ning võivad põhjustada kõnealuste teadete vormi ja menetluskorraga seoses ebakindlust. Kui luuakse ühtne kontaktpunkt, julgustatakse liikmesriike kasutama seda ühtset kontaktpunkti ka selleks, et teatada turvaintsidentidest, millest teatamist nõutakse muude liidu õigusaktide, näiteks määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ kohaselt. Sellise ühtse kontaktpunkti kasutamine turvaintsidentidest teatamiseks määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ alusel ei tohiks mõjutada määruse (EL) 2016/679 ja direktiivi 2002/58/EÜ sätete, eelkõige nendes osutatud asutuste sõltumatust käsitlevate sätete kohaldamist. ENISA peaks koostöös koostöörühmaga töötama suunistes välja ühised teatevormid, et lihtsustada ja ühtlustada liidu õiguse alusel teabe esitamist ning vähendada teavitavate üksuste halduskoormust.
(107) Liikmesriigid peaksid liidu õigusega kooskõlas olevatest kriminaalmenetlusnormidest lähtuvalt julgustama elutähtsaid[140] ja olulisi üksusi, kes kahtlustavad, et intsident on seotud liidu või liikmesriigi õiguses määratletud raske kuriteoga, teatama nendest arvatavalt raske kuritegevusega seotud intsidentidest asjakohastele õiguskaitseasutustele. Kui see on asjakohane, võiksid küberkuritegevuse vastase võitluse Euroopa keskus (EC3) ja ENISA hõlbustada eri liikmesriikide pädevate asutuste ja õiguskaitseasutuste vahelise koostöö koordineerimist, ilma et see mõjutaks Europoli suhtes kohaldatavaid isikuandmete kaitse reegleid.
Kokkuvõttes on NIS2-direktiivi artikli 23 lõike 4 kohaselt asjaomaste teavituste sisu ja tingimused

[138] Eelnõus „üliolulised üksused".
[139] Eelnõus „üldkasutatava elektroonilise side võrgu teenuse osutajad".
[140] Eelnõus „üliolulisi üksusi".

(millega on kavas ka siseriiklik õiguskord kooskõlla viia) järgmised:

a) varajane hoiatus (eelnõus selguse huvides „esmane teade“, vt eelnõus KüTSi § 8 lõikeid 1 ja 4^1) – esitada põhjendamatu viivituseta ning hiljemalt 24 tundi pärast olulisest intsidendist teada saamist; selles teates märgitakse asjakohasel juhul teave, kas olulise intsidendi põhjus on eeldatavasti ebaseaduslik või pahatahtlik tegevus ja kas sellel võib olla piiriülene mõju; eelnõus on esmase teate sisu oma olemuselt sama, mis intsidenditeade, kuid selle erisusega, et eelnõu KüTSi § 8 lõikes 4^1 sätestatud teave esitatakse siis, kui see on olemas;

b) intsidenditeade (eelnõus samuti „intsidenditeade“, vt eelnõus KüTSi § 8 lõiget 4^2) – esitada põhjendamatu viivituseta ja hiljemalt 72 tundi pärast olulisest intsidendist teada saamist; intsidenditeates vajaduse korral ajakohastatakse varajase hoiatuse teates olevat teavet ning antakse esialgne hinnang olulisele intsidendile, sealhulgas selle tõsidusele ja mõjule ning võimaluse korral ka turvarikkemärkidele ehk rikkumisele viitavatele asjaoludele (igasugune tunnus, mis viitab rikkumise toimumisele);

c) vahearuanne (eelnõus samuti „vahearuanne“, vt eelnõus KüTSi § 8 lõiget 4^4) – kui seda soovib Riigi Infosüsteemi Amet tema määratud tähtajal (NIS2-direktiiv tähtaega ei määra). Tegemist on teavitusega, mille eesmärk on näiteks anda pikema kestusega (üle kuu vältava) küberintsidendi korral Riigi Infosüsteemi Ametile intsidendi arenguid ja käsitlemist puudutavat ajakohastatud teavet;

d) lõpparuanne (eelnõus kasutatud kehtiva seaduse sõnastuse osaliseks säilitamiseks sõna „lõppraport“, vt eelnõus KüTSi § 8 lõikeid 4^4 ja 7) – üks kuu pärast intsidenditeate esitamist; kui intsident jätkuvalt kestab, tuleb sel tähtajal esitada vahearuanne ja ühe kuu jooksul pärast intsidendi käsitlemist esitada lõpparuanne; lõpparuande sisu on: i) intsidendi, sealhulgas selle tõsiduse ja mõju üksikasjalik kirjeldus; ii) ohu liik või lähtepõhjus, mis intsidendi tõenäoliselt põhjustas; iii) juba kohaldatud ja kohaldamisel olevad leevendusmeetmed; iv) kui see on kohaldatav, siis intsidendi piiriülene mõju.

Eelnõukohase KüTSi § 8 lõikega 4^2 on kavas võtta üle NIS2-direktiivi artikli 23 lõike 4 punkt b (72 tunni intsidenditeatega seonduv). Vt selle kohta ka eelnõukohase KüTSi § 8 lõike 4^1 selgitusi seletuskirjas.

Eelnõukohase KüTSi § 8 lõikega 4^3 on kavas võtta üle NIS2-direktiivi artikli 23 lõike 4 viimane tekstilõik, millega sätestatakse teavitamiskohustuse erand, mis puudutab üksnes usaldusteenuse osutajat. Viimane peab juba 24 tunni jooksul pärast olulisest intsidendist (eelnõu tähenduses olulise mõjuga küberintsidendist) teada saamist esitama sellise teabe, mille muud teenuseosutajad peavad eelnõu kohaselt esitama alles KüTSi § 8 lõike 4^2 intsidenditeate koosseisus.

Eelnõukohase KüTSi § 8 lõikega 4^4 on kavas võtta üle NIS2-direktiivi artikli 23 lõike 4 punkt c (vahearuandega seonduv). Vt selle kohta ka eelnõukohase KüTSi § 8 lõike 4^1 selgitusi seletuskirjas. Eelnõus on KüTSi § 8 lõike 4^4 teises lauses märgitud, et vahearuandes esitatakse ka „asjakohasel juhul Riigi Infosüsteemi Ameti taotletud lisateave“, mille puhul on mõeldud seda teavet, mida võidakse küsida teenuseosutajalt lisaks konkreetse juhtumi olusid arvestades. Eelnõu järgi tekib KüTSi § 8 lõike 4^4 alusel Riigi Infosüsteemi Ametil võimalus – mitte kohustus – nimetatud vahearuannet küsida ehk ta ei pruugi seda üldse küsida, vaid võib jääda ootama teenuseosutaja esitatavat lõpparuannet (vt eelnõus KüTSi § 8 lõiget 7).

Eelnõu kohaselt KüTSi § 8 lõikes 5 tehtav muudatus (esimeses lauses) ja täiendus (teine lause) on seotud NIS2-direktiivi artikli 23 lõike 1 esimese tekstilõigu teise lause ning lõigete 2 ja 7 ülevõtmisega. Olulise mõjuga küberintsident määratletakse eelnõu kohaselt KüTSi § 8 lõikes 2,

oluline küberoht määratletakse § 2 punktis 22.

Eelnõu kohaselt KüTSi § 8 lõikes 6 tehtav muudatus on seotud NIS2-direktiivi artikli 23 lõike 7 ülevõtmisega. Võrreldes kehtiva sõnastusega on muudatuse tulemusena vaja Riigi Infosüsteemi Ametil vaja eelnevalt konsulteerida asjaomase teenuseosutajaga, kui amet ise soovib teavitada olulise mõjuga küberintsidendist. Alternatiivina on ametil õigus nõuda, et sama avalikkuse teavitamise teeb asjaomane teenuseosutaja. Siinne muudatus ei välista KüTSi § 12 lõikes 3 sätestatud Riigi Infosüsteemi Ameti volitust edastada küberintsidentidega seotud ohuteateid. Siin vt ka eelnõu KüTSi § 16 lõike 1^1 punkti 9 ja § 17 lõike 1^1 punkti 9.

Eelnõu kohaselt KüTSi § 8 lõikes 7 tehtavad muudatused (esimeses lauses) ja täiendus (teine lause) on seotud NIS2-direktiivi artikli 23 lõike 4 esimese tekstilõigu punktide d ja e ülevõtmisega. NIS2-direktiivis kasutatakse sõna „lõpparuanne“, eelnõus on aga kavas osaliselt säilitada kehtiva KüTSi termin („raport“) ja kasutada edaspidi sõna „lõppraport“.

Eelnõu kohaselt KüTSi § 8 lõikes 8 tehtav muudatus on tehniline ja seotud eelmise lõike muudatusega – edaspidi on lõikes asendatud sõna „raporti“ sõnaga „lõppraporti“, et see termin ühtiks eelnõu sama paragrahvi lõikes 7 kasutatava terminiga.

Eelnõukohase KüTSi § 8 lõikega 8^1 on kavas määrata kindlaks, et teenuseosutajad lähtuvad NIS2-direktiivi artikli 23 lõike 11 alusel antud Euroopa Komisjoni rakendusaktist, milles 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 kehtestatud nõuetest.
Euroopa Komisjon on kehtestanud rakendusaktiga erinõuded järgmiste teenuseosutajate suhtes (esitatud on eelnõus kasutatavad terminid): domeeninimede süsteemi teenuse osutajad, tippdomeeninimede registrid, pilvandmetöötlusteenuse osutajad, andmekeskusteenuse osutajad, sisulevivõrguteenuse osutajad, haldusteenuse osutajad, infoturbeteenuse osutajad, internetipõhise kauplemiskoha pidajad, veebipõhise otsingumootori pakkujad, sotsiaalmeediaplatvormi pakkujad ja usaldusteenuse osutajad.
Selle rakendusakti pealkiri on „Euroopa 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, 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“.[141]

KüTSi § 8 lõige 9 tunnistatakse eelnõu kohaselt kehtetuks, kuna kehtiva KüTSi tähenduses digitaalse teenuse osutajad (vt KüTSi kehtiva versiooni § 4 lõiget 1) on edaspidi NIS2-direktiivi ja seeläbi ka KüTSi kohaldamisalas, mistõttu puudub vajadus seda sätet säilitada.

[141] Rakendusakt jõustus 7. novembril 2024 ja on kättesaadav https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32024R2690&qid=1730728447038. Lisainfo: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14241-Cybersecurity-risk-management-reporting-obligations-for-digital-infrastructure-providers-and-ICT-service-managers_en ja https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=PI_COM:Ares(2024)4640447&qid=1728309190768.

Eelnõukohane KüTSi § 8 lõige 10 on seotud erisuse sätestamisega julgeolekuasutuste kontekstis ehk NIS2-direktiivi artikli 8 lõike 1 ülevõtmisega (vt ka eelnõus KüTSi § 5 lõiget 5). Kommenteeritava lõikega on kavas tekitada selgus, keda teavitab julgeolekuasutus küberintsidendist ehk sellises olukorras kohaldatakse eelnõu järgi KüTSi §-s 8 olevaid sätteid *mutatis mutandis* julgeolekuasutuste suhtes.

Eelnõukohase KüTSi § 8[1] lisamisega on kavas säilitada KüTSi kehtiva versiooni § 8 lõike 4 sisu ning võtta üle NIS2-direktiivi artikkel 30.

Eelnõukohase KüTSi § 8[1] lõike 1 eesmärk on luua selgus, et teenuseosutajad võivad vabatahtlikult esitada teavet küberintsidendi, turvahaavatavuse ja küberohu kohta ning muud isikud võivad esitada teavet olulise mõjuga küberintsidendi, turvahaavatavuse ja küberohu kohta. Küberohu ja turvahaavatavuse olemuse kohta vt eelnõus KüTSi § 2 punkte 20 ja 29 ning olulise mõjuga küberintsidendi kohta § 8 lõiget 2, sh selle täiendust. Selguse huvides väärib märkimist, et iga isik võib ükskõik mis ajal teavitada Riigi Infosüsteemi Ametit ükskõik millisest küberruumis avaldunud ohust või tekkinud ohukahtlusest, ilma et ta teaks või peaks teadma, milline juriidiline/erialane termin teavitatavat asjaolu täpselt kirjeldab. Seetõttu võiks eelnõus kavandatava vabatahtliku teavitamise reguleerimise vajaduse esmapilgul tervikuna kahtluse alla seada. Nii see siiski ei ole, sest NIS2-direktiivi artikli 30 lõike 2 järgi tuleb pädeval asutusel (Riigi Infosüsteemi Amet) teatud teavituste puhul (millest kõnealune paragrahv räägibki) järgida kindlaksmääratud menetluskorda, mis eelnõu järgi sätestatakse paragrahvides 8 ja 12. Samuti on KüTSi teenuseosutajate hulgas avaliku sektori üksusi, kelle puhul tagab kommenteeritav paragrahv selguse (volituse), et nad võivad teavitada Riigi Infosüsteemi Ametit ka muudest juhtumitest kui ainult olulise mõjuga küberintsidendist.
Seoses turvahaavatavusest (NIS2-direktiivi sõnastuses „nõrkustest“) teavitamisega on siin asjakohased NIS2-direktiivi põhjendused 58–63:
(58) Kuna võrgu- ja infosüsteemide nõrkuste ärakasutamine võib põhjustada suuri häireid ja olulist kahju, on selliste nõrkuste kiire tuvastamine ja kõrvaldamine riskide vähendamise tähtis tegur. Üksused, mis võrgu- ja infosüsteeme välja töötavad või haldavad, peaksid seetõttu kehtestama asjakohase korra, mille alusel nõrkuste avastamise korral neid käsitleda. Kuna nõrkusi avastavad ja avalikustavad sageli kolmandad isikud, peaks IKT-toodete või IKT-teenuste tootja või osutaja kehtestama ka vajaliku menetluskorra kolmandatelt isikutelt nõrkusi käsitleva teabe saamiseks. Suunised nõrkuste käsitlemiseks ja nende avalikustamiseks on esitatud rahvusvahelistes standardites ISO/IEC 30111 ja ISO/IEC 29147. Selleks et soodustada nõrkuste avalikustamise vabatahtlikku raamistikku, on eriti oluline tugevdada füüsiliste ja juriidiliste isikute ning IKT-toodete või IKT-teenuste tootjate või osutajate vahelise koostöö koordineerimist. Nõrkuste koordineeritud avalikustamise all peetakse silmas struktureeritud protsessi, mille käigus teatatakse potentsiaalselt nõrkade IKT-toodete või IKT-teenuste tootjale või osutajale nõrkustest viisil, mis võimaldab neil nõrkust diagnoosida ja selle kõrvaldada enne, kui nõrkusega seotud üksikasjalik teave avalikustatakse kolmandatele isikutele või üldsusele. Nõrkuste koordineeritud avalikustamise protsess peaks hõlmama ka füüsiliste ja juriidiliste isikute ning potentsiaalselt nõrkade IKT-toodete või IKT-teenuste tootja või osutaja vahelist koordineerimist nõrkuste kõrvaldamise ja avalikustamise ajastamise asjus.
(59) Komisjon, ENISA ja liikmesriigid peaksid ka edaspidi edendama küberturvalisuse riskijuhtimise valdkonna rahvusvaheliste standardite ja tööstusvaldkonna praeguste parimate tavadega kooskõla saavutamist, näiteks tarneahela turvalisuse hindamise, teabevahetuse ja nõrkuste avalikustamise valdkonnas.
(60) Liikmesriigid peaksid võtma koostöös ENISAga meetmeid, et nõrkuste koordineeritud

avalikustamist hõlbustada, kehtestades selleks asjakohase riikliku poliitika. Oma riikliku poliitika raames peaksid liikmesriigid kooskõlas oma õigusega püüdma võimalikult suures ulatuses lahendada probleeme, millega puutuvad kokku nõrkuste valdkonnas uuringuid läbi viivad isikud, sealhulgas probleeme, mis on seotud nende võimaliku kriminaalvastutusega. Võttes arvesse, et mõnes liikmesriigis võib nõrkuste valdkonnas uuringuid läbi viivate füüsiliste ja juriidiliste isikute suhtes kohaldada kriminaal- ja tsiviilvastutust, soovitatakse liikmesriikidel võtta vastu suunised, mis käsitlevad infoturbeuurijate nende tegevuse eest vastutusele võtmisest loobumist ja tsiviilvastutusest vabastamist.
(61) Liikmesriigid peaksid määrama ühe oma CSIRTidest koordinaatoriks, kes tegutseb vajaduse korral usaldatud vahendajana teavitavate üksuste ja IKT-toodete või IKT-teenuste tootjate või osutajate vahel, keda nõrkus tõenäoliselt mõjutab. Koordinaatoriks määratud CSIRTi ülesanneteks peaks eelkõige olema teha kindlaks asjaomased üksused ja võtta nendega ühendust, toetada nõrkusest teavitavaid füüsilisi ja juriidilisi isikuid, pidada läbirääkimisi avalikustamise tähtaegade üle ning hallata mitmeid üksusi mõjutavate nõrkustega seonduvat tegevust (mitut poolt puudutavate nõrkuste koordineeritud avalikustamine). Kui teatatud nõrkus võib oluliselt mõjutada üksusi rohkem kui ühes liikmesriigis, peaksid koordinaatoriks määratud CSIRTid tegema, kui see on kohane, koostööd CSIRTide võrgustiku raames.
(62) Juurdepääs õigele ja õigeaegsele teabele IKT-tooteid ja IKT-teenuseid mõjutavate nõrkuste kohta aitab küberturvalisuse riskijuhtimist tõhustada. Nõrkuste kohta avalikult kättesaadava teabe allikad on üksuste ja nende teenuste kasutajate, aga ka riiklike pädevate asutuste ja CSIRTide jaoks oluline vahend. Sel põhjusel peaks ENISA looma Euroopa nõrkuste andmebaasi, kus üksused, olenemata sellest, kas nad kuuluvad [NIS2-direktiivi] kohaldamisalasse, ja nende võrgu- ja infosüsteemide tarnijad, ning pädevad asutused ja CSIRTid võivad üldtuntud nõrkusi vabatahtlikult avalikustada ning registreerida, mis võimaldab kasutajatel võtta asjakohaseid leevendusmeetmeid. Andmebaasi eesmärk on käsitleda ainulaadseid probleeme, mida riskid liidu üksustele tekitavad. Ühtlasi peaks ENISA kehtestama avaldamisprotsessiga seoses sobiva menetluse, millega anda üksustele aega võtta oma nõrkuste kõrvaldamiseks leevendusmeetmeid ning kasutada tänapäevaseid küberturvalisuse riskijuhtimismeetmeid ning võtta kasutusele masinloetavad andmekogud ja vastavad liidesed. Selleks et edendada nõrkuste avalikustamise kultuuri, ei tohiks avalikustamisel olla nõrkusest teatavale füüsilisele või juriidilisele isikule kahjulikke tagajärgi.
(63) Kuigi sarnaseid nõrkuste registreid või andmebaase on ka juba loodud, majutavad ja haldavad neid üksused, mille asukoht ei ole liidus. ENISA hallatav Euroopa nõrkuste andmebaas tagaks nõrkuste ametlikule avalikustamisele eelneva avalikustamisprotsessi suurema läbipaistvuse ning suurendaks vastupidavust sarnaste teenuste osutamist mõjutava häire või katkestuse korral. Et vältida topelttööd ja püüda saavutada võimalikult suures ulatuses vastastikune täiendavus, peaks ENISA uurima võimalust sõlmida struktureeritud koostöökokkuleppeid kolmandate riikide jurisdiktsiooni alla kuuluvate sarnaste registrite või andmebaasidega. Eelkõige peaks ENISA uurima võimalust teha tihedat koostööd ühiste nõrkuste ja riskide süsteemi operaatoritega.

Eelnõukohase KüTSi § 8[1] lõikega 2 on kavas võtta üle NIS2-direktiivi artikli 12 lõike 1 teise tekstilõigu esimene ja teine lause.
Kommenteeritava lõigu esimene lause ei tähenda, et selles märgitud teate peab esitama anonüümselt. Ka NIS2-direktiivi artikli 12 lõikes 1 on sätestatud, et turvanõrkuste (eelnõu kohaselt turvahaavatavuse) koordineeritud avalikustamise koordinaator ehk küberintsidentide käsitlemise üksus (eelnõu kohaselt Riigi Infosüsteemi Amet, täpsemalt selle struktuuriüksus) tegutseb usaldusväärse vahendajana, hõlbustades vajaduse korral suhtlust turvahaavatavusest teavitava füüsilise või juriidilise isiku ning potentsiaalse turvahaavatavusega IKT-toodete tootja või IKT-

teenuste osutaja vahel, tegutsedes ükskõik kumma poole taotlusel, sh teeb ta kindlaks asjaomased üksused ja võtab nendega ühendust. Seega toimub eelnõu kohaselt suhtlus teate esitaja (füüsiline või juriidiline isik) ja IKT-toote tootja või IKT-teenuse osutaja vahel Riigi Infosüsteemi Ameti kaudu, mis ei tähenda ilmtingimata, et selliste teadete edastamine toimub kohustusliku nõude mõttes anonüümselt. Kommenteeritava lõike esimese lausega on kavas tagada, et kui teate esitaja seda soovib, võib ta esitada teate ka anonüümselt.
Kommenteeritava lõike teise lausega on kavas luua alus juurdepääsupiiranguks, mille pikkus juriidilisest isikust teavitaja puhul on avaliku teabe seaduse § 40 lõike 1 kohaselt kuni viis aastat (võimalik pikendada kuni viie aasta võrra) ning füüsilisest isikust teavitaja puhul avaliku teabe seaduse § 40 lõike 3 kohaselt 75 aastat. Eraisiku isikuandmete puhul on kommenteeritavas lõikes sätestatud juurdepääsupiirangu alusega koos võimalik kasutada ka avaliku teabe seaduse § 35 lõike 1 punktis 12 sätestatud juurdepääsupiirangu alust (nn andmesubjekti eraelu puutumatuse oluline kahjustamine). Viimati nimetatud juurdepääsupiirangu alus kehtib füüsilise isiku ehk andmesubjekti korral, kuid NIS2-direktiiv näeb ette, et turvahaavatuse või potentsiaalse turvahaavatuse teate esitaja võib olla ka juriidiline isik, mistõttu mainitud avaliku teabe seaduse juurdepääsupiirangu alus ei ole juriidiliste isikute puhul piisav. Kokkuvõtteks, kui asjaomast juurdepääsupiirangu alust ei looda, siis ei ole võimalik tagada NIS2-direktiivi artikli 12 lõike 1 teise tekstilõigu esimese ja teise lausega sätestatud ülevõtmist ning rakendamist ehk võimaldada Riigi Infosüsteemi Ametil tagada teate esitaja (füüsilise või juriidilise isiku) anonüümsust. Kommenteeritava lausega loodava juurdepääsupiirangu aluse puhul lähtutakse omakorda ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsiooni[142] artikli 3 lõike 1 esimese tekstilõigu punktides f (*kaitsta eraelu puutumatust ja teisi õigustatud erahuvisid*) ja g (*kaitsta äri- ja teisi majandushuvisid*) sätestatud võimalustest piirata juurdepääsu ametlikele dokumentidele. Kommenteeritavas lõikes piirdutakse ainult potentsiaalsest turvahaavatavusest või turvahaavatavusest teatamise olukordadega, kuna nende teadete esitamine on seotud NIS2-direktiivi kõnealuse artikli kohaselt ainult nimetatud olukordadega. Seetõttu ei sisalda kommenteeritav lõige teatamist küberintsidendist, olulise mõjuga küberintsidendist või küberohust.

Eelnõukohase KüTSi § 8[1] lõikega 3 on kavas võtta üle NIS2-direktiivi artikli 30 lõike 2 esimese tekstilõigu teine lause, sätestades Riigi Infosüsteemi Ameti menetluskorra juhul, kui kommenteeritava paragrahvi alusel esitatakse kõnealune teade.

KüTSi §-d 10 ja 11 tunnistatakse eelnõu kohaselt kehtetuks, kuna digitaalse teenuse osutajad kehtiva KüTSi tähenduses (vt KüTSi kehtiva versiooni § 4 lõiget 1) on edaspidi täies mahus NIS2-direktiivi ja seeläbi ka KüTSi kohaldamisalas ning lähtuvad KüTSi §-dest 7 ja 8, mistõttu puudub vajadus erisusi tekitavaid paragrahve KüTSis säilitada.

Eelnõukohase KüTSi § 12 lõikega 3[1] on kavas võtta üle NIS2-direktiivi artikli 23 lõike 5 laused 1 ja 4. Tagasiside all on mõeldud nii suuniseid kui ka nõu, kuidas olulise mõjuga küberintsidendi käsitlemisel edasi toimetada, samuti ka juhiseid, kuidas konkreetse juhtumi korral teavitada õiguskaitseasutusi. Direktiivi eelmainitud lausetes on kasutatud sõna „üksus“ ja artikli 23 lõikes 1 on sätestatud, et küberintsidendist teatamise kohustus on elutähtsal üksusel (eelnõu mõttes üliolulisel üksusel) ja olulisel üksusel, mille ühisnimetaja on eelnõus KüTSi § 3 lõike 1 tõttu „teenuseosutaja“. Kuna NIS2-direktiivi artikli 30 lõike 2 esimene lause viitab sellele, et ka muude üksuste kui eelnõu mõttes teenuseosutajate esitatud teateid tuleb käsitada samas korras nagu KüTSi

[142] https://www.riigiteataja.ee/akt/216092020001

§ 8 alusel esitatud olulise mõjuga küberintsidendiga seotud teateid, ei ole kommenteeritavas lõikes võimalik sõna „teenuseosutaja“ kasutada – see säte kui menetluskord kohaldub ka nende üksuste esitatud teadetele, kes ei pea kohustuslikus korras KüTSi nõudeid järgima. See siiski ei tähenda, et Riigi Infosüsteemi Ametil lasub kohustus kõikide esitatud teadete puhul tagasisidet anda – see nõue jääb kehtima ainult olulise mõjuga küberintsidendi olukorras.

Eelnõukohase KüTSi § 12 lõikega 3^2 on kavas võtta üle NIS2-direktiivi artikli 30 lõike 2 esimese tekstilõigu teine lause (*Liikmesriigid võivad seada kohustuslike teadete menetlemisele vabatahtlike teadete menetlemisest tähtsamale kohale.*). Kohustuslike teadete puhul on mõeldud eelnõukohase KüTSi § 8 alusel esitatavaid teateid ning vabatahtlike puhul § 8^1 alusel esitatavaid teateid. Kommenteeritava lõikega on võimalik prioriseerida kohustuslikke teateid vabatahtlike teadete ees.

KüTSi § 12 lõikes 4 tehakse eelnõu kohaselt tehniline muudatus (esimeses lauses parandatakse Euroopa Liidu Küberturvalisuse Ameti nimetus) ning lisanduva teise lausega on kavas võtta üle NIS2-direktiivi artikli 23 lõike 6 esimene ja teine lause ning kaudselt ka sama artikli lõige 8.

Eelnõukohase KüTSi § 12 lõikega 4^1 on kavas võtta üle NIS2-direktiivi artikli 23 lõike 9 esimene lause. Esmakordse teavituse kohta vt eelnõukohast KüTSi § 20 lõiget 3 ning sellega seotud selgitusi.
NIS2-direktiivi artikli 4 tõttu ei kohaldata DORA määruse kohastele finantssektori üksustele erinevaid sätteid, sh ka NIS2-direktiivi 23 lõiget 1 (kohustust teavitada olulise mõjuga küberintsidendist). Samal ajal sätestab NIS2-direktiivi artikli 23 lõike 9 esimene lause, et „[ühtne] kontaktpunkt esitab ENISA-le iga kolme kuu tagant koondaruande, mis sisaldab anonüümseid koondandmeid käesoleva artikli lõike 1 ning artikli 30 kohaselt teatatud oluliste intsidentide, intsidentide, küber- ja napilt ära hoitud intsidentide kohta“. Kuna NIS2-direktiivi artikli 23 lõiget 1 (olulistest intsidentidest teavitamise kohustus) ei saa kohaldada DORA määruse kohaste finantssektori üksuste suhtes, siis ei ole eelmainitud koondaruandes võimalik kajastada ka DORA määruse artikli 19 alusel esitatud teateid. Samas näeb NIS2-direktiivi artikkel 30 (eelnõus KüTSi § 8^1) ette, et nii teenuseosutaja kui ka muu isik võib esitada teateid „oluliste intsidentide, intsidentide, küber- ja napilt ära hoitud intsidentide“ kohta. Seega, kui DORA määruse subjektiks olev finantssektori üksus siiski teavitab eelnõu kohaselt KüTSi § 8^1 alusel olulise mõjuga küberintsidendist, küberintsidendist või küberohust, siis esitab Riigi Infosüsteemi Amet eelmainitud koondaruande koosseisus Euroopa Liidu Küberturvalisuse Ametile (ENISA-le) ka kõnealust küberintsidenti või -ohtu puudutava anonüümse teabe.

KüTSi § 12 lõikes 5 tehakse eelnõu kohaselt muudatus, mille eesmärk on väljendada selgemalt Riigi Infosüsteemi Ameti kohustust kaitsta teenuseosutajate huve (sh ärisaladust) ja õigusi. Muudetud sättega on kavas võtta üle NIS2-direktiivi artikli 2 lõige 13. Võrreldes kommenteeritava lõike kehtiva sõnastusega ei kasutata eelnõus lõike tekstis sõnastust „digitaalse teenuse osutaja“, kuna need üksused on täies mahus NIS2-direktiivi ja seeläbi ka KüTSi kohaldamisalas ehk nad on „teenuseosutajad“. Seetõttu puudub vajadus neid uuesti välja tuua või nimetada.

Eelnõuga luuakse **KüTSi § 12^1**, mis on seotud nii NIS2-direktiivi artikli 9 lõigetega 3–5 kui ka põhjendustega 68–73:
(68) Liikmesriigid peaksid aitama kaasa komisjoni soovituses (EL) 2017/1584 ette nähtud küberturvalisuse kriisidele reageerimise ELi raamistiku loomisele olemasolevate koostöövõrgustike, eelkõige Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikule (EU-CyCLONe), CSIRTide võrgustiku ja koostöörühma tegevuse kaudu. EU-CyCLONe ja CSIRTide

võrgustik peaksid tegema koostööd menetluskorra alusel, milles määratakse kindlaks kõnealuse koostöö üksikasjad, ning vältima ülesannete dubleerimist. EU-CyCLONe menetluskorras tuleks täpsustada võrgustiku toimimist puudutav kord, muu hulgas rollid, koostööviisid, teiste asjaomaste osalejatega suhtlemine, teabevahetuse vormid ja kommunikatsioonivahendid. Liidu tasandi kriisiohje puhul peaksid asjaomased pooled lähtuma nõukogu rakendusotsuses (EL) 2018/1993 sätestatud kriisidele poliitilist reageerimist käsitlevast ELi integreeritud korrast (edaspidi „IPCRi kord"). Komisjon peaks selleks rakendama üldise kiirhoiatussüsteemi ARGUS kõrgetasemelise valdkondadevahelise kriisikoordineerimise menetlusprotsessi. Kui kriisil on oluline välispoliitiline või ühise julgeoleku- ja kaitsepoliitikaga seotud mõõde, tuleks käivitada Euroopa välisteenistuse kriisidele reageerimise mehhanism.

(69) Soovituse (EL) 2017/1584 lisa kohaselt tuleks ulatusliku küberturbeintsidendina mõista intsidenti, mille põhjustatud häired on niivõrd laialdased, et ühe liikmesriigi suutlikkusest nendega toimetulekuks ei piisa, või millel on märkimisväärne mõju vähemalt kahele liikmesriigile. Olenevalt nende põhjusest ja mõjust võivad ulatuslikud küberturbeintsidendid eskaleeruda ning muutuda täieulatuslikuks kriisiks, mis takistab siseturu tõrgeteta toimimist või kujutab endast mitme liikmesriigi või kogu liidu üksustele või kodanikele tõsist avaliku julgeoleku- või turvalisusriski. Võttes arvesse selliste intsidentide ulatuslikku haaret ja (enamikul juhtudel) piiriülest laadi, peaksid liikmesriigid ning asjaomased liidu institutsioonid, organid ja asutused tegema koostööd nii tehnilisel, operatiiv- kui ka poliitilisel tasandil, et reageerimist liidu ulatuses nõuetekohaselt koordineerida.

(70) Liidu tasandi ulatuslike küberturbeintsidentide ja kriiside puhul tuleb kiire ja tõhusa reageerimise tagamiseks võtta koordineeritud meetmeid, kuna sektorite ja liikmesriikide omavaheline sõltuvus on väga suur. Kübervastupidavusvõimeliste võrgu- ja infosüsteemide olemasolu ning andmete kättesaadavus, konfidentsiaalsus ja terviklus on väga olulised liidu julgeoleku ning liidu kodanike, ettevõtjate ja institutsioonide kaitsmiseks intsidentide ja küberohtude eest ning samuti selleks, et suurendada üksikisikute ja organisatsioonide usaldust liidu võimekuse vastu edendada ja kaitsta üleilmset, avatud, vaba, stabiilset ja turvalist küberruumi, mis põhineb inimõigustel, põhivabadustel, demokraatial ja õigusriigil.

(71) EU-CyCLONe peaks ulatuslike küberturbeintsidentide ja kriiside korral toimima vahendajana tehnilise ja poliitilise tasandi vahel ning tõhustama operatiivtasandi koostööd ja toetama otsuste tegemist poliitilisel tasandil. Võttes arvesse komisjoni pädevust kriisiohje valdkonnas, peaks EU-CyCLONe koostöös komisjoniga tuginema CSIRTide võrgustiku järeldustele ja kasutama oma võimekust, et koostada ulatuslike küberturbeintsidentide ja kriiside mõjuanalüüs.

(72) Küberründed on oma olemuselt piiriülesed ning oluline intsident võib häirida ja kahjustada elutähtsaid teabetaristuid, millest sõltub siseturu sujuv toimimine. Kõigi asjaomaste osalejate rolli käsitletakse soovituses (EL) 2017/1584. Lisaks vastutab komisjon Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL loodud liidu elanikkonnakaitse mehhanismi raames üldiste valmisolekumeetmete eest, mis hõlmavad hädaolukordadele reageerimise koordineerimiskeskuse ning ühise hädaolukordade side- ja infosüsteemi haldamist, olukorrateadlikkuse ja analüüsivõime säilitamist ja edasiarendamist ning liikmesriigi või kolmanda riigi abitaotluse korral eksperdirühmade mobiliseerimise ja lähetamise võimekuse loomist ja haldamist. Komisjon vastutab ka rakendusotsuse (EL) 2018/1993 kohase IPCRi korra analüüsiaruannete esitamise eest, muu hulgas seoses küberturvalisuse olukorrateadlikkuse ja valmisolekuga, samuti olukorrateadlikkuse ja kriisidele reageerimisega põllumajanduse, ebasoodsate ilmastikutingimuste, konfliktide kaardistamise ja prognooside, loodusõnnetuste varajase hoiatamise süsteemide, tervisealaste hädaolukordade, nakkushaiguste seire, taimetervise, keemiliste ainetega seotud juhtumite, toidu- ja söödaohutuse, loomatervise, rände, tolli, tuumaavariide ja kiirguslike avariiolukordade ning energeetika valdkonnas.

(73) Kui see on asjakohane, võib liit kooskõlas ELi toimimise lepingu artikliga 218 sõlmida kolmandate riikide või rahvusvaheliste organisatsioonidega rahvusvahelisi lepinguid, mis võimaldab neil osaleda ja korraldada osalust mõningates koostöörühma, CSIRTide võrgustiku ning EU-CyCLONe tegevuses. Selliste lepingutega tuleks tagada liidu huvid ja piisaval tasemel andmekaitse. See ei tohiks välistada liikmesriikide õigust teha nõrkuste haldamisel ja küberturvalisuse riskijuhtimisel koostööd kolmandate riikidega, hõlbustades liidu õiguse kohast teatamist ja üldist teabevahetust.

Eelnõukohase KüTSi § 12[1] lõikega 1 on kavas võtta üle NIS2-direktiivi artikli 9 lõige 3, tehes viite nii KüTSi §-le 12 kui ka muudele valdkondlikele seadustele. Menetluslikud raamid kriisiolukorra (sh küberturvalisuse valdkonnaga seotud kriisiolukorra) lahendamiseks on juba olemas hädaolukorra seaduses, mida tulevikus asendab tsiviilkriisi ja riigikaitseseadus ehk kõnealuse eelnõu koostamise aja seisuga need ongi „muud valdkondlikud seadused". Kommenteeritava lõike all mõeldakse ka neid meetmeid ja mehhanisme, mis on ette nähtud Euroopa Parlamendi ja nõukogu määruses (EL) 2025/38, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks, ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus).[143] Nimetatud määrus jõustus 15.01.2025. Seetõttu puudub siin kommenteeritava eelnõuga praegu vajadus ja võimalus seda teemat veel reguleerida. Kui see vajadus peaks tekkima, valmistatakse sel teemal ette asjakohane väljatöötamiskavatsus või eelnõu.

Eelnõukohase KüTSi § 12[1] lõikega 2 on kavas võtta üle NIS2-direktiivi artikli 9 lõige 4 ja lõike 5 teine lause ehk anda kommenteeritava lõikega Riigi Infosüsteemi Ametile ülesanne 1) koostada ja vastu võtta ulatuslike küberintsidentide ning kriiside lahendamise kava, arvestades NIS2-direktiivi artikli 9 lõikes 4 olevaid nõudeid ja 2) teavitada selle kava vastuvõtmisest või kavas tehtavatest muudatustest selles punktis toodud sätete kohaselt. Kommenteeritava lõikega on seotud ka NIS2-direktiivi artikli 9 lõike 5 kolmas lause ehk siin kohaldub eelnõu järgi ka KüTSi § 12 lõike 4 esimese lause lõpp („/---/ kui edastatav teave ei kahjusta riigi julgeolekut või kriminaalmenetlust.").
Kommenteeritav paragrahv on kaudselt seotud ka delegeeritud määruse (EL) 2024/1366 artikli 41 (küberkriisi ohjamise ja kriisile reageerimise kavad) lõikega 3: „3. Direktiivi (EL) 2022/2555 artikli 9 lõike 4 kohaselt nõutavat riiklikku ulatuslike küberturbeintsidentide ja kriiside lahendamise kava loetakse käesoleva artikli kohaseks riiklikuks küberkriisi ohjamise kavaks, kui selles sisalduvad piiriüleste elektrivoogude teemalised kriisiohje- ja reageerimismeetmed."

Eelnõukohase KüTSi § 12[1] lõike 3 eesmärk on määrata, et kõnealuse kava võib teha ka muu dokumendi osana ehk praktikas hädaolukorra seaduse (tulevikus tsiviilkriisi ja riigikaitseseaduse) ja selle alusel kehtestatud määruse alusel koostatava hädaolukorra lahendamise plaanina või selle osana.

Eelnõuga KüTSi § 13 lõikes 1 kavandatavad muudatused on seotud NIS2-direktiivi artiklitega 12 ja 30 (vt eelnõus KüTSi § 8[1]), kuna eelnõus nimetatud nõude järgi tuleb Riigi Infosüsteemi Ametile esitada mh ka teave küberohtude ja turvahaavatavuse kohta, mistõttu nähakse kommenteeritavas paragrahvis tehtavate muudatustega ette, et need kantakse küberintsidentide registrisse.

Eelnõukohane KüTSi § 13 lõige 1[1] on kavas lisada vajaduse tõttu määrata seaduse tasandil

[143] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32025R0038

kindlaks andmekoosseisud, mida küberintsidentide register peab kavandatavate KüTSi §-de 8 või 8^1 kohase teataja kohta kajastama, et Riigi Infosüsteemi Ametil oleks võimalik täita endal õigusaktide, sh KüTSi ja ameti põhimääruse järgi lasuvaid ülesandeid, sealhulgas, kuid mitte üksnes ohuteadete edastamise, kahjulike mõjude leviku ennetamise ning järelevalvetoimingute tegemisega seotud ülesandeid. Võrreldes registri põhimääruses sätestatuga on üldistatult tegemist samade andmekoosseisudega.
Andmeandja puhul on siin ka seos avaliku teabe seaduse § 435 lõikega 2, mille kohaselt on andmeandjaks „riigi- või kohaliku omavalitsuse asutused või muud avalik-õiguslikud või eraõiguslikud isikud, kui neil on seadusega või selle alusel antud õigusaktiga sätestatud kohustus andmekogusse andmeid esitada või kui nad teevad seda vabatahtlikult".

KüTSi § 13 lõikes 3 kavandatav muudatus on sõnastuslik ega ole iseseisva õigusliku mõjuga. Tegemist on tehnilise muudatusega, kuna andmekogu asutatakse seadusega (konkreetsel juhul on see register asutatud kommenteeritava paragrahvi alusel), mitte ei asuta seda minister määrusega.

Eelnõuga KüTSi §-le 13 lisatavad lõiked 4 ja 5 määravad kindlaks i) asjaolud, mis tuleb küberintsidentide registri põhimääruses täpsustada, kuna kehtiv registri põhimääruse volitusnorm neid asjaolusid ei sisalda, ning ii) registriandmete ja registris tehtavate toimingute andmete maksimaalse säilitustähtaja. Säilitamistähtaja puhul tuuakse registri põhimääruses olevad säilitamistähtajad seaduse tasandile. Seega on kommenteeritavate lõigete sõnastuses on lähtutud registri põhimääruses sätestatud normidest. Näiteks on andmeandja all mõeldud avaliku teabe seaduse § 43^5 lõike 2 kohast andmeandjat ehk nendeks on „riigi- või kohaliku omavalitsuse asutused või muud avalik-õiguslikud või eraõiguslikud isikud, kui neil on seadusega või selle alusel antud õigusaktiga sätestatud kohustus andmekogusse andmeid esitada või kui nad teevad seda vabatahtlikult". Registri põhimäärusega seotud muudatused on lisatud sellele seletuskirjale valdkonna eest vastutava ministri määruse kavandina.

KüTSi §-s 13^1 kavandatav muudatus on tehniline, kuna esimene viide määrusele (EL) 2019/881 tehakse eelnõu kohaselt KüTSi § 2 punktis 8.

KüTSi § 14 lõige 2 tunnistatakse eelnõu kohaselt kehtetuks, kuna kehtiva KüTSi tähenduses digitaalse teenuse osutajad (vt KüTSi kehtiva versiooni § 4 lõiget 1) on edaspidi NIS2-direktiivi ja seeläbi ka täies mahus KüTSi kohaldamisalas ning Riigi Infosüsteemi Amet teeb nende üle järelevalvet samadel alustel nagu ka teiste teenuseosutajate puhul.

KüTSi § 14 lõikesse 5 lisatakse eelnõu kohaselt teine lause, et tekitada selgus, mis õigusnorme ja nendega seotud selgitusi kohaldatakse *mutatis mutandis* julgeolekuasutuse suhtes, kui ta teeb sama lõike esimese lause kohaselt haldusjärelevalvet. Seetõttu ei ole ka viidatud õigusnormide selgitustes üle korratud, et asjaomast sätet kohaldatakse ka julgeolekuasutuse suhtes.

Eelnõuga KüTSi §-le 14 lisatavad lõiked 6–8 on seotud järelevalve tegemise aspektide kindlaks määramisega. Siin on ka seos NIS2-direktiivi põhjendustega 122–127 ja 133–135:
(122) Et tugevdada järelevalvevolitusi ja -meetmeid, mis aitavad tagada nõuete tõhusat täitmist, tuleks [NIS2-direktiiviga] ette näha minimaalsed järelevalvemeetmed ja -vahendid, mille abil pädevad asutused saavad teha elutähtsate[144] ja oluliste üksuste üle järelevalvet. Lisaks tuleks

[144] Eelnõus „ülioluliste üksuste".

[NIS2-direktiiviga] kehtestada eraldi järelevalvekord elutähtsate[145] ja oluliste üksuste jaoks, et tagada kõnealuste üksuste ja pädevate asutuste kohustuste vahel õiglane tasakaal. Seetõttu tuleks elutähtsate[146] üksuste suhtes kohaldada põhjalikku eel- ja järelkontrolliga järelevalvekorda, samal ajal kui oluliste üksuste suhtes tuleks kohaldada lihtsustatud, üksnes järelkontrolliga järelevalvekorda. Olulistelt üksustelt ei peaks seega nõudma, et nad dokumenteeriksid süstemaatiliselt küberturvalisuse riskijuhtimise nõuete täitmist. Pädevad asutused peaksid rakendama järelevalve tegemisel tagantjärele reageerimisel põhinevat lähenemisviisi ja seega ei peaks neil olema üldist kohustust nende üksuste üle järelevalvet teha. Oluliste üksuste järelkontrolli võib algatada lähtuvalt tõenditest, vihjetest või teabest, millele on juhitud pädevate asutuste tähelepanu ja mille puhul pädevad asutused leiavad, et need viitavad [NIS2-direktiivi] võimalikele rikkumistele. Selliseid tõendeid, vihjeid või teavet võivad pädevatele asutustele esitada näiteks muud asutused, üksused, kodanikud, meedia või muud allikad, see võib olla avalikult kättesaadav teave või tuleneda muust pädevate asutuste tegevusest oma ülesannete täitmisel.

(123) Järelevalveülesannete täitmine pädevate asutuste poolt ei tohiks asjaomase üksuse äritegevust tarbetult takistada. Kui pädevad asutused täidavad elutähtsate[147] üksustega seotud järelevalveülesandeid, näiteks teevad kohapealseid kontrolle ja kaugjärelevalvet, uurivad [NIS2-direktiivi] rikkumisi, viivad läbi turvaauditeid või turvalisuse kontrolle, peaks nende mõju asjaomase üksuse äritegevusele olema võimalikult väike.

(124) Eelkontrolli tegemisel peaks pädevatel asutustel olema võimalik otsustada, kuidas nad prioriseerivad proportsionaalselt järelevalvemeetmete ja oma käsutuses olevate vahendite kasutamist. See tähendab, et pädevad asutused võivad sellise prioriseerimise üle otsustada lähtuvalt järelevalvemeetoditest, mis peaksid põhinema riskipõhisel lähenemisviisil. Täpsemalt võiksid sellised meetodid sisaldada kriteeriume või võrdlusaluseid oluliste üksuste liigitamiseks riskikategooriatesse ning vastavaid järelevalvemeetmeid ja -vahendeid, mida soovitatakse iga riskikategooria kohta, nagu kohapealsete kontrollide või sihipäraste turvaauditite või turvalisuse kontrollide kasutamine, sagedus või liigid, taotletava teabe liik ja selle teabe üksikasjalikkuse aste. Selliste järelevalvemeetoditega võivad kaasneda ka tööprogrammid ning neid võidakse korrapäraselt hinnata ja läbi vaadata, sealhulgas seoses vahendite jaotamise ja vajadustega. Avaliku halduse üksuste puhul tuleks järelevalvevolitusi teostada kooskõlas riiklike õigus- ja institutsiooniliste raamistikega.

(125) Pädevad asutused peaksid tagama, et elutähtsate[148] ja oluliste üksustega seotud järelevalveülesandeid täidavad koolitatud spetsialistid, kellel peaksid olema nende ülesannete täitmiseks vajalikud oskused, eelkõige seoses kohapealsete kontrollide ja kaugjärelevalvega, sealhulgas andmebaaside, riistvara, tulemüüride, krüpteerimise ja võrkude nõrkuste tuvastamisega. Neid kontrolle ja järelevalvet tuleks teha objektiivselt.

(126) Piisavalt põhjendatud juhtudel, kui pädev asutus on teadlik olulisest küberohust või vahetust riskist, peaks pädeval asutusel olema võimalik teha viivitamata täiteotsuseid, et intsidenti ära hoida või see lahendada.

(127) Et täitmine tõhusalt tagada, tuleks koostada [NIS2-direktiivis] sätestatud küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rikkumise korral miinimumloetelu täitmise tagamise volitustest, mida võib kasutada, ning kehtestada selliste täitmise tagamise jaoks kogu liidus selge ja ühtne raamistik. Igakülgset tähelepanu tuleks pöörata [NIS2-direktiivi] rikkumise laadile, tõsidusele ja kestusele, põhjustatud varalisele või mittevaralisele kahjule, sellele, kas rikkumine oli tahtlik või tingitud hooletusest, varalise või mittevaralise kahju vältimiseks või leevendamiseks

[145] Eelnõus „üliolulise üksuste“.
[146] Eelnõus „üliolulise üksuste“.
[147] Eelnõus „üliolulise üksuste“.
[148] Eelnõus „üliolulise üksuste“.

võetud meetmetele, vastutuse tasemele ja varasematele asjaomastele rikkumistele, pädeva asutusega tehtava koostöö tasemele ning muule raskendavale või leevendavale tegurile. Sellised täitemeetmed, sealhulgas haldustrahvid, peaksid olema proportsionaalsed ja nende määramise suhtes tuleks kooskõlas liidu õiguse üldpõhimõtete ja Euroopa Liidu põhiõiguste hartaga (edaspidi „harta") kohaldada asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust.
(133) Et veelgi suurendada kohaldatavate täitemeetmete tõhusust ja hoiatavust [NIS2-direktiivi] rikkumiste korral, peaks pädevatel asutustel olema õigus ajutiselt peatada või nõuda, et ajutiselt peatataks elutähtsa[149] üksuse osutatavate mõnede või kõigi asjakohaste teenuste või pakutavate tegevuste sertifikaat või luba, ning nõuda, et füüsilisele isikule, kes täidab juhtimisülesandeid üksuse tegevjuhi või seadusliku esindaja tasandil, kehtestataks ajutine juhtimisülesannete täitmise keeld. Võttes arvesse ajutiste peatamiste ja keeldude karmust ja mõju üksuste tegevusele ning seeläbi ka nende tarbijatele, tuleks neid kohaldada alati proportsionaalselt rikkumise raskusega ning iga juhtumi konkreetseid asjaolusid silmas pidades, sealhulgas seda, kas rikkumine oli tahtlik või tulenes ettevaatamatusest, ning seda, milliseid meetmeid varalise või mittevaralise kahju vältimiseks või vähendamiseks võeti. Selliseid ajutisi peatamisi ja keelde tuleks kohaldada üksnes viimase abinõuna, nimelt alles pärast seda, kui muud [NIS2-direktiivis] sätestatud asjakohased täitemeetmed on ammendatud, ja ainult seni, kuni üksus, kelle suhtes neid kohaldatakse, võtab vajalikud meetmed puuduste kõrvaldamiseks või täidab pädeva asutuse need nõuded, millega seoses niisuguseid ajutisi peatamisi ja keelde kohaldati. Selliste ajutiste peatamiste või keeldude määramise suhtes peaks kohaldama kooskõlas liidu õiguse üldpõhimõtete ja hartaga asjakohaseid menetluslikke tagatisi, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust.
(134) Selleks et tagada, et üksused täidavad [NIS2-direktiivis] sätestatud kohustusi, peaksid liikmesriigid seoses järelevalve- ja täitemeetmetega tegema üksteisega koostööd ja üksteist abistama, eelkõige juhul, kui üksus osutab teenuseid rohkem kui ühes liikmesriigis või kui tema võrgu- ja infosüsteemid asuvad muus liikmesriigis kui see, kus ta teenuseid osutab. Abi osutamisel peaks taotluse saanud pädev asutus võtma järelevalve- või täitemeetmeid kooskõlas riigisisese õigusega. Selleks et tagada [NIS2-direktiivi] kohase vastastikuse abi sujuv toimimine, peaksid pädevad asutused kasutama juhtumite ja konkreetsete abitaotluste arutamise foorumina koostöörühma.
(135) Tulemusliku järelevalve ja täitmise tagamiseks, eelkõige piiriülese mõõtmega olukorras, peaks liikmesriik, kes on saanud vastastikuse abi taotluse, võtma kõnealuse taotluse piires asjakohaseid järelevalve- ja täitemeetmeid üksuse suhtes, kelle kohta taotlus tehti ja kes osutab kõnealuse liikmesriigi territooriumil teenuseid või kellel on seal võrgu- ja infosüsteem.

Eelnõukohases KüTSi § 14 lõikes 6 on kavas kindlaks määrata üldised raamid, kuidas Riigi Infosüsteemi Amet järelevalvet teeb.
Kommenteeritava lõike **esimese punktiga** on kavas võtta üle NIS2-direktiivi artikli 31 lõige 2. Sarnast prioriseerimist teeb Riigi Infosüsteemi Amet ka korrakaitseseaduse § 24 alusel tehtava ohuprognoosi korral, kuid kuna viimane on kohaldatav ainult erasektori ehk haldusväliste isikute suhtes ja NIS2-direktiiv on mõeldud kohalduma ka avaliku sektori suhtes, siis tuleb volitus Riigi Infosüsteemi Ametile anda laiemalt, kui seda näeb ette korrakaitseseadus. Siiski on kommenteeritavas lõikes märgitud ka ohuprognoos, et oleks üheselt selge, et ka see on üks lähenemisviis, millest lähtudes Riigi Infosüsteemi Amet enda tööd planeerib.
Kommenteeritava lõike **teise punktiga** on kavas võtta üle NIS2-direktiivi artikli 32 lõige 1 ehk

[149] Eelnõus „üliolulise üksuse".

sätestatakse nõue, et ülioluliste üksuste järelevalve toimub üldreeglina ennetava või järelkontrollina (*ex nunc* või *ex post*) (vt ka NIS2-direktiivi põhjendusi 122 ja 124, mis on esitatud kommenteeritava paragrahvi sissejuhatuses eespool).
Kommenteeritava lõike **kolmanda punktiga** on kavas võtta üle NIS2-direktiivi artikli 33 lõike 1 esimene lause ehk oluliste üksuste kontroll on üldreeglina järelkontroll (*ex post*) olukorras, kus saabub teave, et turvameetmete rakendamisega on probleeme või pole näiteks teatatud olulise mõjuga küberintsidendist (vt ka NIS2-direktiivi põhjendusi 122 ja 124, mis on esitatud kommenteeritava paragrahvi sissejuhatuses eespool).
Kommenteeritava lõike **neljas punkt** on eelnõu kohaselt seotud NIS2-direktiivi artikli 32 lõike 1 ja artikli 33 lõike 1 rakendamisega, sh toetab see ka kommenteeritava lõike punkti 1 (järelevalve prioriseerimisel arvestatakse riski- või ohuprognoosi) alusel edasiste järelevalvetegevuste elluviimist Riigi Infosüsteemi Ameti enda initsiatiivil.

Eelnõukohase KüTSi § 14 lõikega 7 on kavas võtta üle NIS2-direktiivi artikli 32 lõiked 1 ja 7 ning artikli 33 lõike 1 teine lause koos lõikega 5 ehk kommenteeritavas lõikes määratakse kindlaks need asjaolud ja aspektid, millest lähtutakse riiklikus ja haldusjärelevalve menetluses meetmeid kohaldades. Järelevalvemeetmete kohaldamisel arvestatakse rikkumise raskust ja rikutud nõuete olulisust, varasemaid rikkumisi, rikkumisega tekitatud kahju, rikkumisest mõjutatud isikute arvu, rikkumise toimepanija süüd ning seda, missuguseid meetmeid on teenuseosutaja rikkumise ennetamiseks võtnud. Kommenteeritava lõike punktis 1 nimetatud „rikkumise raskuse“ seletab lahti eelnõukohane KüTSi § 14 lõige 8, mis näeb ette loetelu olukordadest, mille puhul on alati tegemist raske rikkumisega.
Eraldi väärib selgitamist, et kommenteeritava lõike punktis 8 on kinnitatud tegevusjuhendite järgimise all mõeldud näiteks olukorda, kus tuleb järgida isikuandmete kaitse üldmääruse artikli 40 alusel vastu võetud toimimisjuhendit. Kommenteeritava lõike punktis 9 on ette nähtud, et üks asjaolu on mh ka järelevalveasutuse (Riigi Infosüsteemi Ameti või julgeolekuasutuse) ning teenuseosutaja vahel toimuv koostöö. See punkt on seotud NIS2-direktiivi § 32 lõike 7 punktiga h, kuid selle sõnastus *(vastutavate füüsiliste või juriidiliste isikute ja pädevate asutuste koostöö tase*) ei anna täit selgust, kas siin on eelnõu kontekstis mõeldud teenuseosutajat või selle teenuseosutaja koosseisus olevat või temaga seotud füüsilist või juriidilist isikut. Seetõttu on nimetatud punkt sõnastatud viisil, et tegemist on koostööga järelevalveasutuse ja teenuseosutaja vahel.

Eelnõukohase KüTSi § 14 lõikega 8 on kavas võtta üle NIS2-direktiivi artikli 32 lõike 7 punkti a alapunktid i–v. Tegemist on alternatiivsete olukordadega, mille puhul on tegemist raske rikkumisega eelnõukohase KüTSi § 14 lõike 7 punkti 1 tähenduses. Eraldi väärib selgitamist, et kommenteeritava lõike punktis 6 on „lubamatult ebatäpsete andmete“ puhul mõeldud olukorda, kus mingi teave on jäetud teadlikult ja põhjendamatult esitamata või rääkimata.

KüTSi § 15 lõiget 2 on kavas täiendada viitega NIS2-direktiivi artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktidele, kuna need rakendusaktid võimaldavad kehtestada ja täpsustada nõudeid, mis eelnõuga kavandatakse sätestada KüTSi §-des 7 ja 8, sh nende alusel antud määrustes. Kui nimetatud lisandust ei tehta, ei teki võimalust kasutada riiklikus järelevalvemenetluses nende rakendusaktide alusel kehtestatud nõuete täitmist kontrollides korrakaitseseaduse §-s 52 (vallasasja hoiulevõtmine) erimeedet.
Kommenteeritava lõikega seotud erimeedet ei ole võimalik kasutada julgeolekuasutusel, kuna ta ei tee riiklikku järelevalvet, sh kommenteeritavas lõikes viidatud nõuete täitmise üle (vt ka eelnõus KüTSi § 14 lõiget 5). Samuti ei ole nende erimeetmete kasutamise õigust Tarbijakaitse ja Tehnilise Järelevalve Ametil, kuna nimetatud amet ei tee järelevalvet kommenteeritavas lõikes viidatud

nõuete täitmise üle (vt ka KüTSi § 14 lõiget 4).

KüTSi §-ga 16 on nähtud ette riikliku järelevalve erisused. Säte on tugevalt seotud KüTSi §-ga 14, mis reguleerib üldiselt riiklikku ja haldusjärelevalvet, ning KüTSi §-ga 15, mis loetleb üles need korrakaitseseaduses sätestatud riikliku järelevalve erimeetmed, mida korrakaitseorgan võib KüTSi alusel riikliku järelevalve tegemisel kohaldada. Haldusjärelevalve jaoks nähakse sarnane regulatsioon eelnõu järgi ette KüTSi §-s 17.
Kooskõlastusele saadetud eelnõu lähtus mõnevõrra teistsugusest struktuurist. Nimelt olid selles eelnõu versioonis Riigi Infosüsteemi Ametile järelevalve tegemisel ette nähtud õigused ja kohustused sätestatud suuresti KüTSi §-s 14. See tekitas aga eelnõu kooskõlastamise käigus küsimusi KüTSis ette nähtud lahenduse ja korrakaitseõiguse omavahelistest seostest, kuivõrd ei olnud selge, kas tegemist on korrakaitseseaduse mõttes riikliku järelevalve erimeetmetega või mitte. Eriti teravalt tõusis see küsimus üles sihipärase turvaauditi tegemise ja selle selgelt erimeetmena sätestamisega. Selleks et sobitada uuendatava KüTSi regulatsioon paremini üldisesse korrakaitseõiguse raamistikku, on eelnõu eelmises versioonis KüTSi § 14 lõike 9 jj lõiked toodud üle eelnõu uues versioonis KüTSi §-desse 16 ja 17.
Sellise struktuuriga, kus eelnõu kohaselt on KüTSi § 15 korrakaitseseaduse viidetele tuginev erimeetmete säte ja muud erisused on reguleeritud eraldi KüTSi §-s 16, soovitakse hoida sarnast joont teiste seadustega, milles on samuti reguleeritud seoseid korrakaitseseadusega (näiteks alkoholiseadus).
Eelnõu kohaselt loetakse kehtiva KüTSi § 16 lõige 1^1 lõikeks 1^7 ja paragrahvi täiendatakse lõigetega 1^1–1^6. Lõikes 1^1 nähakse ette loetelu erimeetmetest, mida Riigi Infosüsteemi Ametil on võimalik riikliku järelevalve ülesannete täitmisel kasutada. Lõikes 1^2 antakse volitusnorm sihipärase turvaauditi täpsemate tingimuste ning sellega seotud kulude kandmise ja hüvitamise kehtestamiseks ministri määrusega. Lõigetes 1^3–1^6 nähakse ette, et üliolulisele üksusele tehtud ettekirjutuse sisuks võib olla ka turvaintsidendi ennetamiseks või heastamiseks vajalike meetmete võtmine ja lisatähtaja andmine puuduste kõrvaldamiseks ning nähakse n-ö viimase võimalusena, kui ka lisatähtaja jooksul ei ole puudusi kõrvaldatud, üliolulise üksuse suhtes kõige rangemate meetmete kohaldamist – teenuseosutajale vajaliku sertifikaadi või loa peatamist ning üliolulise üksuse juhatuse liikme volituste peatamist.

Eelnõukohase KüTSi § 16 lõikega 1^1 on kavas võtta üle NIS2-direktiivi artikli 32 lõiked 2 ja 4 ning artikli 33 lõiked 2 ja 4 ehk sätestada need meetmed, mida Riigi Infosüsteemi Amet saab kasutada riikliku järelevalve menetluses KüTSi alusel. Kommenteeritavas lõikes olevate punktide sisu võib sõltuda sellest, kas tegemist on olukorraga, kus mingi meede on kohaldatav teenuseosutajale (ehk nii üliolulisele üksusele kui ka olulisele üksusele) või ainult üliolulisele üksusele. Kui mingis NIS2-direktiivi sättes on kasutatud sõnastust „korraldus“ või „siduvad juhised“, siis eelnõus on selle all mõeldud ettekirjutust. Enne ettekirjutuse tegemist on järelevalve tegijal võimalik teha teenuseosutajale ettepanek viia oma tegevus kooskõlla õigusaktis ette nähtud nõuetega, sh oleks selle ettepaneku sisu samas sõnastuses kui ettekirjutus. Sellega antaks teenuseosutajale ka ärakuulamise ja vastuväidete esitamise võimalus ning seeläbi ka võimalus lahendada võimalikud rikkumised ettekirjutuseta. Olenevalt olukorra asjaoludest võib järelevalveasutusel tekkida ka vajadus teha kohe ettekirjutus (enne n-ö ettepanekut) rikkumine lõpetada või probleemsed asjad korda teha. Selles olukorras peab järelevalve tegija hindama, mis on sobivaim meede eesmärgi saavutamiseks.
Kommenteeritava lõike **punktides 1, 4, 5, 6, 9 ja 10** on viidatud lisaks KüTSile ka NIS2-direktiivi alusel antavatele rakendusaktidele, kuna nendes rakendusaktides võidakse kehtestada või täpsustada üldisemaid nõudeid, mis võetakse üle KüTSi §-desse 7 ja 8.

Kommenteeritava lõike **punktiga 1** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 2 punktid a ja c ning artikli 33 lõike 2 punkt a. Kommenteeritava punkti kohaselt võib teenuseosutaja suhtes teha kohapealset kontrolli või kaugjärelevalvet. Ülioluliste üksuste suhtes võib teha ka pistelist järelevalvet, mis võib olla muu hulgas ajendatud olulise mõjuga küberintsidendist või KüTSis, KüTSi alusel (näiteks KüTSi § 7 lõike 5 alusel) kehtestatud või NIS2-direktiivi artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis kehtestatud nõude rikkumisest. Pistelise järelevalve all on mõeldud ka NIS2-direktiivi artikli 32 lõike 2 punktis c ette nähtud *ad-hoc*-auditeid.
NIS2-direktiivi artiklid 32 ja 33 eristavad kolme liiki auditeid – regulaarsed, sihipärased ja *ad-hoc*-auditid (inglise keeles vastavalt *regular, targeted and ad hoc audits*). Nende rakendamine praktikas sõltub konkreetsest olukorrast. Regulaarseid auditeid tehakse teatava ajavahemiku tagant. Sihipärast auditit tehakse siis, kui järelevalveasutuse või auditeeritud organisatsiooni koostatud riskianalüüsi või muu asjakohase teabe põhjal on tekkinud vajadus auditit teha. *Ad-hoc*-audit tehakse ennekõike olukorras, kus audit ei ole planeeritud ning seda tehakse konkreetse eesmärgi või vajaduse pärast. Kommenteeritavas punktis on tähenduse mõttes ülioluliste üksuste puhul kasutatud sõnastust „pisteline järelevalve“, et see hõlmaks nii sihipärast kui ka *ad-hoc*-auditit.

Kommenteeritava lõike **punktiga 2** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 2 punkt b ja artikli 33 lõike 2 punkt b, kommenteeritava lõike **punktiga 3** NIS2-direktiivi artikli 32 lõike 2 punkt d ja artikli 33 lõike 2 punkt c.
Kommenteeritava lõike punktides 2 ja 3 on kasutatud vastavalt sõnu „turvaaudit“ (ingl *security audit*) ja „turvalisuse kontroll“ (ingl *security scan*), mis on sisult erinevad tegevused. Näiteks on AKITi kohaselt turvaauditi määratlus rahvusvahelistes standardites ISO 7498 ja ISO/IEC 2382 kui „süsteemi andmike ja toimingute sõltumatu läbivaatus ja uurimine süsteemi turvameetmete adekvaatsuse kontrolliks, kehtivatele poliitika[te]le ja tööprotseduuridele vastavuseks, turvarikete avastamiseks ning võimalike järelduvate meetme-, poliitika- ja protseduurimuudatuste soovitamiseks“.[150] Samas erineb turvalisuse kontroll oma tähenduse ja sisu poolest turvaauditist ehk esimese puhul tehtava toiminguga ei minda kontrollimisega sügavuti (nt ei kontrollita süsteemi lähtekoodi tasandil[151]), seetõttu on ka eelnõusse kavandatud asjaomaste volituste kontekstis eraldi punktid. Samas ei ole nende kahe punkti puhul mõeldud ainult turvahaavatavuse tuvastamist (võrdle NIS2-direktiivi artikli 11 lõike 3 punktiga e), vaid laiemat kontrolli, tuvastamaks järelevalvemenetluse raames, kas KüTSis sätestatud, selle alusel või NIS2-direktiivi artikli 21 lõike 5 või artikli 23 lõike 11 alusel kehtestatud nõudeid on rikutud.
Seoses sihipärase turvaauditi tegemisega on oluline selgitada ka seda, et turvaauditit tellides ei ole tegemist avalik-õigusliku ülesande delegeerimisega. Turvaaudit on välise osapoole (IT-audiitori) hinnang auditeeritava üksuse küberturvalisuse meetmetele. Riigi Infosüsteemi Amet tellib selle hinnangu audiitorilt, kuid see hinnang ei ole ametile siduv. Amet kasutab seda hinnangut enda edasises järelevalvemenetluses ja otsustab selle pinnalt nt ettekirjutuse tegemise vajaduse, kuid järelevalve tegemise õigus avalikku ülesannet täites jääb siiski talle kui pädevale asutusele. Seega avaliku ülesande delegeerimist välisele osapoolele ei toimu. Seetõttu ei sõlmita IT-audiitoritega ka halduslepingut, vaid need audiitorid, kelle teenuseid hakkab amet tulevikus kasutama, leitakse riigihanke teel ning nendega sõlmitakse eraõiguslikud teenuse osutamise lepingud.

Kommenteeritava lõike **punktiga 4** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 4 punkt a ja artikli 33 lõike 4 punkt a. Tegemist on hoiatuse tegemise meetmega, mida saab kohaldada, kui

[150] https://akit.cyber.ee/term/301-turvaaudit
[151] Turvalisuse kontrolli selgituse kohta vt nt https://www.lawinsider.com/dictionary/security-scan.

õigusaktis olevat nõuet on rikutud.

Kommenteeritava lõike **punktiga 5** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 4 punkt b ja artikli 33 lõike 4 punkt b, sh on kommenteeritavas punktis sätestatud, et selle alusel „nõutakse ettekirjutuse saajalt sellise tegevuse või tava lõpetamist, millega rikutakse [õigusaktis või selle alusel] kehtestatud nõuet“ ja lisaks saab nõuda ka „sama tegevuse või tava kasutamisest hoidumist“. Kuigi viidatud NIS2-direktiivis on sätestatud ka heastamine, hõlmab see õigusaktides või selle alusel kehtestatud nõuete rikkumisega seotud puuduste kõrvaldamist.

Kommenteeritava lõike **punktiga 6** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 4 punkt d ja artikli 33 lõike 4 punkt d.

Kommenteeritava lõike **punktiga 7** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 4 punkt e ja artikli 33 lõike 4 punkt e. Kommenteeritava lõike **punktiga 8** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 4 punkt f ja artikli 33 lõike 4 punkt f. Kommenteeritava lõike **punktiga 9** võetakse üle NIS2-direktiivi artikli 32 lõike 4 punkt h ja artikli 33 lõike 4 punkt g.
Kommenteeritava lõike punktide 7 ja 9 puhul võib tunduda, et tegemist on sisult sama teema reguleerimisega, kuid tegelikkuses nii ei ole. Eelnõukohaste KüTSi § 16 lõike 1^1 punktide 7 ja 9 sisu teatud ulatuses kattub, kuid nendes punktides on ka nõudeid, mis erinevad. Näiteks viitab punkt 7 ka parandusmeetmete info avalikustamise kohustusele, kuid punkt 9 seda aspekti ei hõlma; samuti on punktis 7 nõutav teavitus veidi kitsam ehk seal ei ole tingimata/alati mõeldud laiema avalikkuse teavitamist, kuid punkt 9 on pigem seotud laiema avalikkuse teavitamisega.
Kommenteeritava lõike punkt 7 viitab eelnõus KüTSi § 8 lõikele 5, mille sisu on eelnõu kohaselt järgmine: „Teenuseosutaja on asjakohasel juhul kohustatud teavitama mõistliku aja jooksul isikut, keda olulise mõjuga küberintsident või oluline küberoht võib mõjutada, või avalikkust, kui mõjutatud isikuid ei ole võimalik eraldi teavitada. Teates annab teenuseosutaja [võimaluse korral] teada olulisest küberohust ja meetmetest, mida mõjutatud isik saab olulisele küberohule reageerimiseks võtta.“
Kommenteeritava lõike punkt 9 viitab eelnõus KüTSi § 16 lõike 1^1 punktile 9, mille sisu on eelnõu kohaselt järgmine: „ettekirjutus, millega nõutakse ettekirjutuse saajalt käesolevas seaduses, selle alusel või Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikli 21 lõike 5 või artikli 23 lõike 11 alusel vastu võetud rakendusaktis sätestatud nõude rikkumise asjaolude avalikustamist ettekirjutuses ette nähtud viisil“.

Kommenteeritava lõike **punktiga 10** on kavas võtta üle NIS2-direktiivi artikli 32 lõike 4 punkt g, mida kohaldatakse ainult üliohuliste üksuste puhul ehk taolist meedet ei ole ette nähtud NIS2-direktiivi artiklis 33 oluliste üksuste puhul. Üle võetava NIS2-direktiivi sätte eestikeelses tõlkes on kasutatud sõna „seireametnik“, kuid eelnõus on selle asemel kasutatud sõna „vastavushaldur“. Selle sisu on selgitatud näiteks Eesti infoturbestandardi portaali rollisõnastikus kui „organisatsioonile kohaldatavate õiguslike, lepinguliste ja muude nõuete väljaselgitaja ning nende täitmise kontrollija (ingl *Compliance Manager*)“.[152] Kõnealuses ettekirjutuses tuleks ka selgelt ära määrata, mis on vastavushalduri ülesanded. See ei tähenda, et teenuseosutaja peab lähtuma Eesti infoturbestandardist, kui ta on otsustanud lähtuda rahvusvahelisest standardist ISO/IEC 27001 või kui tema riskijuhtimismeetmete (eelnõu mõttes turvameetmete) nõuded tulenevad NIS2-direktiivi artikli 21 lõike 5 alusel kehtestatud rakendusaktist.
NIS2-direktiivi kõnealuse sätte volitust saaks tõlgendada ka nii, et pädev asutus määrab

[152] https://eits.ria.ee/et/versioon/2023/eits-poohidokumendid/rollisoonastik

ettekirjutusega kindlaks konkreetse vastavushalduri, kes jälgib, kas ettekirjutuse adressaat täidab vajalikud nõuded. Niisuguse tõlgenduse puhul ei oleks seda paindlikkust, et ettekirjutuse adressaat ise saaks valida ja määrata kindlaks vastavushalduri, kes ettekirjutusega kindlaks määratud ülesannet täidab. Seetõttu on kasutatud eelnõus olevat sõnastust ja tõlgendust.

Eelnõukohasesse KüTSi § 16 lõikesse 1^2 kavandatakse volitusnorm sihipärase turvaauditi tegemise täpsemate tingimuste ning sellega seotud kulude kandmise ja hüvitamise korra kehtestamiseks ministri määrusega. Määruses nähakse täpsemalt ette korralduslikud reeglid selle kohta, kuidas Riigi Infosüsteemi Amet sihipärast turvaauditit teeb või selle audiitorilt tellib. Ameti õigus sihipäraseid turvaauditeid teha ja teenuseosutaja kohustus neile alluda tuleneb aga seadusest. NIS2-direktiivi artikli 32 lõike 2 kolmanda tekstilõigu teises lauses ja artikli 33 lõike 2 kolmanda tekstilõigu teises lauses on nähtud ette, et sõltumatu organi tehtava sihipärase turvaauditi kulu tasub auditeeritud üksus (teenuseosutaja), välja arvatud igakülgselt põhjendatud juhtudel, kui pädev asutus otsustab teisiti. Seega jääb NIS2-direktiivist tuleneva üldise põhimõtte kohaselt kulu auditeeritava üksuse kanda. Tegemist on küsimusega, mille kohta tehti eelnõu kooskõlastamisel mitu märkust, seetõttu on otsustatud auditeeritavale üksusele kulu hüvitamise täpsemad tingimused ja kord näha ette ministri määruses. Seletuskirjale on lisatud selle määruse kavand, kus aga kõik detailid ei ole veel paigas. Määruse ettevalmistamisel tuleb analüüsida ja paika panna need olukorrad või tingimused, mille puhul jääb sihipärase turvaauditi kulu auditeeritava üksuse asemel Riigi Infosüsteemi Ameti kanda, samuti ka tingimused ja kord, kuidas auditeeritav isik (teenuseosutaja) sihipärase turvaauditi eest tasub.

Eelnõukohase KüTSi § 16 lõikega 1^3 on kavas võtta üle NIS2-direktiivi artikli 32 lõike 4 punkt b, kus on lauseosa „sealhulgas meetmete kohta, mis on vajalikud intsidendi ennetamiseks või heastamiseks, nende meetmete rakendamise tähtaegade ja rakendamisest aruandmise kohta“, mis kehtib ainult ülioluliste üksuste suhtes. Oluliste üksuste kohta sellist lauseosa NIS2-direktiivi artikli 33 lõike 4 punktis b ei ole.

Eelnõukohaste KüTSi § 16 lõigetega 1^4–1^6 on kavas võtta üle NIS2-direktiivi artikli 32 lõige 5. Kavandatavad lõiked kehtivad ainult ülioluliste üksuste suhtes.

Eelnõukohases KüTSi § 16 lõikes 1^4 on kavas NIS2-direktiivi artikli 32 lõike 5 esimese tekstiosa alusel reguleerida olukorda, kus juba võetud järelevalvemeetmed ei ole olnud tulemuslikud. Selline olukord võib tekkida, kui näiteks järelevalvatav teenuseosutaja ei ole järjepidevalt talle tehtud hoiatusi arvestanud või ettekirjutusi täitnud, mistõttu ei anna varem kasutatud meetmed tulemust ehk neid ei rakendata järjepidevalt. Sellisel juhul annab Riigi Infosüsteemi Amet ülioluliselle üksusele lisatähtaja puuduste kõrvaldamiseks või ameti esitatud nõuete täitmiseks.

Eelnõukohase KüTSi § 16 lõikega 1^5 on kavas võtta üle artikli 35 lõike 5 punktid a ja b. Oluline on rõhutada, et tegemist on n-ö viimase võimaluse abinõudega, mida järelevalveasutus saab rakendada üksnes juhul, kui varem rakendatud järelevalvemeetmed ei ole andnud tulemust ning ülioluline üksus ei ole ka talle antud lisatähtaja jooksul puudust või puudusi kõrvaldanud. Lõike 1^5 punktides 1 ja 2 sätestatavate meetmete kasutamiseks peab Riigi Infosüsteemi Amet hindama, kas need on kõige sobivamad meetmed konkreetses olukorras tekkinud probleemi lahendamiseks ehk tegemist ei saa olla kergekäeliselt kasutatavate meetmetega. Seetõttu ei hakka praktikas tõenäoliselt olema tegemist tihedat rakendamist leidvate meetmetega. Sellest hoolimata ei ole ka võimalik jätta nende meetmete kasutamise volitused Eesti õiguses loomata, kuna see tooks kaasa NIS2-direktiivi ebaõige ülevõtmise.

Siinsete punktidega on seotud ka NIS2-direktiivi põhjendus 133:
(133) Et veelgi suurendada kohaldatavate täitemeetmete tõhusust ja hoiatavust [NIS2-direktiivi] rikkumiste korral, peaks pädevatel asutustel olema õigus ajutiselt peatada või nõuda, et ajutiselt peatataks elutähtsa üksuse[153] osutatavate mõnede või kõigi asjakohaste teenuste või pakutavate tegevuste sertifikaat või luba, ning nõuda, et füüsilisele isikule, kes täidab juhtimisülesandeid üksuse tegevjuhi või seadusliku esindaja tasandil, kehtestataks ajutine juhtimisülesannete täitmise keeld. Võttes arvesse ajutiste peatamiste ja keeldude karmust ja mõju üksuste tegevusele ning seeläbi ka nende tarbijatele, tuleks neid kohaldada alati proportsionaalselt rikkumise raskusega ning iga juhtumi konkreetseid asjaolusid silmas pidades, sealhulgas seda, kas rikkumine oli tahtlik või tulenes ettevaatamatusest, ning seda, milliseid meetmeid varalise või mittevaralise kahju vältimiseks või vähendamiseks võeti. Selliseid ajutisi peatamisi ja keelde tuleks kohaldada üksnes viimase abinõuna, nimelt alles pärast seda, kui muud [NIS2-direktiivis] sätestatud asjakohased täitemeetmed on ammendatud, ja ainult seni, kuni üksus, kelle suhtes neid kohaldatakse, võtab vajalikud meetmed puuduste kõrvaldamiseks või täidab pädeva asutuse need nõuded, millega seoses niisuguseid ajutisi peatamisi ja keelde kohaldati. Selliste ajutiste peatamiste või keeldude määramise suhtes peaks kohaldama kooskõlas liidu õiguse üldpõhimõtete ja hartaga asjakohaseid menetluslikke tagatisi, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust.
Kommenteeritava paragrahvi lõike 13 punktis 1 märgitud sertifikaadi all mõeldakse mõnda sertifikaati, mis on näiteks seotud küberturvalisuse tagamisega või sellekohaste nõuete järgimisega ehk siin ei saa nõuda ettekirjutusega sellise sertifikaadi ajutist peatamist, mis pole seotud KüTSis olevate nõuete täitmisega. Samas punktis mainitud loa all on mõeldud näiteks majandustegevuse registris oleva loa peatamise nõudmist ettekirjutusega. Nimetatud punkti kohaselt võib sama toimingu teha ka Riigi Infosüsteemi Amet, kui talle on mõne õigusaktiga selline pädevus antud.
Kommenteeritava lõike punkt 2 on sõnastatud krediidiasutuste seaduse § 50 lõike 1 eeskujul. Seega ei ole tegemist Eesti õiguses ka täiesti uudse või senitundmatu lahendusega. Eelnõu on pärast kooskõlastust muudetud nii, et ettekirjutus tehakse konkreetsele üliolulisele üksusele, kes peab juhatuse liikme volitused ajutiselt peatama. See tähendab, et ettekirjutuse subjekt on ikkagi konkreetne juriidiline isik, mitte mõni juriidilise isiku organ.
Otsus nõuda üliolulistelt üksuselt juhtorgani liikme volituste peatamist on oma olemuselt haldusakt haldusmenetluse seaduse § 51 lõike 1 tähenduses. Sellega kehtestatakse järelevalvesubjektile kohustus (ja piiratakse tema õigusi). Seetõttu on ettekirjutuse tegemine õige õiguslik vorm seda nõuda. Sellist mehhanismi, millega oleks haldusorganil võimalik teha ettekirjutus kohtu kaudu, Eesti õigus ei tunne. Küll aga on oluline rõhutada, et Riigi Infosüsteemi Ameti ettekirjutus allub loomulikult kohtulikule kontrollile. Üliolulisel üksusel on võimalik esitada selle peale halduskohtusse kaebus ja nõuda esialgse õiguskaitse korras ka ettekirjutuse täitmise peatamist. Seega on võimalik kohtumenetluse ajaks saada esialgne õiguskaitse, mis võimaldab senisel juhatuse liikmel tegevust jätkata. Üliolulisele üksusele on tagatud kõik halduskohtumenetluses ette nähtud tagatised, sellele eelnevas faasis kohalduvad Riigi Infosüsteemi Ametile kõik haldusmenetluse seaduses ette nähtud haldusmenetluse nõuded.
Võrdluseks võib välja tuua, et sarnast lahendust, kus pädev järelevalveasutus nõuab järelevalvesubjektilt endalt juhatuse liikme tagasikutsumist, on kasutatud ka teiste riikide NIS2-direktiivi ülevõtmiseks koostatud eelnõudes. Näiteks on see nii kavandatud Eesti õiguskorra kujundamisel oluliseks eeskujuks olnud Saksamaa Liitvabariigi vastavas seaduseelnõus (kõnealuse

[153] Eelnõus „üliolulise üksuse“.

eelnõu koostamise ajal ei ole Saksamaal veel eelnõu seadusena vastu võetud)[154].
Eelnõuga ei määrata kindlaks konkreetseid olukordi, millal võidakse taotleda üliolulise üksuse juhatuse liikme volituste ajutist peatamist ettekirjutusega, kuna seda ei täpsustata ka NIS2-direktiivis. Need konkreetsemad olukorrad ja põhjendused tuleb kindlaks määrata KüTSi alusel tehtavas Riigi Infosüsteemi Ameti ettekirjutuses.
Juhatuse liikme volituste peatamise regulatsioon ei saa kohalduda üksustele, millel ei ole enda juriidilise vormi tõttu juhatust, näiteks FIEdele. Samuti ei ole sellist regulatsiooni nähtud ette eelnõukohases KüTSi §-s 17, mis reguleerib haldusjärelevalvet, sest avalikule sektorile on NIS2-direktiivi artikli 32 lõike 5 kolmandas alalõigus nähtud ette välistus.

Eelnõukohase KüTSi § 16 lõike 1^6 järgi kohaldatakse lõikes 1^5 ette nähtud meetmeid, kuni ülioluline üksus võtab kasutusele vajalikud meetmed puuduste kõrvaldamiseks või Riigi Infosüsteemi Ameti esitatud nõuete täitmiseks.

KüTSi § 16 lõikest 2 jäetakse eelnõu kohaselt välja tekstiosa „ja käesoleva seaduse § 3 lõike 1 punktis 1 sätestatud teenuse osutaja puhul ka elutähtsa teenuse toimepidevust korraldavat asutust". Muudatus on välja pakutud põhjusel, et sama regulatsioon on eelnõus ette nähtud KüTSi § 17^4 lõikes 2. Eelnõukohane KüTSi § 17^4 reguleerib Riigi Infosüsteemi Ameti koostööd teiste ametiasutustega. Viidatud sätte lõikes 2 on ette nähtud, et amet vahetab infot elutähtsat teenust korraldava asutusega. Kuna eelnõuga luuakse KüTSi eraldi paragrahv – § 17^4 – ameti koostööülesannete kohta, siis sobib seni KüTSi § 16 lõikes 2 ette nähtud sama sisuga reegel olemuslikult just sinna. Seetõttu on vaja vastav tekstiosa KüTSi § 16 lõikest 2 dubleerimise vältimiseks välja jätta.

KüTSi § 17 reguleerib haldusjärelevalve meetmeid. NIS2-direktiivi artiklid 32 ja 33 kohalduvad nii eraõiguslikele kui ka avalik-õiguslikele üksustele. Eelnõukohases KüTSi §-s 17 on nähtud ette järelevalve erimeetmed, mida saab kohaldada haldusjärelevalve raames, st avalik-õiguslike üksuste suhtes. Nende eraldi reguleerimise eesmärk on säilitada võimalikult palju KüTSi senist loogikat.
Eelnõukohased KüTSi § 17 lõiked 1^1–1^3 on identsed eelnõukohaste KüTSi § 16 lõigetega 1^1–1^3, seega kehtivad kõik eespool KüTSi § 16 kohta antud selgitused ka KüTSi § 17 kohta.
Eraldi peab märkima seda, et NIS2-direktiivi artikli 32 lõikes 5 sätestatu ei kohaldu keskvalitsuse avaliku halduse üksuse või kohaliku tasandi avaliku halduse üksuse (eelnõu mõttes kohaliku omavalitsuse avaliku halduse üksuse) suhtes, sealhulgas juhul, kui sama üksus on kvalifitseeritud usaldusteenuse osutaja. Seetõttu ei reguleerita eelnõukohases KüTSi §-s 17 lubade ja sertifikaatide peatamist ega juhatuse liikme volituste peatamist (erinevalt eelnõukohasest KüTSi § 16 lõikest 1^5). Samuti on oluline rõhutada, et eelnõuga KüTSi § 16 lõikes 1^5 sätestatavate täitemeetmete õigusi ei anta julgeolekuasutusele (vt eelnõus KüTSi § 14 lõiget 5), kuna NIS2-direktiivi artikli 32 lõike 5 kolmanda tekstilõigu kohaselt „käesolevas lõikes sätestatud täitemeetmeid ei kohaldata nende avaliku halduse üksuste suhtes, kelle suhtes kohaldatakse [NIS2-direktiivi]". Kuna julgeolekuasutus saab teha ainult haldusjärelevalvet ehk järelevalvet avaliku halduse üksuse suhtes, siis ei ole võimalik eelnõukohases KüTSi § 16 lõikes 1^5 sätestatavaid õigusi anda ka julgeolekuasutusele. Samas antakse julgeolekuasutusele eelnõuga lisanduva KüTSi § 14 lõike 5 teise lause tõttu teatavad volitused, mis on sätestatud kommenteeritavas paragrahvis.

[154] Gesetzentwurf – der Bundesregierung. Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz): https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html.

Eelnõuga KüTSi §-s 17[1] kavandatavad muudatused on seotud nii sunniraha kui meetme laiendamisega haldusjärelevalvemenetlusele kui ka sunniraha kohaldamise ülemmäära muutmisega. Muudatused on seotud ka NIS2-direktiivi artikli 34 lõike 6 ülevõtmise ja kohase rakendamisega: „Liikmesriigid võivad näha ette õiguse määrata sunniraha, mille eesmärk on sundida elutähtsat[155] või olulist üksust käesoleva direktiivi rikkumist lõpetama, kooskõlas pädeva asutuse eelneva otsusega." NIS2-direktiiv sunniraha kohta midagi enamat ei selgita, sh ei ole kindlaks määratud ka sunniraha ülemmäär ega selle kindlaks määramise tingimused. Nii üliolulise üksuste (NIS2-direktiivi artikli 32 lõige 1) kui ka oluliste üksuste (NIS2-direktiivi artikli 33 lõige 1) puhul on ette nähtud nõue, et järelevalve- ja täitemeetmed peavad olema mõjusad, proportsionaalsed ja heidutavad ning et nende puhul võetakse arvesse iga üksikjuhtumi asjaolusid. Kuigi NIS2-direktiivis ei ole sõnaselgelt märgitud samade nõuete kohaldamist ka sunniraha kontekstis, on võimalik nimetatud nõudeid omistada ka olukorras, kus on vajadus sunniraha rakendada. Seda enam, et Eesti õiguses on sunniraha kui instituut osa haldusmenetlusest, st riiklikust ja haldusjärelevalvemenetlusest.

Sunniraha on haldussunnivahend ning selle sisu on asendustäitmise ja sunniraha seaduse § 10 lõike 1 kohaselt „hoiatuses kindlaksmääratud summa, mille peab adressaat tasuma, kui ta ettekirjutusega pandud kohustust hoiatuses märgitud tähtaja jooksul ei täida".

Eelnõuga laiendatakse sunniraha määramise võimalust KüTSi alusel haldusjärelevalve menetluses eelnõuga sätestatud suuruses. See siiski ei tähenda, et niisugust õigust praegu ei ole. Vabariigi Valitsuse seaduse § 75[1] lõige 4 reguleerib haldusjärelevalve teostamist teise haldusekandja üle, mille korral on sunniraha ülemmäär 9600 eurot. Eelnõuga on kavas ühtlustada nii KüTSi alusel määratava kui ka haldusjärelevalve käigus määratava sunniraha ülemmäär ning sätestada see ühes õigusaktis ehk KüTSis. Arvestades NIS2-direktiiviga lisanduvate haldustrahvide (mis võetakse üle väärteokoosseisudena) ülemmäärade suurusi, ei ole kohane jätta sunniraha sama suureks, nagu kehtivad seadused ette näevad (riiklikus järelevalves kuni 20 000 eurot ja haldusjärelevalves kuni 9600 eurot).

Ka isikuandmete kaitse seaduse §-s 60 on sätestatud sunniraha ülemmäär, mis on suurem kui Vabariigi Valitsuse seaduses. Tolle paragrahvi puhul on isikuandmete kaitse seaduse seletuskirja[156] lk-l 46 sedastatud järgmist: „Eelnõu paragrahviga 59 kehtestatakse sunniraha ülemmääraks kuni 20 000 000 eurot või ettevõtja puhul kuni 4 protsenti tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem. Sunniraha ülemmäär on siis sama suur kui väärteokaristuse ülemmäär ning võimaldab Andmekaitse Inspektsioonil efektiivselt sekkuda isikuandmete töötlemise nõuete rikkumisel."

Eelneva taustal tuleb siiski tähele panna, et Vabariigi Valitsuse seaduse §-s 75[1] sätestatu ei mõjuta asendustäitmise ja sunniraha seaduse § 5 viimases lauses sätestatut, mille kohaselt sunnivahendit ei rakendata riigiasutuse suhtes. Teisisõnu ei saa riigiasutust allutada (sh haldusjärelevalve raames) sunnirahale ega ka väärteomenetlusele või selle raames mõistetavale rahalisele karistusele. Riigiasutuste omavahelised vaidlused, sh järelevalveolukordadest tekkinud erimeelsused, tuleb muude haldusmenetluslike meetmete ammendumisel (olukorras, kus muu kui riigiasutuse puhul asutaks järgmisena rakendama sunniraha) lahendada Vabariigi Valitsuse seaduse §-s 101 ettenähtud korras (s.o üldjuhul alluvuskorras).

Kommenteeritava paragrahvi puhul on sunniraha ülemmäära kindlaks määramisel lähtutud asjaolust, et NIS2-direktiivi artiklis 34 olevate haldustrahvide suurus sama rikkumise eest erineb

[155] Eelnõus „üliolulist üksust".

[156] Isikuandmete kaitse seadus 679 SE: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5c9f8086-b465-4067-841e-41e7df3b95af/. Riigikogusse esitatud eelnõul kandis see paragrahv numbrit 59, kuid Riigikogus toimunud arutelude käigus lisati teise lugemise käigus juurde § 11, mille tõttu paragrahvide numeratsioon muutus.

ehk sõltub asjaolust, kas rikkumise toimepanija on ülioluline üksus või oluline üksus (vt allpool eelnõukohaste KüTSi §-de 18^2 ja 18^3 seletust). Need halduskaristused kavandatakse võtta üle väärteokoosseisudena ning soovitakse vältida olukorda, kus väärteokoosseisuga määratava trahvi ülemmäär on väiksem kui sunniraha ülemmäär ehk seda, et sunniraha ülemmäär määratakse kindlaks üliolulise üksusega seotud trahvi suuruse järgi, kuid sunniraha adressaat on oluline üksus, kelle rahatrahvi ülemmäär on väiksem kui üliolulisel üksusel. Seetõttu on eelnõus sätestatud, et ettekirjutuse täitmata jätmise korral on asendustäitmise ja sunniraha seaduses sätestatud korras rakendatava sunniraha kohaldamise igakordne ülemmäär kas (olenevalt sellest, kumb summa on suurem):
a) 7 000 000 eurot või
b) kuni 1,4 protsenti teenuseosutaja omanikust ettevõtja eelmise majandusaasta ülemaailmsest aastasest kogukäibest.
Sunniraha ülemmäära valik sõltub siis ka sellest, kas 1) tegemist on ettevõtja või avaliku sektoriga (nii kohaliku tasandi avaliku halduse üksuse kui ka teiste teisese halduse kandjate puhul ei kohaldu variandis b olev protsendiga arvutatav ülemmäär) ning 2) kumb summa on suurem (see aspekt avaldub ennekõike erasektoris oleva teenuseosutaja korral).
Sunniraha rakendamisel tuleb arvestada proportsionaalsuse põhimõttega. Sunniraha võib rakendada vaid ettekirjutuse täitmisele kallutamiseks. Sunnivahendit ei tohi rakendada karistusena. Haldusorgan peab valima sunnivahendi, mis isikut võimalikult vähe kahjustades sunnib teda ettekirjutust täitma. Proportsionaalsuse hindamisel võib arvesse võtta ka ettekirjutuse olulisust, rikkumise asjaolusid ja isiku majanduslikku seisundit.[157] Kohustuse täitmise tagamiseks kasutatakse leebeimat sunnivahendit ja -määra, mis eelduste kohaselt on tõhusaimad. Haldusorgan peab valima sunnivahendi, mis isikut võimalikult vähe kahjustades sunnib teda täitma talle ettekirjutusega pandud kohustust (asendustäitmise ja sunniraha seaduse § 3 lõige 3).
Seetõttu peab järelevalve tegija (Riigi Infosüsteemi Amet, julgeolekuasutus ning Tarbijakaitse ja Tehnilise Järelevalve Amet) sunniraha määramisel hindama, millises määras sunniraha rakendamine on Eesti kontekstis proportsionaalne.

Eelnõukohase KüTSi §-ga 17^3 on kavas võtta üle NIS2-direktiivi artikli 26 lõige 5 ja artikkel 37. Selles paragrahvis antakse asjaomased õigused ja kohustused ainult Riigi Infosüsteemi Ametile, kuna vastastikuse abiga seotud menetlused on olemuselt seotud ennekõike teenustega, mida osutavad erasektoris olevad KüTSi üksused. Seetõttu ei ole võimalik vastavaid õigusi ja kohustusi anda julgeolekuasutustele (vt KüTSi § 14 lõiget 5 ja selle täiendust). Kuna Tarbijakaitse ja Tehnilise Järelevalve Ametile (vt KüTSi § 14 lõiget 4) ei anta seoses NIS2-direktiiviga järelevalvevolitusi juurde, siis ei anta talle ka vastastikuse abiga seotud õigusi ja kohustusi. Kommenteeritava paragrahviga on seotud ka NIS2-direktiivi põhjendused 134 ja 135:
(134) Selleks et tagada, et üksused täidavad [NIS2-direktiivis] sätestatud kohustusi, peaksid liikmesriigid seoses järelevalve- ja täitemeetmetega tegema üksteisega koostööd ja üksteist abistama, eelkõige juhul, kui üksus osutab teenuseid rohkem kui ühes liikmesriigis või kui tema võrgu- ja infosüsteemid asuvad muus liikmesriigis kui see, kus ta teenuseid osutab. Abi osutamisel peaks taotluse saanud pädev asutus võtma järelevalve- või täitemeetmeid kooskõlas riigisisese õigusega. Selleks et tagada [NIS2-direktiivi] kohase vastastikuse abi sujuv toimimine, peaksid pädevad asutused kasutama juhtumite ja konkreetsete abitaotluste arutamise foorumina koostöörühma.
(135) Tulemusliku järelevalve ja täitmise tagamiseks, eelkõige piiriülese mõõtmega olukorras, peaks liikmesriik, kes on saanud vastastikuse abi taotluse, võtma kõnealuse taotluse piires

[157] Riigikohtu Halduskolleegiumi otsus asjas nr 3-3-1-72-14, p-d 14 ja 27.

asjakohaseid järelevalve- ja täitemeetmeid üksuse suhtes, kelle kohta taotlus tehti ja kes osutab kõnealuse liikmesriigi territooriumil teenuseid või kellel on seal võrgu- ja infosüsteem.

Eelnõukohase KüTSi § 17[3] lõikega 1 on kavas võtta üle NIS2-direktiivi artikli 37 lõike 1 esimese tekstilõigu esimene lause. Selle kohaselt teevad Riigi Infosüsteemi Amet ja välisriigis NIS2-direktiivi artikli 8 alusel nimetatud pädevad asutused koostööd asjakohase teabe vahetamiseks ning vajaduse korral abistavad üksteist, kui üksus osutab teenuseid:
a) mitmes Euroopa Liidu liikmesriigis või
b) ühes või mitmes Euroopa Liidu liikmesriigis, kuid tema võrgu- ja infosüsteemid asuvad ühes või mitmes muus liikmesriigis.

Eelnõukohase KüTSi § 17[3] lõikega 2 on kavas võtta üle NIS2-direktiivi artikli 37 lõike 1 esimese tekstilõigu punktid b ja c ning teise tekstilõigu esimene lause. Kommenteeritavas lõigus on kasutatud NIS2-direktiivi vastavas tekstis oleva sõna „teabenõue“ asemel sõna „teabepäring“, kuna teabenõue on sõnastatud avaliku teabe seaduse §-s 6 ning NIS2-direktiivis kasutatav sõna ei lähe tähenduse poolest kokku avaliku teabe seaduse teabenõudega.

Eelnõukohase KüTSi § 17[3] lõikega 3 on kavas võtta üle NIS2-direktiivi artikli 37 lõike 1 esimese tekstilõigu punkt b ehk luua Riigi Infosüsteemi Ametile volitus esitada teise Euroopa Liidu liikmesriigi NIS2-direktiivi artikli 8 alusel nimetatud pädevale asutusele vastastikuse abi taotlus, kui tegemist on kommenteeritava paragrahvi lõikes 1 sätestatud olukorraga.

Eelnõukohase KüTSi § 17[3] lõikega 4 on kavas võtta üle NIS2-direktiivi artikli 37 lõike 1 teise tekstilõigu teine lause ehk määrata kindlaks need olukorrad, millal Riigi Infosüsteemi Amet võib talle esitatud abitaotluse tagasi lükata. Tegemist on alternatiivsete olukordadega.

Eelnõukohase KüTSi § 17[3] lõikega 5 on kavas võtta üle NIS2-direktiivi artikli 37 lõike 1 teise tekstilõigu kolmas lause ehk sätestada, et Riigi Infosüsteemi Amet peab konsulteerima enne talle esitatud abitaotluse tagasilükkamist:
a) teiste asjaomaste pädevate asutustega ja
b) kui üks nendest asjaomastest pädevatest asutustest seda taotleb, siis ka Euroopa Komisjoni ning Euroopa Liidu Küberturvalisuse Ametiga.

Eelnõukohase KüTSi § 17[3] lõikega 6 on kavas võtta üle NIS2-direktiivi artikli 37 lõige 2. Kommenteeritava lõike kohaselt võib Riigi Infosüsteemi Amet võtta KüTSis nimetatud järelevalve- või täitemeetmeid, mille rakendamisse on kaasatud teise riigi pädeva asutuse töötajad või ametnikud. Meetmete kasutamisel lepitakse asutuste vahel kokku ka ühistegevuse kord ja protseduurid.

Eelnõukohase KüTSi § 17[3] lõikega 7 on kavas võtta üle NIS2-direktiivi artikli 26 lõige 5. Selle lõike kohaldamise eeldus on, et 1) Riigi Infosüsteemi Amet on saanud vastastikuse abi taotluse mõnelt muult NIS2-direktiivi artikli 8 kohaselt pädevalt asutuselt digitaalse teenuse osutaja kohta ning 2) see digitaalse teenuse osutaja osutab Eesti territooriumil teenuseid või tal on Eesti territooriumil võrgu- ja infosüsteem. Kui need tingimused on täidetud, on Riigi Infosüsteemi Ametil õigus võtta selle digitaalse teenuse osutaja suhtes talle esitatud vastastikuse abi taotluses märgitud ulatuses asjakohaseid järelevalve- ja täitemeetmeid.

Eelnõukohase KüTSi peatükiga 4[1] luuakse §-d 17[4]–17[6], mis on seotud koostöö, vastastikuse

hindamise ja teabevahetusega.

Eelnõukohase KüTSi §-ga 17[4] on kavas võtta üle NIS2-direktiivi artikli 2 lõige 13, artikli 8 lõige 4, artikli 10 lõiked 4 ja 7, artikli 13 lõiked 1, 4 ja 5, artikli 23 lõige 10, artikli 31 lõige 3, artikli 32 lõiked 9 ja 10, artikli 33 lõige 6, artikli 35 lõiked 1 ja 3 ning artikli 37 lõike 1 esimese tekstilõigu punkt a. Kommenteeritava paragrahvi kehtestamine toetab ka NIS2-direktiivi artikli 2 lõike 13 ülevõtmist.

Eelnõukohase KüTSi § 17[4] lõikega 1 on kavas anda kõnealused ülesanded nii Riigi Infosüsteemi Ametile kui ka julgeolekuasutusele, sh kohaldub mõlemale ka lõige 6. Ülejäänud kommenteeritava paragrahvi sätted on seotud ennekõike Riigi Infosüsteemi Ametiga. Lõige 1 ehk selle punktid 1–10 on seotud ennekõike NIS2-direktiivi artikli 13 lõike 4 ülevõtmisega. Kommenteeritava lõike esimene ja kolmas punkt on seotud lennunduse valdkonna järelevalveasutustega. Teine punkt on seotud usaldusteenuste valdkonnas järelevalvet tegevate asutustega (kelleks Eestis on praegu e-identimise ja e-tehingute usaldusteenuste seaduse § 2 ja § 22 kohaselt Riigi Infosüsteemi Amet, kuid kõnealuse punktiga peetakse silmas ka teiste riikide samasuguseid asutusi). Kommenteeritava lõike neljas punkt on seotud nii NIS2-direktiivi artikli 32 lõike 10 esimese lausega ja artikli 33 lõike 6 esimese lausega kui ka artikli 35 lõigetega 1 ja 3. Viies punkt on seotud ka NIS2-direktiivi artikli 32 lõikega 3 (koostöö isikuandmete kaitse valdkonna järelevalveasutustega). Kuues punkt on seotud NIS2-direktiivi artikli 13 lõigetega 1 ja 3. Kommenteeritava lõike seitsmes punkt on seotud nii NIS2-direktiivi artikli 37 lõike 1 esimese tekstilõigu punktiga a kui ka nende pädevate järelevalveasutustega, kes on nimetatud delegeeritud määruse (EL) 2024/1366 artikli 3 lõikes 2 või kes on sama määruse artikli 4 kohaselt kindlaks määratud. Üheksas punkt on seotud NIS2-direktiivi artikli 10 lõike 4 ülevõtmisega. Kümnenda punkti puhul on kasutatud viidet isikuandmete kaitse seaduse § 13 lõikes 2 olevale õiguskaitseasutuse mõistele, kuna mujal ei ole seda selgitatud või defineeritud.

Eelnõukohane KüTSi § 17[4] lõige 2 on seotud NIS2-direktiivi artikli 13 lõike 5, artikli 23 lõike 10 ja artikli 32 lõike 9 rakendamisega. Kõnealuses eelnõus on sõnastuse puhul eeskuju võetud eelnõuga nr 426 SE hädaolukorra seadusesse lisandunud koostöösätetega, tagamaks kooskõla mõlema õigusakti vahel. Kommenteeritavas lõikes on viidatud hädaolukorra seaduse § 37 lõikele 5, kuid see viide tuleb asendada viitega tsiviilkriisi ja riigikaitseseaduse vastavale sättele, kui tolle seaduse eelnõu on vastu võetud ning lõplik sõnastus on teada. Kommenteeritava lõike viimases lauses on märgitud nii riiklikku kui ka haldusjärelevalve menetlusi – kuigi üldreeglina on elutähtsa teenuse osutaja eraettevõte, siis eelnõuga nr 426 SE lisatakse elutähtsa teenuse osutaja ülesanne ka Eesti Rahvusringhäälingule, mis ei ole ettevõte, vaid avalik-õiguslik juriidiline isik.

Eelnõukohane KüTSi § 17[4] lõige 3 on seotud NIS2-direktiivi artikli 32 lõike 10 teise lause ja artikli 33 lõike 6 teise lause ülevõtmisega. Selles lõikes viidatakse ainult riiklikule järelevalvele, kuna DORA määruse artikli 31 kohaselt saab kriitilise tähtsusega kolmandast isikust IKT-teenuse osutajana käsitleda ennekõike erasektoris olevat KüTSi teenuse osutajat.

Eelnõukohane KüTSi § 17[4] lõige 4 on seotud NIS2-direktiivi artikli 13 lõigete 3 ja 5 ülevõtmisega. Eelnõukohane **KüTSi § 17[4] lõige 5** on seotud NIS2-direktiivi artikli 8 lõike 4 ja artikli 37 lõike 1 esimese tekstilõigu punkti a ülevõtmisega. Eelnõukohane **KüTSi § 17[4] lõige 6** on seotud NIS2-direktiivi artikli 10 lõike 7 ülevõtmisega.

Eelnõukohase KüTSi §-ga 17[5] on kavas võtta üle NIS2-direktiivi artikli 10 lõige 4 ja artikkel 29.

Tegemist on vabatahtliku küberturvalisusalase teabevahetuse kokkuleppega, kus võivad osaleda nii Riigi Infosüsteemi Amet, teenuseosutajad kui ka muud isikud. Näiteks võivad küberturvalisusalase teabevahetuse kokkuleppega ühineda ka need teenuseosutajad, kellele KüTSi § 1 lõike 4 tõttu kohaldatakse mõnda muud õigusakti (nt DORA määrust).
Kommenteeritava paragrahviga on seotud ka NIS2-direktiivi põhjendused 118–121:
(118) Kui [NIS2-direktiivi] alusel vahetatakse või edastatakse või jagatakse muul moel teavet, mida käsitatakse kooskõlas liikmesriigi või liidu õigusega salastatud teabena, tuleks järgida asjaomaseid salastatud teabe käitlemise erireegleid. Ühtlasi peaksid ENISA-l olema taristu, kord ja reeglid, mille abil käsitleda tundlikku ja salastatud teavet kooskõlas ELi salastatud teabe kaitseks kohaldatavate turvareeglitega.
(119) Kuna küberohud on muutumas komplekssemaks ja keerukamaks, sõltuvad selliste ohtude head tuvastus- ja ennetusmeetmed suuresti ohte ja nõrkusi puudutava teabe korrapärasest jagamisest üksuste vahel. Teabevahetus aitab suurendada teadlikkust küberohtudest ja see omakorda suurendab üksuste võimekust hoida ära ohtude muutumist intsidentideks ning võimaldab üksustel intsidentide mõju paremini piirata ja neil tõhusamalt taastuda. Liidu tasandi suuniste puudumise tõttu on sellist teadmuse jagamist pärssinud eri tegurid, eelkõige ebakindlus seoses konkurentsi ja vastutust käsitlevate normide järgimisega.
(120) Liikmesriigid peaksid üksusi julgustama ja abistama, et nad kasutaksid kollektiivselt individuaalseid teadmisi ja praktilisi kogemusi strateegilisel, taktikalisel ja operatiivtasandil, et suurendada oma võimekust küberohte õigesti ennetada, avastada, neile reageerida, nendest taastuda ja nende mõju leevendada. Seega on vaja võimaldada sõlmida liidu tasandil vabatahtlikud küberturvalisuse alase teabevahetuse kokkulepped. Selleks peaksid liikmesriigid aktiivselt abistama ja julgustama üksusi, näiteks küberturvalisuse teenuseid ja teadusuuringuid pakkuvaid üksusi, ning [NIS2-direktiivi] kohaldamisalast välja jäävaid asjaomaseid üksusi sellistes küberturvalisuse alase teabevahetuse kokkulepetes osalema. Sellised kokkulepped tuleks sõlmida kooskõlas liidu konkurentsinormide ja liidu andmekaitseõigusega.
(121) Isikuandmete töötlemist sellises ulatuses, mis on vajalik ja proportsionaalne võrgu- ja infosüsteemide turvalisuse tagamiseks elutähtsates[158] ja olulistes üksustes, võib pidada seaduslikuks selle alusel, et selline töötlemine on vajalik vastutava töötleja seadusjärgse kohustuse täitmiseks kooskõlas määruse (EL) 2016/679 artikli 6 lõike 1 punkti c ja artikli 6 lõike 3 nõuetega. Isikuandmete töötlemine võib olla vajalik ka elutähtsate[159] ja oluliste üksuste ning nende üksuste nimel tegutsevate turvatehnoloogiate ja -teenuste pakkujate õigustatud huvides vastavalt määruse (EL) 2016/679 artikli 6 lõike 1 punktile f, sealhulgas juhul, kui selline töötlemine on vajalik küberturvalisuse alase teabevahetuse kokkulepete puhul või asjakohase teabe vabatahtlikuks esitamiseks kooskõlas [NIS2-direktiiviga]. Selliste meetmete võtmiseks, mis on seotud intsidentide ennetamise, avastamise, tuvastamise, ohjamise, analüüsimise ja lahendamisega, samuti niisuguste meetmete võtmiseks, millega suurendatakse teadlikkust konkreetsetest küberohtudest, võimaldatakse teabevahetust nõrkuste[160] vähendamise ja nõrkuste[161] koordineeritud avalikustamise kontekstis, samuti vabatahtlikku teabevahetust seoses kõnealuste intsidentide, küberohtude ja nõrkuste[162], rikkeindikaatorite[163], taktika, meetodite ja menetluskorra, küberturvalisuse hoiatussüsteemide ja konfiguratsioonivahenditega, võib olla vaja töödelda

[158] Eelnõus „üliolulistes üksustes“.
[159] Eelnõus „ülioluliste üksuste“.
[160] Eelnõus „turvahaavatavuste“.
[161] Eelnõus „turvahaavatavuste“.
[162] Eelnõus „turvahaavatavuste“.
[163] Eelnõus „turvarikkemärkide“.

teatavat liiki isikuandmeid, nagu IP-aadresse, internetiaadresse (URLe), domeeninimesid, meiliaadresse, ja kui neis avalduvad isikuandmed, ajatempleid. Isikuandmete töötlemine pädevate asutuste, ühtsete kontaktpunktide ja CSIRTide poolt võib olla juriidiline kohustus või seda võib pidada vajalikuks avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks vastavalt määruse (EL) 2016/679 artikli 6 lõike 1 punktile c või e ja artikli 6 lõikele 3 või elutähtsate[164] ja oluliste üksuste õigustatud huvi korral, nagu on osutatud kõnealuse määruse artikli 6 lõike 1 punktis f. Lisaks võiks riigisiseses õiguses sätestada reeglid, mis võimaldavad pädevatel asutustel, ühtsetel kontaktpunktidel ja CSIRTidel sellises ulatuses, mis on vajalik ja proportsionaalne elutähtsate[165] ja oluliste üksuste võrgu- ja infosüsteemide turvalisuse tagamiseks, töödelda isikuandmete eriliike kooskõlas määruse (EL) 2016/679 artikliga 9, eelkõige nähes ette sobivad ja konkreetsed meetmed füüsiliste isikute põhiõiguste ja huvide kaitsmiseks, sealhulgas tehnilised piirangud selliste andmete taaskasutamisele ning turva- ja eraelu puutumatuse säilitamise tipptasemel meetmete kasutamine, nagu pseudonüümimine või krüpteerimine, kui anonüümimine võib taotletavat eesmärki oluliselt mõjutada.

Eelnõukohase KüTSi § 17[5] lõikega 1 on kavas võtta üle NIS2-direktiivi artikli 29 lõiked 1 ja 2, määrates kindlaks alternatiivsed olukorrad, mille puhul küberturvalisusalase teabevahetuse kokkuleppe osapooled sedasorti teabevahetust teevad. Tuleb arvestada asjaoluga, et tegemist on kogukondlikus laadis infovahetamisega ja siin ei saa näiteks üks kogukonna liige nõuda teiselt liikmelt, et see annaks või edastaks kommenteeritavas lõikes ette nähtud teavet. Samas tuleb siin ka eristada juhtumit või olukorda, kus see teine liige peab mõne muu kehtiva või tulevikus kehtima hakkava õigusnormi tõttu vastavat teavet esitama.

Eelnõukohase KüTSi § 17[5] lõikega 2 on kavas võtta üle NIS2-direktiivi artikli 29 lõige 2. Selles lõikes nähakse ette, et kommenteeritava paragrahviga seotud teabevahetuse kokkuleppeid võib olla rohkem kui üks, kuna NIS2-direktiiv ei näe ette ainult ühe teabevahetuse kokkuleppe sõlmimise võimalust ning eelnõus soovitakse seda eraldi rõhutada. Küll aga ilmneb NIS2-direktiivi sätetest, et teabevahetus peaks toimuma teatud taseme formaalsusega, mitte suvaliselt, seega teabevahetuse kokkuleppe raames, millega ühinemisest või millest taganemisest tuleb teenuseosutajatel ka järelevalveasutust teavitada (vt kommenteeritava paragrahvi lõiget 5).

Eelnõukohase KüTSi § 17[5] lõikega 3 on kavas võtta üle NIS2-direktiivi artikli 29 lõige 2 ja lõike 3 teine lause, määrates ära, milliseid aspekte on võimalik teabevahetuse kokkuleppes täpsustada. See lõige annab esmase selguse, milliste nüansside ja teemade peale mõelda, kui hakatakse teabevahetuse kokkulepet sõlmima. Näiteks võiks teabevahetuse kokkuleppes määrata kindlaks, kuidas toimub ühinemine selle kokkuleppega ja kuidas toimub sellest taganemine ning kes ja kuidas sellised otsused vastu võtab.

Eelnõukohase KüTSi § 17[5] lõikega 4 on kavas võtta üle NIS2-direktiivi artikli 10 lõige 4 ja artikli 29 lõike 3 kolmas lause. Kommenteeritavas lõikes mainitud tingimus võib olla näiteks (valgus)foorprotokolli kasutamine.[166]

Eelnõukohase KüTSi § 17[5] lõikega 5 on kavas võtta üle NIS2-direktiivi artikli 29 lõige 4, millega nähakse ette Riigi Infosüsteemi Ameti teavitamine, kui:

[164] Eelnõus „ülioluliste üksuste".
[165] Eelnõus „ülioluliste üksuste".
[166] (Valgus)foorprotokolli selgitust vt: https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/fooriprotokoll.

a) teenuseosutaja on ühinenud teabevahetuse kokkuleppega või
b) teenuseosutaja taganemine teabevahetuse kokkuleppest on jõustunud.
Variandi b puhul on mõeldud olukorda, kus on esitatud teabevahetuse kokkuleppest taganemise avaldus ja teabevahetuse kokkuleppe haldaja on selle rahuldanud ehk teenuseosutaja pole enam selle kokkuleppe osapool ning on seejuures eemaldatud ka näiteks selle teabevahetusega seotud e-kirja nimekirjast või muust infosüsteemist või platvormilt.

Eelnõukohase KüTSi §-ga 17[6] on kavas võtta üle NIS2-direktiivi artikkel 19, millega sätestatakse vastastikuse hindamise võimalus. Kommenteeritava paragrahviga on seotud ka NIS2-direktiivi põhjendused 75 ja 76:
(75) Kasutusele tuleks võtta vastastikune hindamine, et aidata õppida ühistest kogemustest, tugevdada vastastikust usaldust ja saavutada küberturvalisuse ühtlaselt kõrge tase. Vastastikune hindamine võib anda väärtuslikke teadmisi ja viia soovitusteni, mis tugevdavad üldist küberturvalisuse võimekust, luues uue funktsionaalse tee parimate tavade jagamiseks liikmesriikide vahel ning aidates tõsta liikmesriikide küberturvalisuse taset. Lisaks peaks vastastikuses hindamises võtma arvesse sarnaste mehhanismide, näiteks CSIRTide võrgustiku vastastikuse hindamise süsteemi tulemusi, looma lisaväärtust ja vältima dubleerimist. Vastastikuse hindamise rakendamine ei tohiks piirata konfidentsiaalse ja salastatud teabe kaitset käsitlevate riiklike või liidu õigusaktide kohaldamist.
(76) Koostöörühm peaks kehtestama liikmesriikide jaoks enesehindamise metoodika, mille eesmärk on hõlmata selliseid tegureid nagu küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rakendamise tase, pädevate asutuste võimekuse tase ja ülesannete täitmise tulemuslikkus, CSIRTide tegevusvõimekus, vastastikuse abi rakendamise tase, küberturvalisuse alase teabevahetuse korra rakendamise tase või konkreetsed piiriülese või valdkondadevahelise iseloomuga küsimused. Liikmesriike tuleks julgustada tegema korrapäraselt enesehindamisi ning esitama ja arutama oma enesehindamise tulemusi koostöörühmas.

Eelnõukohase KüTSi § 17[6] lõikega 1 on kavas võtta üle NIS2-direktiivi artikli 19 lõike 1 esimese tekstilõigu teine lause, mille järgi on vastastikuses hindamises osalemine vabatahtlik.

Eelnõukohane KüTSi § 17[6] lõige 2 on seotud NIS2-direktiivi artikli 19 lõike 6 viienda lause (*vastastikuses hindamises osalevad küberturvalisuse valdkonna eksperdid ei avalda vastastikuse hindamise käigus saadud tundlikku või konfidentsiaalset teavet kolmandatele isikutele*) ülevõtmisega. Kommenteeritava punkti puhul tuleb arvestada ka asjaoluga, et ametnike suhtes on vastav NIS2-direktiivi nõue sätestatud avaliku teenistuse seaduse §-s 55 ning töötajate puhul on nimetatud nõude täitmisega seotud töölepingu seaduse § 6 lõige 3 ja § 22. Samamoodi on siin ka asjakohane avaliku teabes seaduse § 38 lõike 3 lause 2 ning juurdepääsupiirangu alustena kommenteeritava paragrahvi alusel koostatud või saadud teabele võib siin kasutada sama seaduse § 35 lõike 1 punkte 3, 9 ja 10. Samas, kui kommenteeritava paragrahviga seotud vastastikusesse hindamisse kaasatakse eksperdina keegi muu isik, kellele eelnimetatud nõuded ei kohaldu (nt käsunduslepingu alusel), siis on võimalik sõlmida konfidentsiaalsuskinnitus. Seetõttu ongi loodud kommenteeritav punkt, et see hõlmaks ka neid muid osapooli.
Saladuses hoidmise kohustuse kohta tuleb ka märkida, et üldreeglina on asutusesiseseks kasutamiseks mõeldud teabe puhul juurdepääsupiirangu pikkus kuni viis aastat, mida võib pikendada kuni viie aasta võrra (vt avaliku teabe seaduse § 40 lõiget 1). Selline juurdepääsupiirangu tähtaeg on aga kohaldatav ennekõike olukorras, kus tegemist on Eestis loodud avaliku teabega. Kui mingi teave on saadud välisriigilt või rahvusvaheliselt organisatsioonilt, tuleb lähtuda teabe saatja (algse looja) juurdepääsupiirangu tähtajast (vt avaliku teabe seaduse § 40

lõiget 1^1). Eraldi teema on, kui mingi teave klassifitseerub riigisaladuseks või salastatud välisteabeks – sel juhul lähtutakse teabe kaitse ja tähtaegade puhul ennekõike riigisaladuse ja salastatud välisteabe seadusest ja sellega seotud või selles viidatud muudest õigusaktidest.

Eelnõukohasesse KüTSi § 17^6 lõikesse 3 kavandatakse volitusnorm, mille alusel antava määrusega (vastastikuses hindamises osalemise täpsemad tingimused ja kord, sealhulgas vastastikuse hindamise korralduse nõuded, selles osalevate asutuste ülesanded ja vastastikuses hindamises osalevad isikud) võetakse üle ülejäänud osa NIS2-direktiivi artiklist 19, kui Eesti on valmis ja soovib vastastikuse hindamise mehhanismiga liituda. Asjaomane rakendusakti kavand on eelnõu materjalidele lisatud.

KüTSi § 18 tunnistatakse eelnõu kohaselt kehtetuks, kuna NIS2-direktiivi ülevõtmisel on tekkinud vajadus eristada üliolulisi ja olulisi üksusi ning neile määratavaid rahatrahve. Seetõttu on eelnõus ka KüTSi §-d 18^2–18^3, samuti on sellega seotud §-d 18^4 ja 18^5.

Eelnõukohased KüTSi §-d 18^2–18^5 on seotud väärteokoosseisude sätestamisega.
Lisanduvate KüTSi §-de 18^2 ja 18^3 puhul tuleb arvestada asjaoluga, et Eesti õiguskorras puuduvad haldustrahvid (*administrative fines*), mistõttu kavandatakse sarnaselt isikuandmete kaitse üldmääruse põhjendusega 151 viia NIS2-direktiiviga ette nähtud haldustrahvi määramise menetlus läbi väärteomenetlusena. Eelnõus pakutav lahendus on ka kooskõlas kehtiva õigusega ehk ennekõike KüTSi § 19 lõikega 2, mis on seotud NIS2-direktiivi artikli 35 rakendamisega.
Lisanduvad sätted on seotud ka NIS2-direktiivi põhjendustega 127–132:
(127) Et täitmine tõhusalt tagada, tuleks koostada [NIS2-direktiivis] sätestatud küberturvalisuse riskijuhtimismeetmete ja teatamiskohustuse rikkumise korral miinimumloetelu täitmise tagamise volitustest, mida võib kasutada, ning kehtestada selliste täitmise tagamise jaoks kogu liidus selge ja ühtne raamistik. Igakülgset tähelepanu tuleks pöörata [NIS2-direktiivi] rikkumise laadile, tõsidusele ja kestusele, põhjustatud varalisele või mittevaralisele kahjule, sellele, kas rikkumine oli tahtlik või tingitud hooletusest, varalise või mittevaralise kahju vältimiseks või leevendamiseks võetud meetmetele, vastutuse tasemele ja varasematele asjaomastele rikkumistele, pädeva asutusega tehtava koostöö tasemele ning muule raskendavale või leevendavale tegurile. Sellised täitemeetmed, sealhulgas haldustrahvid, peaksid olema proportsionaalsed ja nende määramise suhtes tuleks kooskõlas liidu õiguse üldpõhimõtete ja Euroopa Liidu põhiõiguste hartaga (edaspidi „harta“) kohaldada asjakohaseid menetluslikke kaitsemeetmeid, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust.
(128) [NIS2-direktiivis] ei nõuta, et liikmesriigid näeksid ette kriminaal- või tsiviilvastutuse füüsiliste isikute suhtes, kes vastutavad selle eest, et üksused järgiksid [NIS2-direktiivi], kui selle rikkumise tagajärjel on tekitatud kahju kolmandatele isikutele.
(129) Et tagada [NIS2-direktiivis] sätestatud kohustuste tõhus täitmine, peaks igal pädeval asutusel olema õigus haldustrahve määrata või nende määramist taotleda.
(130) Kui haldustrahv määratakse elutähtsale[167] või olulisele üksusele, kes on ettevõtja, tuleks selline ettevõtja lugeda ettevõtjaks ELi toimimise lepingu artiklite 101 ja 102 tähenduses. Kui haldustrahv määratakse isikule, kes ei ole ettevõtja, peaks pädev asutus sobiva trahvisumma määramisel arvesse võtma üldist sissetulekutaset selles liikmesriigis ja isiku majanduslikku olukorda. See, kas ja mil määral tuleks kohaldada haldustrahve avaliku sektori asutustele, peaks olema liikmesriikide otsustada. Haldustrahvi määramine ei mõjuta pädevate asutuste muude volituste rakendamist ega muude karistuste kohaldamist, mis on sätestatud [NIS2-direktiivi]

[167] Eelnõus „üliolulisele üksusele“.

ülevõtvates liikmesriigi õigusnormides.
(131) Liikmesriikidel peaks olema võimalik kehtestada kriminaalkaristusi käsitlevad normid, mida kohaldatakse [NIS2-direktiivi] ülevõtvate liikmesriigi õigusnormide rikkumise korral. Kriminaalkaristuste määramine selliste liikmesriigi normide rikkumise korral ja seotud halduskaristuste määramine ei tohiks aga kaasa tuua ne bis in idem *põhimõtte rikkumist, nagu seda on tõlgendanud Euroopa Liidu Kohus.*
(132) Kui [NIS2-direktiiviga] ei ole halduskaristusi ühtlustatud või vajaduse korral muudel juhtudel, näiteks [NIS2-direktiivi] olulise rikkumise korral, peaksid liikmesriigid rakendama süsteemi, mis näeb ette tõhusad, proportsionaalsed ja heidutavad karistused. Selliste karistuste laad ja see, kas tegemist on kriminaal- või halduskaristusega, tuleks kindlaks määrata liikmesriigi õigusega.
NIS2-direktiivi artikli 34 lõike 1 kohaselt peavad liikmesriigid tagama, et haldustrahvid, mis määratakse sama artikli kohaselt üliolulistele ja olulistele üksustele NIS2-direktiivi rikkumise korral, on mõjusad, proportsionaalsed ja heidutavad ning et nende puhul võetakse arvesse iga üksikjuhtumi asjaolusid. NIS2-direktiivi artikli 34 lõike 3 kohaselt peab haldustrahvi määramise ja selle suuruse üle otsustamisel võtma iga üksikjuhtumi puhul nõuetekohaselt arvesse vähemalt NIS2-direktiivi artikli 32 lõikes 7 sätestatud asjaolusid (vt ka NIS2-direktiivi vastavustabelis olevaid selgitusi väärteomenetluse kontekstis, samuti taustaks eelnõus KüTSi § 14 lõiget 7), näiteks rikkumise raskust ja rikutud sätete olulisust, rikkumise kestust, varasemaid rikkumisi ning rikkumise toimepanija tahtlust või hooletust.
Eelnõuga nähakse ette, et NIS2-direktiiviga seotud haldustrahve kohaldatakse väärteomenetluses, NIS2-direktiivi artikli 32 lõikes 7 olevad asjaolud on aga sellised, mis võimaldavad väärteomenetluse seadustiku § 3^1 alusel hinnata, kas väärteomenetluse alustamine on toimepandud väärteo asjaolusid arvesse võttes põhjendatud, vajalik ja mõistlik. Seetõttu on üsna tõenäoline, et maksimummääras trahvimine oleks Eestis erandlik ja vähetõenäoline, arvestades nii seda, et järelevalveasutus (Riigi Infosüsteemi Amet) peab igal juhul hindama, kas väärteomenetluse läbiviimine ning trahvi määramine on konkreetse rikkumise olemust ja iseloomu arvestades vajalik ja proportsionaalne, kui ka Eestis tegutsevate ettevõtete majandustegevuse mahtu ja ulatust. Siiski ei saa seda täielikult välistada, näiteks juhul, kui järelevalvaja tuvastab, et rikkumine on väga suur ning näiteks piiriülese tegevusega ettevõtja puhul on ülemaailmne aastakäive väga suur. Ühtlasi tuleb arvestada, et üliolulisi ja olulisi üksusi puudutavate trahvimäärade ülempiiride miinimum on ette nähtud NIS2-direktiiviga (artikli 34 lõiked 4 ja 5) ning liikmesriikidel ei ole võimalik neid väiksemana kehtestada. Igal juhul peab väärteotrahvi määraja hindama paljusid asjaolusid ning NIS2-direktiiv ei kirjuta ette, millises määras peab järelevalveasutus teatud laadi rikkumiste korral trahvima, vaid tegemist on järelevalveasutuse kaalutlusõigusega. Seega peab järelevalveasutus tegema kaks erinevat kaalutlusotsust.
Esiteks tuleb otsustada, kas konkreetse rikkumise korral on väärteomenetluse alustamine vajalik ning proportsionaalne või on tõhusam rakendada teisi järelevalvemeetmeid. Teiseks tuleb juhul, kui väärteokoosseisu nõuded on täidetud ja järelevalveasutus otsustab alustada väärteomenetlust, määrata asjakohaseid tegureid arvesse võttes trahvi suurus. Ennekõike peab trahv vastama rikkumise laadile, raskusele ja tagajärgedele ning järelevalveasutus peab hindama kõiki juhtumi asjaolusid järjepideval ja objektiivselt põhjendatud viisil. Tõhususe, proportsionaalsuse ja heidutusvõime hindamine peab iga juhtumi puhul kajastama ka taotletavat eesmärki, milleks on kas küberturvalisuse tagamisega seotud nõuete täitmine või ebaseadusliku käitumise karistamine (või mõlemad).
Kuivõrd Eestis kohaldatakse NIS2-direktiivis ette nähtud haldustrahve väärteomenetluse raames, tuleb lähtuda väärteomenetluse üldreeglitest. Väärteomenetluse seadustiku § 3 lõige 1 selgitab, et väärteomenetlusõigus kehtib füüsilise ja juriidilise isiku suhtes. Ainult kirjalikku

hoiatamismenetlust (väärteomenetluse seadustiku § 54[1]) kohaldatakse ka riigi, kohaliku omavalitsuse ja avalik-õigusliku juriidilise isiku suhtes. Samas ei vasta eelnõuga ette nähtavad süüteokoosseisud kirjalikule hoiatamismenetlusele. Seega ei ole KüTSis ette nähtavaid väärteotrahve võimalik kohaldada riigi ja kohaliku omavalitsuse suhtes.
Rahatrahvide kohaldamise ühtse praktika tagamiseks on kohtuvälise menetleja juhil võimalik kasutada väärteomenetluse seadustiku § 10 lõikes 2[1] sätestatud võimalust anda suurendatud ülemmääraga rahatrahvi kohaldamiseks üldiseid juhiseid.
NIS2-direktiivi artikli 34 lõiked 4 ja 5 näevad ette, et trahv määratakse protsendina (vastavalt 2% või 1,4%) vastava üksuse eelmise majandusaasta üleilmsest aastasest kogukäibest. NIS2-direktiivis ei ole antud käibe arvutamiseks lisajuhiseid. Euroopa Komisjon on eelnõu koostajatele selgitanud, et NIS2-direktiivi põhjendus 130 (vt eespool) ja isikuandmete kaitse üldmääruse põhjendus 150[168] on oma sisult identsed, mistõttu tuleb trahvi arvutamisel lähtuda samadest põhimõtetest, nagu näeb ette isikuandmete kaitse üldmäärus. See omakorda tähendab, et ülemaailmse aastase kogukäibe väljaselgitamisel tuleb lähtuda samadest alustest. Seetõttu on siin asjakohane tsiteerida karistusseadustiku § 47 lõiget 4: „Käesoleva seadustiku eriosa või muu seadus võib ette näha rahatrahvi kohaldamise käesoleva paragrahvi lõigetes 1 ja 2 sätestatust erineval alusel ja määras, võttes arvesse reguleeritava valdkonna eripära.“ Karistusseadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu (Euroopa Liidu õigusest tulenevad rahatrahvid) 94 SE[169] arutelul Riigikogus sooviti algselt määrata ning paika panna ühised reeglid, kuidas ja millistest asjaoludest lähtudes käibe suurust arvutatakse. Eelnõu nr 94 SE teise lugemise eel jõuti järeldusele, et Euroopa Liidu õigus on pidevas muutumises, mistõttu ei ole võimalik algselt planeeritud raame käibe arvutamiseks tekitada. Seetõttu loodi karistusseadustiku § 47 lõikesse 4 „üldine alus, mis võimaldaks reguleeritava valdkonna eripära arvestades kalduda kõrvale sama paragrahvi lõigetes 1 ja 2 sätestatud rahatrahvi määradest ja arvutamise alustest. Seadusandja peaks seda võimalust valdkonnaseaduste muutmisel kasutama aga üksnes põhjendatud juhul, võttes arvesse reguleeritava valdkonna eripära (sh Euroopa Liidu õiguse nõudeid). Karistusseadustiku § 47 (rahatrahv) lõikes 1 on sätestatud, et kohus või kohtuväline menetleja võib väärteo eest kohaldada rahatrahvi kolm kuni kolmsada trahviühikut. Trahviühik on rahatrahvi baassumma, mille suurus on 4 eurot. Sama sätte lõige 2 võimaldab juriidilisele isikule võib kohus või kohtuväline menetleja väärteo eest kohaldada rahatrahvi 100–400 000 eurot.“[170]
Karistusseadustiku § 47 lõike 1 puhul tuleb arvestada asjaoluga, et alates 01.01.2025. a on trahviühiku suuruseks 8 eurot, mitte 4 eurot.
Kui tulevikus leitakse riigis haldustrahvi instituudile parem või ühetaolisem analoog, siis on võimalik ka analüüsida, kas ja mis ulatuses saaks KüTSi eelnõuga planeeritud väärteokoosseisud

[168] Isikuandmete kaitse üldmääruse põhjendus 150: *Selleks et tugevdada ja ühtlustada väärteokaristusi käesoleva määruse rikkumise korral, peaksid igal järelevalveasutusel olema volitused määrata trahve. Käesolevas määruses tuleks loetleda rikkumised, sätestada asjaomaste trahvide ülemmäär ja nende määramise kriteeriumid, mille üle peaks iga juhtumi puhul eraldi otsustama pädev järelevalveasutus, võttes arvesse konkreetse olukorra kõiki asjakohaseid asjaolusid, pidades eelkõige silmas rikkumise laadi, raskusastet, ajalist kestvust ja tagajärgi ning meetmeid, mis võetakse käesoleva määruse kohaste kohustuste täitmise tagamiseks ja rikkumise tagajärgede vältimiseks või leevendamiseks. Kui trahv on määratud ettevõtjale, tuleks ettevõtja määratlemisel lähtuda ELi toimimise lepingu artiklites 101 ja 102 toodud määratlusest. Kui trahvid määratakse isikule, kes ei ole ettevõtja, peaks järelevalveasutus sobiva trahvisumma määramisel arvesse võtma üldist sissetulekutaset selles liikmesriigis ja isiku majanduslikku olukorda. Trahvide ühesuguse kohaldamise parandamiseks võib kasutada ka järjepidevuse mehhanismi. See, kas ja kui palju tuleks avaliku sektori asutustele määrata trahve, peaks olema liikmesriikide otsustada. Trahvi määramine või hoiatuse tegemine ei mõjuta järelevalveasutuse muude volituste rakendamist ega muude määruse kohaste karistuste määramist.*
[169] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1bfa1944-2de6-449d-a788-887bc84cfd0f/.
[170] *Op cit*, teise lugemise muudatusettepanekute loetelu, p 3.1 selgitus lk-del 2–3.

viia haldustrahvi või muu sellele vastava analoogse meetme kujule.

Eelnõukohase KüTSi §-ga 18[2] on kavas võtta üle NIS2-direktiivi artikli 34 lõige 4, mille sisu on järgmine: „Liikmesriigid tagavad, et kui elutähtsad üksused[171] rikuvad [NIS2-direktiivi] artiklit 21 või 23, määratakse kooskõlas käesoleva artikli lõigetega 2 ja 3 elutähtsatele üksustele[172] haldustrahv, mille maksimummäär on vähemalt 10 000 000 eurot või kuni 2% selle ettevõtja ülemaailmsest aastasest kogukäibest eelneval majandusaastal (olenevalt sellest, kumb summa on suurem), kellele elutähtis üksus[173] kuulub."
Eeltoodu tõttu on ette nähtud, et väärteokaristus määratakse olukorras, kus on rikutud KüTSi § 7 lõigetes 1–3, 5 ja 7 või § 8 lõigetes 1, 1^1, 4^1–5, 7 ja 8^1 sätestatud nõudeid (vt neid sätteid ka eelnõus ja seletuskirjas). Väärteokoosseis ei tähenda, et kõiki neid sätteid on rikutud, vaid asjakohasel juhul võib piisata ka ühe õigusnormi rikkumisest. Kommenteeritava paragrahvi lõige 1 määrab väärteotrahvi olukorras, kus ülioluline üksus on füüsiline isik, ning lõige 2 määrab väärteotrahvi olukorras, kus ülioluline üksus on juriidiline isik.
NIS2-direktiivi artikli 6 punkt 38 määratleb termini „üksus", mis on kavas võtta üle KüTSi § 2 punktiga 36 sõnastuses „juriidiline isik, kes on asutatud ja keda tunnustatakse tema tegevuskohajärgse riigi õiguse kohaselt ning kellel võivad olla õigused ja kohustused, või füüsiline isik". See tähendab, et eelnõuga sätestatavate nõuete subjekt võib olla kas füüsiline isik või juriidiline isik. Kui NIS2-direktiiv eristab üliolulisi üksusi ja olulisi üksusi, siis süüteokoosseisude puhul on vaja eristada ka füüsilist ja juriidilist isikut, kuna sanktsioonid (sh nende liigid) on nende isikute puhul erinevad. Kommenteeritavas paragrahvis on ka lisaeeldus – puudub KüTSi §-s 18^4 sätestatud väärteokoosseis. Sellekohane täiendus on lisatud, kuna osa piiriüleste elektrivoogudega seotud üksustest on ka NIS2-direktiivi kohaldamisalas. Seetõttu tuleb eristada olukorda, kus rikkuja on samal ajal ka üksus, kellele kohalduvad delegeeritud määruses (EL) 2024/1366 olevad nõuded (vt ka seletuskirjas KüTSi § 18^4 selgitusi).

Eelnõukohase KüTSi §-ga 18[3] on kavas võtta üle NIS2-direktiivi artikli 34 lõige 5, mille sisu on järgmine: „Liikmesriigid tagavad, et [NIS2-direktiivi] artikli 21 või 23 rikkumise korral määratakse kooskõlas käesoleva artikli lõigetega 2 ja 3 olulistele üksustele haldustrahv, mille maksimummäär on vähemalt 7 000 000 eurot või kuni 1,4 % selle ettevõtja ülemaailmsest aastasest kogukäibest eelneval majandusaastal (olenevalt sellest, kumb summa on suurem), kellele oluline üksus kuulub."
Kommenteeritava paragrahvi selgitused on sisuliselt samad, nagu on eelnõukohase KüTSi § 18^2 puhul, kuid selle erisusega, et § 18^3 puhul on rikkujaks oluline üksus.

Eelnõukohane KüTSi § 18[4] on seotud delegeeritud määruse (EL) 2024/1366 nõuete rikkumisega. Asjaomane erikoosseis on kavas tekitada, kuna NIS2-direktiivi rakendamisega hõlmataks KüTSi alla ainult üksikud üksused, kes on muidu hõlmatud delegeeritud määruse kohaldamisalasse – seda juhul, kui on täidetud mõlemad järgmised eeldused:
a) tegemist on piiriüleste elektrivoogude olukorraga;
b) need üksused on delegeeritud määruse (EL) 2024/1366 artikli 24 kohaselt suure või ülisuure mõjuga üksused.
Delegeeritud määruse (EL) 2024/1366 artikli 3 punktis 10 on termini „piiriülene elektrivoog" puhul viidatud määruse (EL) 2019/943 artikli 2 punktis 3 nimetatud piiriülesele võimsusvoole, mis on defineeritud kui „füüsiline elektrienergia voog liikmesriigi ülekandevõrgus, mille tekitab

[171] Eelnõus „üliolulised üksused".
[172] Eelnõus „üliolulistele üksustele".
[173] Eelnõus „ülioluline üksus".

väljaspool liikmesriiki asuvate tootjate, tarbijate või nende mõlema tegevuse mõju selle liikmesriigi ülekandevõrgule“.
Delegeeritud määruse (EL) 2024/1366 artikli 3 punktis 23 on „suure mõjuga üksus“ defineeritud kui „suure mõjuga protsessi teostav üksus, mille pädevad asutused on kindlaks teinud kooskõlas [delegeeritud määruse (EL) 2024/1366] artikliga 24“. Delegeeritud määruse (EL) 2024/1366 artikli 3 punktis 24 on termin „suure mõjuga protsess“ defineeritud kui „mis tahes tegevusprotsess, mida viib läbi üksus, mille puhul elektrienergia küberturvalisuse mõjuindeksid ületavad suure mõju künnise“.
Delegeeritud määruse (EL) 2024/1366 artikli 3 punktis 5 on „ülisuure mõjuga üksus“ defineeritud kui „üksus, kes viib läbi ülisuure mõjuga protsessi ja mille pädevad asutused on kindlaks teinud kooskõlas [delegeeritud määruse (EL) 2024/1366] artikliga 24“. Delegeeritud määruse (EL) 2024/1366 artikli 3 punktis 7 on termin „ülisuure mõjuga protsess“ defineeritud kui „üksuse tegevusprotsess, mille puhul elektrienergia küberturvalisuse mõjuindeksid ületavad ülisuure mõju künnise“.
Delegeeritud määruse (EL) 2024/1366 artikli 3 punktis 21 on „elektrienergia küberturvalisuse mõjuindeks“ ehk ECII-indeks defineeritud kui „indeks või liigitusskaala, mille abil järjestatakse küberrünnete võimalikud tagajärjed piiriüleste elektrivoogudega seotud tegevusprotsessidele“.
Ehk tegemist ei ole igasuguste üksustega, vaid nendega, mis kuuluvad vastava määratluse alla. Samuti ei ole kommenteeritava paragrahviga loodav väärteokoosseis erikoosseisu (vt KüTSi §-e 18^2 ja 18^3) kõigi NIS2-direktiivi ülevõtmisel KüTSi lisanduvate teenuseosutajate suhtes. Tegemist on ainult üksikute üksustega, kelle puhul see on vastav eri-väärteokoosseis – nimelt on nendeks üksusteks delegeeritud määruse artikli 2 lõike 1 punktis a (direktiivi (EL) 2019/944 artikli 2 punktis 57 määratletud elektriettevõtjad), punktis b (määruse (EL) 2019/943 artikli 2 punktis 8 määratletud määratud elektriturukorraldajad), punktis h (NIS2-direktiivi I lisas nimetatud laadimispunkti käitajad) ja punktis j (NIS2-direktiivi artikli 6 punktis 40 määratletud turbetarnijad (NIS2-direktiivis hallatud turbeteenuste osutajad, eelnõus infoturbeteenuse osutajad) nimetatud üksused.
Tuleb arvestada, et lisaks eelmainitud üksustele on kõnealuses delegeeritud määruse artikli 2 lõikes 1 märgitud ka muid üksusi, kellele määruse nõuded ja seeläbi ka kommenteeritava paragrahviga ette nähtud väärteokoosseis kohaldub.
Kuna ka eelmainitud NIS2-direktiiviga hõlmatud üksused on (vähemalt osaliselt) eeldatavasti üliolulised üksused, siis ei ole võimalik väärteotrahvi ülemmäära sätestamisel võtta eeskuju eelnõukohasest KüTSi §-st 18^3 ehk NIS2-direktiivis olulistele üksustele ette nähtud trahvide ülemmäärast. Seetõttu on rahatrahvide ülemmäära sätestamisel kommenteeritavas paragrahvis võetud eeskujuks eelnõukohases KüTSi §-s 18^2 olevast väärteokoosseisu ülemmäärast.
Kommenteeritava lõikega loodav väärteokoosseis sätestatakse ka seetõttu, et vastasel juhul ei oleks kõnealuse delegeeritud määruse kohaldamisalasse jäävate üksuste (sh ka NIS2-direktiiviga hõlmatud üksuste) puhul ette näha sarnast süüteokoosseisu nagu NIS2-direktiivi artikli 34 lõiked 4 ja 5 seda ette näevad, mis tekitaks võimaliku õigusliku lünga küberturvalisusega seotud nõuete täitmise tagamise kontrolli kontekstis.

Eelnõukohane KüTSi § 18^5 on seotud delegeeritud määruse (EL) 2024/1366 artikli 15 lõike 4 täitmisega, mille lõike 1 kohaselt määratakse seaduslik esindaja. Nimetatud seaduslik esindaja määratakse viidatud artikli lõike kohaselt, kui:
a) tegemist on piiriüleste elektrivoogude olukorraga (see tingimus ei ole *expressis verbis* viidatud lõikes, kuid on n-ö vaikiv eeltingimus);
b) tegemist on üksusega, kellel ei ole Euroopa Liidus tegevuskohta, kuid kes osutab teenuseid Euroopa Liidus asuvatele üksustele, ja
c) üksus on saanud teate, et ta on suure või ülisuure mõjuga üksus (vt delegeeritud määruse (EL)

2024/1366 artiklit 24).
Delegeeritud määruse (EL) 2024/1366 artikli 15 lõike 4 sisu on järgmine: „Käesolevast määrusest tulenevate kohustuste täitmata jätmise korral võib määratud seadusliku esindaja vastutusele võtta, ilma et see piiraks vastutust või kohtumenetlusi, mis võidakse algatada suure või ülisuure mõjuga üksuse enda suhtes.“
Delegeeritud määruse (EL) 2024/1366 artikli 15 lõike 2 kohaselt tuleb sellele esindajale anda ülesanne võtta vastu kõigi Euroopa Liidu pädevate asutuste [delegeeritud määruse (EL) 2024/1366 tähenduses] või küberintsidentide käsitlemise üksuste ehk CSIRTide pöördumisi (lisaks esindatavale suure või ülisuure mõjuga üksusele või selle üksuse asemel) seoses selle üksuse kohustustega, mis tulenevad delegeeritud määrusest (EL) 2024/1366. Suure või ülisuure mõjuga üksus annab oma seaduslikule esindajale vajalikud volitused ja piisavad vahendid, et tagada esindaja tõhus ja õigeaegne koostöö asjaomaste pädevate asutuste [delegeeritud määruse (EL) 2024/1366 tähenduses] või CSIRTidega.
Kuna delegeeritud määrus ei määratle, kas kõnealune seaduslik esindaja võib olla füüsiline või juriidiline isik, kohalduvad eelnõu kohaselt kommenteeritava paragrahvi süüteokoosseisud mõlemal juhul.

KüTSi § 19 lõike 1 muudatusega on kavas määrata eelnõukohastes KüTSi §-des 18^2–18^5 sätestatud väärtegude kohtuväliseks menetlejaks Riigi Infosüsteemi Amet. Kuigi julgeolekuasutusel on KüTSi § 14 lõike 5 kohaselt pädevus ka haldusjärelevalvet teha, ei ole talle võimalik selleks menetluspädevust luua. Seda põhjusel, et ainult kirjalikku hoiatamismenetlust (väärteomenetluse seadustiku § 54^1) kohaldatakse riigi, kohaliku omavalitsuse ja avalik-õigusliku juriidilise isiku suhtes, kuid eelnõuga KüTSis ette nähtavate väärteotrahvide puhul ei ole tegemist kirjaliku hoiatamismenetlusega, mistõttu ei ole KüTSis sätestatavaid väärteotrahve võimalik valitsusasutuste ja nende hallatavate asutuste ega kohaliku omavalitsuse üksuse asutuste suhtes kohaldada.

Eelnõukohane KüTSi § 19 lõige 2 on seotud NIS2-direktiivi artikli 35 ülevõtmise ning kohase rakendamisega. See on seotud koostööga isikuandmete kaitse valdkonna järelevalveasutustega ning nende teavitamisega, kui Riigi Infosüsteemi Amet on „järelevalve või täitmise tagamise käigus saanud teadlikuks sellest, et [NIS2-direktiivi] artiklites 21 ja 23 sätestatud kohustuste rikkumisega elutähtsa[174] või olulise üksuse poolt võib kaasneda isikuandmetega seotud rikkumine [isikuandmete kaitse üldmääruse artikli 4 punkti 12 tähenduses] ja millest tuleb teavitada kõnealuse määruse artikli 33 kohaselt.“.

Eelnõukohase KüTSi § 19 lõikega 4 on kavas määrata osa KüTSis eelnõuga sätestatavate väärtegude aegumistähtaeg.
Eelnõuga nr 94 SE tehti karistusseadustiku § 81 lõikesse 3 muudatus, et väärteo aegumistähtaeg on üldreeglina kaks aastat (kui selle lõpuleviimisest kuni selle kohta tehtud otsuse jõustumiseni on möödunud kaks aastat), kuid see võimaldab ka eriseadusega ette näha kuni viieaastast aegumistähtaega. Eelnõuga nr 94 SE muudeti ka isikuandmete kaitse seaduse § 73 lõiget 1, mille kohaselt on selles seaduses nimetatud väärtegude aegumistähtaeg kolm aastat.
Küberturvalisuse valdkonnaga seotud rikkumiste tuvastamine on sageli keeruline ning siin ei oleks üldreegel ehk kaheaastane aegumistähtaeg sobilik selleks, et rikkumisi avastada ja menetleda. Seetõttu tuleb eelnõuga ette näha ja pikendada KüTSi §-des 18^2, 18^3 ja 18^4 sätestatud väärtegude aegumistähtaega kahelt aastalt kolme aastani.

[174] Eelnõus „üliolulise üksuse“.

Selline pikem aegumistähtaeg on vajalik ka juhul, kui Riigi Infosüsteemi Amet tuvastab menetluses, et tegemist võib olla isikuandmete kaitse valdkonna nõuete rikkumisega, mistõttu ta teavitab sellest KüTSi § 19 lõike 2 kohaselt Andmekaitse Inspektsiooni. Kui Andmekaitse Inspektsioon ei alusta väärteomenetlust väärteokoosseisu puudumise tõttu (nt kui rikkumine ei ole seotud isikuandmete ja nende töötlemisega), siis jääb Riigi Infosüsteemi Ametil aega KüTSis sätestatud süüteokoosseisu olemasolul väärteomenetlus läbi viia.
KüTSis olevate muude väärteokoosseisude (vt KüTSi §-e 18^1 ja 185) kohta säilib praegu kehtiv üldreegel ehk kaheaastane aegumistähtaeg.

KüTSi §-s 20 kavandatavad muudatused tulenevad NIS2-direktiivi rakendamisega seotud esmastest ülesannetest Riigi Infosüsteemi Ametile. Sätestatavad tähtajad on määratud, lähtudes NIS2-direktiivi vastavate sätetega seotud tähtaegadest (alates NIS2-direktiivi kehtima hakkamisest).
Ülesannete tähtaegade arvutamise algusaeg on seotud eelnõu jõustumise kuupäevaga (vt eelnõu § 11). Hoolimata kommenteeritava lõike jõustumise tähtajast, on Riigi Infosüsteemi Ametil võimalik kommenteeritava paragrahviga seotud ülesandeid täita ka varem, st eelnõu vastuvõtmise protsessi ajal, et kiirendada iga ülesande täitmist.

Eelnõukohase KüTSi § 20 lõikega 1 kavandatav nõue on seotud NIS2-direktiivi artikli 3 lõike 3 ülevõtmise ja rakendamisega. Eelnõukohase KüTSi § 3^1 lõike 2 kohaselt koostab Riigi Infosüsteemi Amet iga kahe aasta järel teenuseosutajate ja domeeninimede registreerimise teenuse osutajate nimekirja. Kõnealune lõige on omakorda seotud KüTSi § 3^1 lõikega 1, mis määrab, millist teavet peavad teenuseosutajad ja domeeninimede registreerimise teenuse osutajad Riigi Infosüsteemi Ametile esitama. Selle info põhjal paneb Riigi Infosüsteemi Amet kokku KüTSi § 3 lõikes 2 nimetatud üksuste loetelu. Sisu poolest vastab vaadeldav säte NIS2-direktiivi artikli 3 lõikele 3.
Nimetatud lõige näeb ette järgmist: „Hiljemalt 17. aprilliks 2025 koostavad liikmesriigid elutähtsate[175] ja oluliste üksuste ning domeeninime registreerimise teenuseid osutavate üksuste[176] loetelu. Liikmesriigid vaatavad loetelu läbi ja asjakohasel juhul ajakohastavad seda korrapäraselt ning seejärel vähemalt iga kahe aasta järel.“ Selle lõike põhisisu on kirjas eelnõukohases KüTSi § 3^1 lõikes 2, kuid selle kohustuse esmakordse täitmise tähtaeg tuleb eraldi määrata, seetõttu tehakse seda kommenteeritavas lõikes.
NIS2-direktiivi hakati kohaldama alates 2024. aasta 18. oktoobrist ning NIS2-direktiivi artikli 3 lõikes 3 sätestatud tähtpäev (2025. aasta 17. aprill) saabus kuus kuud pärast NIS2-direktiivi kohaldamise kuupäeva. Arvestades siinse eelnõu vastuvõtmiseks vajalikku protseduuri ja aega, ei ole nimetatud kuupäev realistlik (ja on eelnõu Vabariigi Valitsusele esitamise ajaks ka möödas), mistõttu tuleb kommenteeritava lõikega seotud tähtaeg määrata teisiti. NIS2-direktiivi vastavas sättes tähtaja seadmise eeskujul kavandatakse ka kommenteeritava lõike puhul tähtajaks kuus kuud eelnõuga lisanduva KüTSi § 3^1 lõike 2 jõustumisest arvates (see lõige jõustub eelnõu jõustumise kuupäeval).

Eelnõukohase KüTSi § 20 lõikega 2 kavandatav nõue on seotud NIS2-direktiivi artikli 3 lõike 5 ülevõtmise ja rakendamisega. Nimetatud lõige näeb ette järgmist: „Hiljemalt 17. aprilliks 2025 ja seejärel iga kahe aasta järel teatavad pädevad asutused:
a) komisjonile ja koostöörühmale iga I või II lisas osutatud sektori ja allsektori kohta lõike 3

[175] Eelnõus „ülioluliste üksuste“.
[176] Eelnõus „domeeninimede registreerimise teenuse osutajate“.

kohases loetelus sisalduvate üksuste arvu ning
b) komisjonile asjakohase teabe seoses artikli 2 lõike 2 punktide b–e kohaselt kindlaks määratud elutähtsate[177] ja oluliste üksuste arvuga, I või II lisas osutatud sektori ja allsektoriga, kuhu need kuuluvad, nende osutatavate teenuste liigiga ning sellega, millise artikli 2 lõike 2 punktide b–e sätte kohaselt need kindlaks määrati.“ Tolle lõike põhisisu on kirjas eelnõukohase KüTSi § 3^1 lõigetes 5–7, kuid selle kohustuse esmakordse täitmise tähtaeg tuleb eraldi määrata, seetõttu tehakse seda kommenteeritavas lõikes.
NIS2-direktiivi artikli 3 lõikes 5 ette nähtud tähtaeg (2025. aasta 17. aprill) saabus kuus kuud pärast NIS2-direktiivi kohaldamise kuupäeva. Arvestades siinse eelnõu vastuvõtmise protseduuri ja aega, ei ole nimetatud kuupäev (2025. aasta 17. aprill) realistlik (see kuupäev on eelnõu Vabariigi Valitsusele esitamise ajaks ka möödas), mistõttu tuleb kommenteeritava lõikega seotud tähtaeg määrata teisiti. NIS2-direktiivi vastavas sättes tähtaja seadmise eeskujul kavandatakse ka kommenteeritava lõike puhul tähtajaks kuus kuud eelnõuga lisanduva KüTSi § 3^1 lõigete 5–7 jõustumisest arvates. Viidatud punktid jõustuvad eelnõu jõustumise kuupäeval.

Eelnõukohase KüTSi § 20 lõikega 3 kavandatav nõue on seotud NIS2-direktiivi artikli 23 lõike 9 esimese lause ülevõtmise ja rakendamisega. Nimetatud lause näeb ette järgmist: „Ühtne kontaktpunkt esitab ENISA-le iga kolme kuu tagant koondaruande, mis sisaldab anonüümseid koondandmeid käesoleva artikli lõike 1 ning artikli 30 kohaselt teatatud oluliste intsidentide, intsidentide, küber- ja intsidendiohtude kohta.“ Tolle lõike põhisisu on kirjas eelnõukohases KüTSi § 12 lõikes 4^1, kuid seal ei ole määratud selle kohustuse esmakordse täitmise tähtaega, seetõttu tehakse seda kommenteeritavas lõikes.
Tähtaja määramisel lähtutakse asjaolust, et kuigi NIS2-direktiivi vastavas lõikes pole konkreetset tähtpäeva mainitud, on nõude järgimine seotud NIS2-direktiivi kehtima hakkamisega Euroopa Liidu tasandil (18.10.2024). NIS2-direktiivi artikli 23 lõikes 9 ette nähtud tähtaeg (2025. aasta 17. jaanuar) saabus kolm kuud pärast NIS2-direktiivi kohaldamise kuupäeva. Arvestades siin kommenteeritava eelnõu vastuvõtmise protseduuri ja aega, ei ole see kuupäev (2025. aasta 17. jaanuar) realistlik (ja on eelnõu Vabariigi Valitsusele esitamise ajaks ka möödas), mistõttu tuleb kommenteeritava lõikega seotud tähtaeg määrata teisiti. NIS2-direktiivi vastavas sättes tähtaja seadmise eeskujul kavandatakse ka kommenteeritava lõike puhul tähtajaks kolm kuud eelnõuga lisanduva KüTSi § 12 lõike 4^1 jõustumisest arvates. Viidatud lõige jõustub eelnõu jõustumise kuupäeval.

Eelnõukohane KüTSi § 28^1. Eelnõuga on kavas täiendada KüTSi §-ga 28^1, milles nähakse ette üleminekusätted seaduse rakendamiseks teenuseosutajatele, kes on juba kehtiva KüTSi subjektid, aga kes peavad seadusemuudatuse tõttu hakkama uusi nõudeid rakendama senisest laiemas ulatuses (senisel regulatiivsel lähenemisel põhinenud teenusepõhised nõuded *vs*. organisatsiooniülesed nõuded NIS2-direktiivi alusel). Väärib rõhutamist, et seda sätet kohaldatakse üksnes piiratud aja jooksul pärast seadusemuudatuse jõustumist. Kui eelnõukohane KüTSi § 20 näeb Riigi Infosüsteemi Ametile ette tähtajad eelnõuga loodavate reeglite esmaseks rakendamiseks, siis kõnealuses §-s nähakse ette tähtajad KüTSi subjektidele eelnõust tulenevate reeglite rakendamiseks.
Kõnealune säte ei kohaldu sellistele KüTSi subjektidele (teenuseosutajatele ja domeeninimede registreerimise teenuse osutajatele), kes täidavad KüTSi kohaselt teenuseosutaja või domeeninimede registreerimise teenuse osutaja definitsiooni tunnustele vastavuse esimest korda kas KüTSi uute reeglite jõustumise mõjul või millalgi tulevikus. Sellistele isikutele kohaldub

[177] Eelnõus „üliolulise üksuste“.

eelnõukohane KüTSi § 4^1, mis reguleerib nõuete esmakordset täitmist. Siin kommenteeritav säte kohaldub üksnes sellistele teenuseosutajatele, kes on juba praegu KüTSi kohaldamisalas (vt kehtiva KüTSi § 3 lõikeid 1 ja 4). Seetõttu on ka kõigis selle sätte lõigetes viidatud teenuseosutaja tunnustele vastamisele enne uute KüTSi reeglite jõustumist.
Kõnealune säte kohaldub üksnes teenuseosutajatele (sh digitaalse teenuse osutajatele ja näiteks ka elutähtsa teenuse osutajatele), mitte aga domeeninime registreerimise teenuse osutajatele, sest kehtiva KüTSi kohaselt ei vasta viimased teenuseosutaja tunnustele. Tegemist on KüTSi mõttes täiesti uute subjektidega ja seetõttu kohaldub neile eelnõukohane KüTSi § 4^1, täpsemalt selle lõige 1 (nende üksuste puhul vt ka eelnõukohase KüTSi § 2 punkti 2 ja § 4^1 lõike 3 selgitusi).

Eelnõukohane KüTSi § 28^1 lõige 1. Teenuseosutaja, kes vastas teenuseosutaja tunnustele enne eelnõukohase KüTSi § 3^1 lõike 1 jõustumist (ehk enne Riigi Infosüsteemi Ametile enda kohta teabe esitamise kohustuse jõustumist), täidab KüTSi § 3^1 lõikes 1 sätestatud kohustuse kolme kuu jooksul alates viidatud lõike jõustumisest. KüTSi § 3^1 lõikes 1 on sätestatud teave, mille teenuseosutajad peavad Riigi Infosüsteemi Ametile esitama. Kommenteeritava KüTSi § 28^1 lõikest 1 tuleneb neile selleks tähtaeg – kolm kuud alates KüTSi § 3^1 lõike 1 jõustumisest. Selliselt on Riigi Infosüsteemi Ametil omakorda võimalik koostada KüTSi § 3^1 lõikes 2 sätestatud nimekiri kõigist teenuseosutajatest.

Eelnõukohane KüTSi § 28^1 lõige 2. Digitaalse teenuse osutaja, kes oli teenuseosutaja enne eelnõukohase KüTSi § 4 lõike 7 jõustumist (vt siin ennekõike kehtiva KüTSi § 4 lõiget 1), täidab eelnõu järgi KüTSi § 4 lõigetes 1 ja 10 sätestatud kohustused kolme kuu jooksul alates KüTSi § 4 lõike 7 jõustumisest. KüTSi § 4 lõikes 1 on nähtud ette digitaalse teenuse osutaja kohustus esitada Riigi Infosüsteemi Ametile andmeid. Eelnõukohasest KüTSi § 4 lõikest 10 tuleneb digitaalse teenuse osutajale kohustus teatud juhtudel määrata digitaalse teenuse osutaja esindaja, sealhulgas tuleb teha esindaja kontaktandmed püsivalt avalikult kättesaadavaks. Kommenteeritava KüTSi § 28^1 lõikest 2 tuleneb neile selleks tähtaeg – kolm kuud alates KüTSi § 4 lõike 7 jõustumisest. Sätte rakendamine on seotud selle lõike jõustumisega, kuivõrd see on uus säte, mis luuakse kõnealuse eelnõuga. See võimaldab siduda kõnealuses sättes nimetatud kohustuste täitmise eelnõust tulenevate muudatuste jõustumisega. Tähtaja määramisel on võetud eeskuju NIS2-direktiivi artikli 27 lõikest 3, mis on kavas võtta üle eelnõukohase KüTSi § 4 lõikega 6. See sätestab digitaalse teenuse osutajale kohustuse teavitada KüTSi § 4 lõikes 1 ette nähtavate andmete muudatustest viivitamata, kuid hiljemalt kolme kuu jooksul alates muudatuse kuupäevast. Edastatava teabe hulgas on ka teave digitaalse teenuse osutaja esindaja kontaktandmete kohta ehk need kohustused on omavahel seotud: kui on kohustus esindaja määrata ja seda pole tehtud, siis pole ka võimalik edastada esindaja kontaktandmeid. NIS2-direktiiv ei sätesta, millise tähtaja jooksul peab digitaalse teenuse osutaja enda esindaja määrama (vt NIS2-direktiivi artikli 26 lõiget 3, mis võetakse üle eelnõukohase KüTSi § 4 lõikega 10), kuid kuna eelnõukohases KüTSi § 4 lõikes 1 oleva teabe uuendamine peab toimuma kolme kuu jooksul alates vastavast muudatusest, lähtutakse kõnealuses lõikes samast tähtajast.

Eelnõukohane KüTSi § 28^1 lõige 3. Teenuseosutaja ja digitaalse teenuse osutaja, kes oli teenuseosutaja enne eelnõukohase KüTSi § 3^1 lõike 1 kavandatavat jõustumist (ehk enne Riigi Infosüsteemi Ametile enda kohta teabe esitamise kohustuse jõustumist), viib eelnõu kohaselt oma tegevuse KüTSis ja selle alusel kehtestatavate nõuetega vastavusse kolme aasta jooksul alates viidatud lõike jõustumisest. Sätte eesmärk on anda sellistele KüTSi subjektidele, kes on juba kehtiva KüTSi subjektid, kuid peavad nüüd arvestama eelnõuga kavandatavate KüTSi reeglitega, kolmeaastane üleminekuaeg oma tegevuse kooskõlla viimiseks uute reeglitega ning nende

rakendamiseks. Täiesti uute KüTSi subjektide suhtes kohaldatakse eelnõu kohaselt KüTSi §-s 4^1 ette nähtavat reeglit.
Praktikas ei hakata kohaldama kommenteeritavat lõiget (st selle esimest lauset) neile teenuseosutajatele, kelle kogu tegevusele kohalduvad KüTSi nõuded ka kehtiva KüTSi järgi – näiteks eelnõukohastes KüTSi § 2 punktides 14 ja 15 nimetatud keskvalitsuse avaliku halduse üksused ning kohaliku omavalitsuse avaliku halduse üksused.
Siin kommenteeritavat lõiget hakatakse kohaldama neile elutähtsa teenuse osutajatele, kes vastavad mõlemale järgmisele tunnusele:

a) elutähtsa teenuse osutaja oli enne kõnealuse eelnõu jõustumist KüTSi subjekt KüTSi kehtiva redaktsiooni § 3 lõike 1 punkti 1 alusel;
b) elutähtsa teenuse osutajale kohalduvad hädaolukorra seaduse § 53 lõiked 12 ja 13 (ehk ta oli elutähtsa teenuse osutaja enne 18.10.2024 ning tema suhtes ei koostata hädaolukorra seaduse § 38 lõikes 1^2 nimetatud haldusakti ja tema suhtes ei kohaldata sama seaduse § 38 lõikes 1^3 sätestatud kohustuse täitmise tähtaegu).

Kommenteeritava paragrahvi lõigetes 1 ja 2 sätestatavad kohustused täidab teenuseosutaja eelnõu kohaselt nendes lõigetes määratud tähtajaks. Seega, kohustus esitada Riigi Infosüsteemi Ametile eelnõukohases KüTSi § 3^1 lõikes 1 ja § 4 lõikes 1 nimetatud andmed (sealhulgas kohustus digitaalse teenuse osutajal asjakohasel juhul määrata esindaja) tuleb täita kolme kuu jooksul alates eelnõuga tehtavate muudatuste jõustumisest. Seejärel on teenuseosutajatel kolm aastat arvates muudatuste jõustumisest (ehk hiljemalt kaks aastat ja üheksa kuud teavituse tegemisest, kui teavitus tehti viimasel päeval) aega enda tegevus üldiselt uute KüTSi reeglitega kooskõlla viia.

Eelnõukohane KüTSi § 28^1 lõige 4 näeb ette erireegli lõike 3 suhtes. Elutähtsa teenuse osutaja, kellel tekkis esmakordselt KüTSi järgimise kohustus pärast 2024. aasta 18. oktoobrit ja kes vastas eelnõuga KüTSis sätestatavatele teenuseosutaja tunnustele enne, kui jõustub eelnõukohane KüTSi § 3^1 lõige 1, peab oma tegevuse viima vastavusse KüTSi ja selle alusel kehtestatavate nõuetega hädaolukorra seaduse § 38 lõike 1^3 punktis 3 sätestatavas korras määratavaks tähtajaks. Selline üleminekureegel on vajalik põhjusel, et elutähtsa teenuse osutaja on eelnõukohase KüTSi mõttes ülioluline üksus, kuid ta määratakse elutähtsa teenuse osutajaks hädaolukorra seaduse § 38 alusel haldusaktiga. Seetõttu on ka neile KüTSi reeglite kohaldamine seotud nende elutähtsa teenuse osutajaks määramisega hädaolukorra seaduse tähenduses.
Hädaolukorra seaduse muudatusi on põhjalikumalt selgitatud hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu nr 426 SE seletuskirjas.[178]
Hädaolukorra seaduse § 38 lõike 1^3 kohaselt antakse selles haldusaktis, millega isik elutähtsa teenuse osutajaks määratakse, tähtaeg hädaolukorra seaduses ja muudes õigusaktides elutähtsa teenuse toimepidevuse tagamiseks sätestatud nõuete täitmiseks. KüTSi nõudeid võib pidada „muudes õigusaktides elutähtsa teenuse toimepidevuse tagamiseks sätestatud nõueteks“. Seetõttu on ka KüTSi rakendamine elutähtsa teenuse osutajatele seotud hädaolukorra seaduse alusel haldusaktis määratava tähtajaga.
Juba olemasolevatele elutähtsa teenuse osutajatele kohalduvad hädaolukorra seaduse üleminekusätted. Hädaolukorra seaduse § 53 lõigete 12 ja 13 kohaselt loetakse enne 2024. aasta 18. oktoobrit hädaolukorra seaduse § 38 lõike 2 tingimustele vastav isik elutähtsa teenuse osutajaks päevast, mil ta esmakordselt täitis nimetatud tingimused. See tähendab, et nende kohta ei koostata eraldi haldusakti. Seetõttu on ka kommenteeritavas üleminekusättes lähtutud samast 18.10.2024. a tähtpäevast. Lõige 4 kohaldub üksnes sellistele elutähtsa teenuse osutajatele, kes määrati elutähtsa teenuse osutajaks haldusaktiga pärast 18.10.2024.

[178] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/57e67d9e-ba15-412e-8b25-cda84efca58a/

Nendel elutähtsa teenuse osutajatel, kes olid enne KüTSi subjektid ainult konkreetse elutähtsa teenuse poolest, kuid kellele nüüd laienevad nõuded tervenisti, tuleb seetõttu lähtuda eelnõukohasest KüTSi § 28^1 lõikest 3, kus sätestatakse ka nende üleminekuaeg KüTSi reeglite rakendamiseks. Nendele elutähtsa teenuse osutajatele, kes saavad KüTSi teenuseosutajateks pärast siin kommenteeritava eelnõu jõustumist, hakkab kohalduma eelnõukohase KüTSi § 4^1.
Nagu eelnõukohase KüTSi § 28^1 lõike 3 puhul, peab ka elutähtsa teenuse osutaja täitma kommenteeritava paragrahvi lõigetes 1 ja 2 sätestatavad kohustused nendes sätetes eelnõuga ette nähtud tähtajal ehk kolme kuu jooksul arvates vastavaid kohustusi ette nägevate sätete jõustumisest. Seejärel on elutähtsa teenuse osutajal aega enda tegevus KüTSiga kooskõlla viia hädaolukorra seaduse § 38 lõike 1^3 punkti 3 kohaselt määratud tähtaja jooksul.

Eelnõukohane KüTSi § 28^2. Eelnõu kohaselt täiendatakse KüTSi uue §-ga 28^2, milles nähakse ette küberturvalisuse taseme tõstmise toetusega seotud sätted. Eesmärk NIS2-direktiivi üle võtva eelnõu vastuvõtmise järel on a) alustada kohe toetuste andmisega ning b) anda toetust nii praegustele kui ka tulevastele KüTSi subjektidele.

Eelnõukohane KüTSi § 28^2 lõige 1 määrab kindlaks, kellele on toetus mõeldud ning mis eesmärgil seda saab kasutada. Toetus on mõeldud:

a) KüTSi teenuseosutajatele, kes nii kehtiva KüTSi kohaselt kui ka eelnõuga kavandatu järgi peavad edaspidi KüTSi nõudeid täitma*;*
b) muudele isikutele, kes soovivad KüTSi nõudeid täita või oma küberturvalisuse taset parandada. Selleks võib olla näiteks üksus, kes ei ole KüTSi teenuseosutaja, kuid kes osutab KüTSi teenuseosutajale toetavaid teenuseid ehk on n-ö alltöövõtja (näiteks eelnõu tähenduses haldusteenuse osutaja või infoturbeteenuse osutaja, kuid kes ei täida soovituse 2003/361/EÜ kohaseid keskmise suurusega ettevõtja näitajaid ehk tegemist võib olla teenuseosutaja tarneahelas oleva üksusega), samuti ka mõni muu üksus, kes ei pea eelnõu kohaselt KüTSi nõudeid järgima, kuid soovib enda küberturvalisuse taset parandada. Selleks võib olla ka domeeninimede registreerimise teenuse osutaja, kes ei ole teenuseosutaja, kuid kes peab üksikuid KüTSi nõudeid täitma (vt selle kohta eelnõukohase KüTSi § 2 punkti 2 selgitust).

Ka avalikul kooskõlastusringil olnud eelnõu tagasisides sooviti teada saada, kas see toetus on mõeldud ka muudele üksustele kui KüTSi subjektidele (teenuseosutajatele), näiteks tema alltöövõtjatele. Eelnõu tagasisides mainiti, et on ettevõtjaid, kes peavad KüTSi nõudeid järgima seetõttu, et nad osutavad KüTSi subjektile teenust (eelduslikult lepinguliste kohustuste tõttu). Et KüTSi subjekt ei peaks loobuma oma koostööpartnerist, kes peab vastama KüTSi nõuetele, oli tagasiside andjate ootus, et see toetus laieneks ka KüTSi subjekti alltöövõtjale. See on ka üks põhjus, miks kommenteeritavas paragrahvis sätestatavat toetust soovitakse anda ka muudele isikutele kui KüTSi teenuseosutajatele.

Eelnõukohane KüTSi § 28^2 lõige 2 sätestab, et tegemist on pigem ajutise toetusega ehk seda ei anta lõpmatult, vaid kuni toetuseelarve ammendumiseni (vt ka seletuskirja peatükki 7.4).

Vabariigi Valitsuse istungil 26.09.2023[179] kiideti Vabariigi Valitsuse protokollilise otsusega heaks 2024. a riigieelarve seaduse eelnõu, kus otsustati arvata õigusaktidest tulenevateks lisakuludeks vajalikud lisavahendid Majandus- ja Kommunikatsiooniministeeriumile. 2024. a

[179] https://valitsus.ee/uudised/valitsus-kiitis-heaks-ja-saadab-riigikogule-2024-riigieelarvega-seotud-eelnoud, https://www.riigikogu.ee/tegevus/eelnoud/eelnou/1ef04a09-9881-4ba1-92fa-99e924d5f5f9/riigieelarve-seaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus/

struktuurimuudatuse käigus planeeriti riigieelarve strateegia 2025–2028 protsessis need vahendid Justiits- ja Digiministeeriumile. Nimetatud vahendeid kajastatakse Vabariigi Valitsuse sihtotstarbelise reservi tegevuste loetelus jaotises „Õigusaktidest tulenevad meetmed“ ja neid eraldatakse vastavalt vajadusele kooskõlastatult Justiits- ja Digiministeeriumi riikliku küberturvalisuse talitusega. Siinse eelnõu teisel lugemisel Riigikogus taotleb ministeerium riigieelarve seaduse § 58 lõike 11 alusel ning kooskõlas Vabariigi Valitsuse 31.07.2024. a määruse nr 123 „Vabariigi Valitsuse reservist vahendite eraldamise ja eraldatud vahendite kasutamise kord“ § 1 punktiga 2 Vabariigi Valitsuse sihtotstarbeliste vahendite reservist Vabariigi Valitsuse protokollilise otsusega määratud vahendite eraldamist ministeeriumi vastavate aastate eelarvesse, et katta kõnealuse eelnõuga NIS2-direktiivi ülevõtmist toetava meetme käivitamise ja rakendamise kulud.

Eelnõukohase KüTSi § 28[2] lõikega 3 on kavas sätestada riikliku küberturvalisuse valdkonna eest vastutavale ministrile volitusnorm kehtestada määrus, milles täpsustatakse toetuse taotlemise, andmise, kasutamise ja tagasinõudmise tingimused ja kord. Lisaks kommenteeritavale lõikele on määruse andmise volitusnormiks ka riigieelarve seaduse § 53[1] lõige 1, mis on muude sarnaste toetuste puhul olnud piisav volitusnorm konkreetse toetusega seotud määruse kehtestamiseks.[180] Määruse kavandi leiab seletuskirja lisast 2 (määruste kavandid). Kui selle toetuse raames otsustatakse sõlmida haldusleping, kohaldatakse ka riigieelarve seaduse § 53[1] lõiget 2 ning seal viidatud sätteid.

KüTSi muutmise viimase punktiga on kavas sõnastada normitehniline märkus ümber nii, et edaspidi viidatakse varasema küberturvalisuse valdkonna direktiivi asemel NIS2-direktiivile.

Eelnõu §-d 2–9 on ennekõike seotud kas 1) NIS2-direktiivis ette nähtud muudatusega, 2) KüTSi §-dele 7 ja 8 tehtud ristviite kaotamisega või 3) muude tehniliste muudatustega, mis on vajalikud kõnealuse eelnõu rakendamiseks.

§ 2. E-identimise ja e-tehingute usaldusteenuste seaduse muudatus

E-identimise ja e-tehingute usaldusteenuste seaduse § 4 sisu on praegu järgmine:
„§ 4. Turvaintsidentidest teavitamise kohustus
Usaldusteenuse osutaja teavitab pädevat asutust Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 19 lõike 2 kohasest turvaintsidendist viivitamata, kuid mitte hiljem kui 24 tunni jooksul pärast sellest teadasaamist.“
See paragrahv on kavas tunnistada kehtetuks, kuna NIS2-direktiivi artikliga 42 jäetakse määruse (EL) nr 910/2014 artikkel 19 nimetatud määrusest välja alates 18.10.2024. Viidatud artikli 19 põhisisu (usaldusteenuse osutajate suhtes kohaldatavad turvanõuded) on NIS2-direktiivi artiklite 21 ja 23 tõttu edaspidi eelnõu kohaselt KüTSi §-des 7 ja 8, sh seal viidatud Euroopa Komisjoni rakendusaktides. Seetõttu tunnistataksegi eelnõu kohaselt kõnealune § 4 kehtetuks.

§ 3. Eesti Rahvusringhäälingu seaduse muudatused

Kehtivas õiguses on Eesti Rahvusringhäälingu seaduses (§ 5 lg 2[1], § 34 lg 4[1]), elektroonilise side

[180] Riigieelarve seaduse § 53[1] lõike 1 ja selle ning muude õigusaktide alusel kehtestatud määrused on leitavad siit: https://www.riigiteataja.ee/dynaamilised_lingid.html?dyn=130042025004&id=47f6ff40-c8bf-4acf-ad60-e32c9009de5f-468a1454-dfcf-4618-aac0-a3e2fbb20930. Teise olukorra puhul vt nt ettevõtlus- ja infotehnoloogiaministri 21.03.2022. a määrust nr 23 „Ettevõtja rakendusuuringute määrus“ ning haridus- ja teadusministri 03.04.2024. a määrust nr 13 „Välisriigis kõrgharidustasemel õppimiseks ja erialaseks täiendamiseks antavate stipendiumite andmise tingimused ja kord“.

seaduses (§ 87^2 lg 6, § 100^3 lg 2, § 100^4 lg 2, § 100^5 lg 2, § 133 lg 5), hädaolukorra seaduses (§ 41 lg 1 ja § 45 lg 1 p 4), lennundusseaduses (§ 59^1, § 60^1 lg 5), raudteeseaduses (§ 8, § 143 lg 1 p 8 ja lg 8), sadamaseaduses (§ 13 lg 4, § 42 lg 5) ja tervishoiuteenuste korraldamise seaduses (§ 10 lg 2, § 17 lg 1^2, § 22 lg 4^2, § 60 lg 2) sätestatud nõue stiilis „X on kohustatud Y teenuse osutamiseks kasutatavate võrgu- ja infosüsteemide turvalisuse tagamiseks täitma küberturvalisuse seaduse §-dega 7 ja 8 ning nende alusel kehtestatud nõudeid“ ning et „Riigi Infosüsteemi Amet teostab viidatud nõude teemal järelevalvet küberturvalisuse seaduses sätestatud pädevuse piires.“
Eelnõu koostades nähti kolme varianti tegeleda asjaoluga, et eriseadustes on olemas viited KüTSi §-dele 7 ja 8 ning nende nõuete täitmisele vastava KüTSi teenuseosutaja poolt, sh ka järelevalve korralduse kohta:
1) eemaldada taolised ristviited valdkondlikest eriseadustest;
2) lisada eelnõu kohaselt uute KüTSi teenuseosutajate puhul nendesse valdkondlikesse eriseadustesse sama sisuga sätted, nagu on praegu eespool mainitud eriseadustes;
3) jätta senine olukord muutmata.
Siinse seletuskirja kontekstis mõeldaks eriseaduste all muid seadusi kui KüTSi, mis selle kohase teenuseosutaja tegevust reguleerib.
Kolmas variant ehk senise olukorra muutmata jätmine ei sobi, kuna selle tagajärjel osas eriseadustes oleksid asjaomased õigusnormid ja teistes ei oleks. Seega tuleb teha valik esimese ja teise variandi vahel.
Esimest varianti rakendades oleks ühes seaduses ehk KüTSis loetelu kõikidest tema subjektidest ehk teenuseosutajatest ja domeeninimede registreerimise teenuse osutajatest koos nõuetega, mida need üksused peavad küberturvalisuse valdkonnas täitma. See tagaks ka suurema selguse ja kindluse, et KüTS on Eesti õiguses üks ühine n-ö horisontaalne õigusakt, millest KüTSis nimetatud teenuseosutajad ja domeeninimede registreerimise teenuse osutajad lähtuvad. Kuigi ka siin oleks erisusi, tuleksid need ennekõike Euroopa Liidu õiguse nõuetest ning sellises olukorras kehtib eelnõu kohaselt KüTSi § 1 lõige 4 (vt asjaomaseid selgitusi).
Teine variant tähendaks, et eelnõuga tuleb täiendada muid valdkondlikke eriseadusi, mis reguleerivad eelnõu tähenduses uusi KüTSi teenuseosutajaid. See tähendaks täienduste või muudatuste tegemist vähemalt järgmistes seadustes: arenguseire seadus, avaliku teabe seadus, e-identimise ja e-tehingute usaldusteenuste seadus, elektrituruseadus, elektroonilise side seadus, kaugkütteseadus, kohaliku omavalitsuse korralduse seadus, maagaasiseadus, metsaseadus, raudteeseadus, sadamaseadus, väärtpaberituru seadus, veeseadus, postiseadus ja Vabariigi Valitsuse seadus, aga ka muud seadused, mis reguleerivad avalik-õiguslike juriidiliste isikute tegevust. Nende seaduste arv on suurem, kuna täiendusi tuleks teha ka nendes seadustes, mis reguleerivad avaliku sektori subjekte ehk kehtiva KüTSi puhul § 3 lõikes 4 olevaid organisatsioone, mida eelnõuga kavandatu kohaselt hõlmavad edaspidi KüTSi § 3 lõike 2 punktid 3, 4 ja 7 ning lõike 4 punktid 1–4 ja 6. Kui tulevikus lisanduks KüTSi uusi teenuseosutajate valdkondi või sektoreid, tuleks teha täiendusi ka nendes eriseadustes. See kõik omakorda suurendab õigusloome mahtu.
Arvestades eeltoodut, on eelnõu koostajad lähtunud esimesest variandist ehk eelnõuga eemaldatakse eriseadustest viited KüTSi asjaomastele sätetele, sh vastavate nõuete järelevalve korraldusele. Selle variandi puhul on vaja ka vähem õigusloomet, kuna ei teki vajadust teha uute valdkondade eriseadustes ristviiteid KüTSi nõuetele (ka tulevikus). Kui mõne konkreetse ja kitsa erisuse tekitamiseks eriseaduses peaks vajadus tekkima, saab seda analüüsida KüTSile tehtava ristviite koostamise käigus.
Eeltoodu tõttu tunnistatakse ka Eesti Rahvusringhäälingu seaduse § 5 lõige 2^1 kehtetuks, kuna see teeb viite KüTSi §-dele 7 ja 8.
Eesti Rahvusringhäälingu kohta on asjakohane mainida, et 531 SE kohaste ehk KüTSi 2022. aastal

jõustunud muudatuste tulemusena pidanuks Eesti Rahvusringhääling saama avalik-õigusliku juriidilise isikuna kogu oma tegevusega KüTSi tähenduses teenuseosutajaks alates 01.01.2027. a. Sel teemal on 531 SE seletuskirja lk-l 29 märgitud:
Eelnõu § 3 jäetakse Eesti Rahvusringhäälingu seaduse § 5 lõikest 21 välja sõnad „käesoleva paragrahvi lõike 1 punktis 10 sätestatud ülesande täitmiseks kasutatavate“.
[531 SE seletuskirjas in tolle seaduseelnõu] § 1 punkti 5 juures on selgitatud, miks eemaldatakse Eesti Rahvusringhääling KüTS § 3 lõike 1 loetelust. „Nimetatud muudatuse tõttu tuleb ka Eesti Rahvusringhäälingu tegevust reguleeriv eriseadus, kus on viited KüTS §-de 7 ja 8 kohaldumisele, viia kooskõlla kavandatava KüTS § 3 lõikega 1 ning lõikega 4. Eesti Rahvusringhäälingu kui teenuse osutaja kohta käivas eriseaduses tehakse muudatus, et valdkondlik seadus oleks ülejäänud eelnõuga kooskõlas. Siinne muudatus jõustub samal ajal eelnõu § 1 punktiga 5 ehk 2027. aasta 1. jaanuaril.
Kuivõrd Eesti Rahvusringhääling on teenuseosutaja kehtiva KüTSi § 3 lõike 1 punkti 10 alusel kuni 2026. aasta 31. detsembrini (vt eelnõu § 1 punkti 5 ja § 4 lõike 2 selgitusi) ja eelnõu § 1 punkti 6 kohaselt oleks KüTSi § 3 lõike 4 punkti 11 alusel alates 2027. aasta 1. jaanuarist (eelnõu § 4 lõike 2 tõttu), siis kohaldatakse samast kuupäevast Eesti Rahvusringhäälingule küberturvalisuse nõudeid KüTSi teenuseosutaja kohustusi reguleerivate sätete alusel.
Vahepeal on toimunud muudatused Eesti Rahvusringhäälingu seaduse (eelnõu nr 426 SE) tõttu, mille vastuvõtmise järel on Eesti Rahvusringhääling edaspidi elutähtsa teenuse osutaja hädaolukorra seaduse tähenduses. Eelnõuga nr 426 SE on kavas hädaolukorra seaduse § 38 lõike 1^3 punktis 3 ette näha, et uued elutähtsa teenuse osutajad peavad elutähtsa teenuse toimepidevuse tagamiseks oma tegevuse sellele sätestatud nõuetega vastavusse viima kuni viie aasta jooksul alates elutähtsa teenuse osutajaks määramisest arvates. Viimane lauseosa tähendab ennekõike seda, et elutähtsa teenuse osutaja suhtes on tehtud elutähtsa teenuse osutajaks määramise haldusakt, milles sätestatakse ka KüTSi nõuete täitmise tähtaeg. Seega on Eesti Rahvusringhäälingul lisaaeg, et enda tegevus ka eelnõuga KüTSis sätestatavate nõuetega vastavusse viia.
Kuigi siin kommenteeritava eelnõuga muudetakse ka hädaolukorra seaduse § 38 lõike 1^3 punkti 3 sõnastust, jääb selle põhisisu samaks (vt eelnõu § 5 punkti 1 selgitusi).

Lisaks on kavas tunnistada Eesti Rahvusringhäälingu seaduse § 34 lõige 4^1 kehtetuks, kuna see on seotud eelkirjeldatud muudatusega. Kui muudatust ei tehtaks, oleks nimetatud seaduses jätkuvalt nõue, et Riigi Infosüsteemi Amet teeb KüTSi alusel järelevalvet kommenteeritavas õigusnormis viidatud nõuete täitmise üle.

§ 4. Elektroonilise side seaduse muudatused

Elektroonilise side seaduse § 87^2 on kavas tunnistada kehtetuks, kuna NIS2-direktiivi artikliga 43 jäeti direktiivi (EL) 2018/1972 artiklid 40 ja 41 nimetatud direktiivist alates 18.10.2024 välja. Viidatud artiklite põhisisu (vastavalt „võrkude ja teenuste turvalisus“ ning „rakendamine ja jõustamine“) on NIS2-direktiivi artiklite 21 ja 23 tõttu siin kommenteeritava eelnõu kohaselt edaspidi KüTSi §-des 7 ja 8, sh seal viidatud Euroopa Komisjoni rakendusaktides. Lisaks on ka elektroonilise side seaduse § 87^2 lõikes 6 viide KüTSi §-dele 7 ja 8 (vt sel teemal ka eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Elektroonilise side seaduse § 100^3 lõige 3 on kavas tunnistada kehtetuks, kuna selles on viide KüTSi §-dele 7 ja 8 (vt eelnõu § 3-ga Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Elektroonilise side seaduse § 100^4 lõige 2 on kavas tunnistada kehtetuks, kuna selles on viide

KüTSi §-dele 7 ja 8 (vt eelnõu § 3-ga Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Elektroonilise side seaduse § 100[5] lõige 2 on kavas tunnistada kehtetuks, kuna selles on viide KüTSi §-dele 7 ja 8 (vt eelnõu § 3-ga Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Elektroonilise side seaduse § 133 lõige 5 on kavas tunnistada kehtetuks, kuna eelnevalt kommenteeritud muudatustega on kavas tunnistada kehtetuks ristviited KüTSi §-dele 7 ja 8 ning tolle seaduse § 133 lõige 5 määrab kindlaks eelmainitud lõigetes sätestatu üle järelevalve tegemise aspektid. Kui muudatust ei tehtaks, oleks nimetatud seaduses jätkuvalt nõue, et Riigi Infosüsteemi Amet teeb elektroonilise side seaduse ja KüTSi alusel järelevalvet kommenteeritavas õigusnormis viidatud nõuete täitmise üle (vt ka eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Kavatsus tunnistada kehtetuks e**lektroonilise side seaduse § 170[1]** on seotud sama seaduse § 87[2] ja 188 lõike 8 kehtetuks tunnistamistega ehk ennekõike NIS2-direktiivi artikli 43 ülevõtmisega. Elektroonilise side seaduse § 170[1] näeb ette väärteokoosseisu sidevõrkude ja -teenuste turvalisusele ning terviklikkusele kehtestatud nõuete rikkumise korral. Nende nõuete sisu on määratud kindlaks sama seaduse §-s 87[2], mis on kavas tunnistada kehtetuks. Kõnealuse väärteokoosseisu põhisisu hakkab edaspidi olema KüTSi 5. peatükis.

Kavatsus tunnistada kehtetuks **elektroonilise side seaduse § 188 lõige 8** on seotud sama seaduse § 87[2] ja 170[1] kehtetuks tunnistamistega ehk ennekõike NIS2-direktiivi artikli 43 ülevõtmisega. Eelnõu kohaselt kehtetuks tunnistatava lõike (elektroonilise side seaduse § 188 lõige 8) järgi on Riigi Infosüsteemi Amet elektroonilise side seaduse §-s 170[1] sätestatud väärteo kohtuväline menetleja. Kuna viidatud väärteokoosseisu sisaldav säte tunnistatakse kehtetuks ja selle põhisisu on eelnõu kohaselt edaspidi KüTSis, tuleb ka menetluspädevuse määramisega seotud õigusnorm kehtetuks tunnistada.

§ 5. Hädaolukorra seaduse muudatused

Eelnõu § 5 punkt 1 on seotud asjaoluga, et 01.06.2025 jõustusid muudatused, mis on seotud hädaolukorra seaduse § 41 lõike 2 muutmisega.[181] Tolle eelnõuga muudeti hädaolukorra seaduse § 38 lõiget 1[4] ja § 41 lõiget 2 ning tehti ka muudatused nendes lõigetes sätestatud järelevalve pädevuse kohta: Riigi Infosüsteemi Ameti asemel teeb seda elutähtsa teenuse toimepidevust korraldav asutus või tema hädaolukorra seaduse § 37 lõike 5 alusel määratud asutus, sh finantsjärelevalve subjektide puhul Finantsinspektsioon. Kuna siin kommenteeritava eelnõu § 5 punktiga 3 on kavas tunnistada kehtetuks hädaolukorra seaduse § 41 lõige 1, tekiks selle muudatuseta olukord, kus kommenteeritava punktiga seotud õigusnormi järgi ei oleks ühemõtteliselt selge, et elutähtsa teenuse osutaja puhul on üleminekuaeg küberturvalisuse seaduse nõuete täitmiseks kuni viis aastat alates elutähtsa teenuse osutajaks määramisest arvates.
Eelnõu kohaselt on hädaolukorra seaduse § 38 lõike 1[3] punkti 3 sõnastus edaspidi järgmine (allajoonitud osa on lisanduv lauseosa):
3) täitma käesoleva seaduse § 37 lõike 2 alusel, §-s 41 ning muudes õigusaktides elutähtsa teenuse toimepidevuse tagamiseks sätestatud nõudeid, arvestades, et käesoleva seaduse §-s 41 ning küberturvalisuse seaduses sätestatud nõuete ja kohustuse täitmise tähtaeg ei oleks pikem kui viis

[181] Hädaolukorra seaduse muutmise seadus 589 SE: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/b4e53a2e-fb45-410c-8092-89be721e4146/.

aastat elutähtsa teenuse osutajaks määramisest arvates.

Eelnõu § 5 punkt 2 on seotud asjaoluga, et 01.06.2025 jõustus hädaolukorra seaduse § 38 lõike 1^4 muudatus, mis viitab sama seaduse § 41 lõikele 1. Kuna eelnõu § 5 punktiga 3 on kavas tunnistada kehtetuks hädaolukorra seaduse § 41 lõige 1, tekiks muudatuseta olukord, kus siin kommenteeritava punktiga muudetavas lõikes (hädaolukorra seaduse § 38 lõige 1^4) viidataks kehtetule õigusnormile. Muudatusega tagatakse muudetava sätte olemus ja sisu – erisus on see, et tehakse otseviide KüTSile.
Eelnõu kohaselt on hädaolukorra seaduse § 38 lõike 1^4 sõnastus edaspidi järgmine (allajoonitud osa on lisanduv tekstiosa, läbikriipsutatud tekst on asendatud tekstiosa):
(1^4) Enne käesoleva paragrahvi lõikes 1^2 nimetatud haldusakti andmist võib elutähtsa teenuse toimepidevust korraldav asutus või tema käesoleva seaduse § 37 lõike 5 alusel määratud asutus küsida Riigi Infosüsteemi Ametilt arvamust ~~§ 41 lõikes 1~~ küberturvalisuse seaduses sätestatud nõuete ja kohustuse täitmise tähtaja määramise kohta.

Eelnõu § 5 punkt 3 on seotud asjaoluga, et eelnõu kohaselt kehtetuks tunnistatavas lõikes (hädaolukorra seaduse § 41 lõige 1) on viide KüTSi §-dele 7 ja 8 (vt eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi). Seetõttu tunnistataksegi eelnõu kohaselt kõnealune paragrahv kehtetuks.

§ 6. Käibemaksuseaduse muudatused

Eelnõu §-s 6 kavandatav muudatus on tehniline. Kommenteeritava lõike kehtiv sõnastus on järgmine:
„(1^2) Kui isik võimaldab küberturvalisuse seaduse tähenduses internetipõhise kauplemiskoha kaudu ühendusevälisest riigist imporditud kaupade kaugmüüki saadetistes, mille tegelik väärtus ei ületa 150 eurot, loetakse, et internetipõhist kauplemiskohta omav isik on soetanud ja võõrandanud need kaubad ise. Tegelikku väärtust mõistetakse käesolevas seaduses komisjoni delegeeritud määruse (EL) 2015/2446, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) nr 952/2013 seoses liidu tolliseadustiku teatavaid sätteid täpsustavate üksikasjalike eeskirjadega (ELT L 343, 29.12.2015, lk 1–557), tähenduses.“
Selle lõike järgi on internetipõhine kauplemiskoht defineeritud KüTSis (konkreetsemalt KüTSi kehtiva redaktsiooni § 2 punktis 5), kuid eelnõu kohaselt muutub KüTSis viidatud termini määratlus ehk edaspidi on see „internetipõhine kauplemiskoht tarbijakaitseseaduse tähenduses“ (vt ka eelnõu KüTSi § 2 punkti 13 ja selle selgitust).
Kommenteeritavat paragrahvi muutmata tekiks olukord, kus käibemaksuseadus viitaks KüTSi terminile, mis omakorda viitaks tarbijakaitseseaduse terminile ehk tekiks kaks edasiviidet seadustele, see ei oleks aga kohane.

§ 7. Lennundusseaduse muudatused

Eelnõu § 7 punkt 1 on seotud järgmise, punktiga 2 kavandatava kehtetuks tunnistamisega: lennundusseaduse § 50^{25} viitab sama seaduse §-le 59^1. 477 SE seletuskirjas (lk 68–69) on selle sätte kohta selgitatud järgmist:
LennS-i § 50^{25} käsitleb võrgu- ja infosüsteemi turvalisuse tagamist. Lõige 1 sätestab, et maapealne teenindaja ja omakäitleja kohustuvad lennujaama haldaja poolt kasutatava võrgu- ja infosüsteemi turvalisuse tagamiseks täitma küberturvalisuse seaduse nõudeid ulatuses, milles maapealse teenindaja ja omakäitleja tegevus või tegevusetus mõjutab lennujaama haldaja võrgu- ja

infosüsteemi turvalisust. Tegemist ei ole otseselt [direktiivist 96/67/EÜ][182] tuleneva nõudega. Küberturvalisuse seaduse nõuete täitmine on vajalik lennujaama ohutuse ja tõrgeteta toimimise tagamiseks. EL-i lennundusohutuse alusmäärus[183] nõuab üksnes seda, et maapealse teeninduse teenuste osutajal peab olema juhtimissüsteem, mis tagab ohutusriskide juhtimise. EL-i lennundusohutuse alusmäärusest ei tulene maapealse teeninduse teenuse osutajale iseseisvat küberturvalisuse tagamise kohustust. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus, ja selle ülevõtmiseks vastu võetud küberturvalisuse seadus ei kohaldu maapealse teeninduse osutajatele. Samas ei ole lennuvälja käitajal võimalik lennujaama küberturvalisust tagada ilma, et küberturvalisuse tagamisel osaleksid ka lennujaamas tegutsevad maapealse teeninduse osutajad. Euroopa Komisjoni rakendusmäärus (EL) 2019/1583, millega muudetakse EL-i määrust 2015/1998 küberkaitsemeetmete osas, ei ole [tolle] eelnõu koostamise ajal veel kohaldatav (kohaldamistähtaeg on 31. detsembril 2021, lähtudes COVID-19 pandeemia tõttu määruse muutmisest[184]). Samas ei näe ka see määrus ette küberturvalisusega seotud kohustusi maapealse teeninduse osutajatele, vaid üksnes lennujaama käitajatele, lennuettevõtjatele ja riiklikus tsiviillennunduse julgestusprogrammis määratud üksustele. Eri maapealsete teenindajate ja omakäitlejate kokkupuuted võrgu- ja infosüsteemidega võivad olla väga erineva ulatusega, mistõttu on küberturvalisuse seaduse nõuete täitmine nõutud üksnes ulatuses, milles maapealse teenindaja ja omakäitleja tegevus või tegevusetus mõjutab lennujaama haldaja võrgu- ja infosüsteemi turvalisust. Lõige 2 sätestab, et maapealne teenindaja ja omakäitleja kohustuvad tegema lennujaama haldajaga koostööd [lennundusseaduse] §-s 59[1] sätestatud süsteemi turvalisuse tagamisel. Tegemist on kohustusega, mis vastab lennujaama haldaja §-st 59[1] tulenevale kohustusele tagada teenuse osutamiseks kasutatava võrgu- ja infosüsteemi turvalisus. [Lennundusseaduse] tasandil kehtestatud koostöökohustus ennetab võimalikke vaidlusi selle üle, kas lennuvälja käitajal on oma §-st 59[1] tulenevate kohustuste täitmiseks õigus nõuda, et maapealse teeninduse teenuste osutajad teeksid lennujaama käitajaga võrgu- ja infosüsteemi turvalisuse tagamiseks koostööd.

Selguse mõttes esitatakse lennundusseaduse §-s 50[25] mainitud terminid ja selgitused:

- lennundusseaduse § 50[17] lõike 1 kohaselt on maapealne teenindaja „isik, kes osutab kolmandale isikule üht või mitut liiki maapealse teeninduse teenust“, sama paragrahvi lõiked 2–4 täpsustavad lisatingimusi maapealsele teenindajale;
- lennundusseaduse § 50[15] kohaselt on maapealne teenindus „teenused, mis on loetletud nõukogu direktiivi 96/67/EÜ lisas“;
- lennundusseaduse § 50[16] lõike 1 kohaselt on omakäitlus „olukord, kus lennujaama kasutaja osutab otseselt endale üht või mitut liiki maapealse teeninduse teenust ega sõlmi kolmanda isikuga selliste teenuste osutamise lepingut“;
- lennundusseaduse § 50[16] lõike 2 kohaselt on omakäitleja „lennujaama kasutaja, kes tegeleb lennujaamas omakäitlusega“;
- lennundusseaduse § 50[4] lõike 1 kohaselt on lennujaama kasutaja „isik, kes õhu kaudu veab

[182] Nõukogu direktiiv 96/67/EÜ juurdepääsu kohta maapealse käitluse turule ühenduse lennujaamades: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A01996L0067-20240520.

[183] Euroopa Parlamendi ja nõukogu määrus (EL) 2018/1139, mis käsitleb tsiviillennunduse valdkonna ühisnorme ja millega luuakse Euroopa Liidu Lennundusohutusamet: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A02018R1139-20250525.

[184] Allviide 477 SE seletuskirjast: *Euroopa Komisjoni 30. juuni 2020 rakendusmäärus (EL) 2020/910, millega muudetakse rakendusmäärusi (EL) 2015/1998, (EL) 2019/103 ja (EL) 2019/1583 kolmandatest riikidest saabuva kauba ja posti suhtes julgestuskontrollimeetmeid kohaldavate lennuettevõtjate, käitajate ja üksuste määramise osas ning teatavate küberjulgeolekut, taustakontrolli, lõhkeaine avastamissüsteemi seadmete standardeid ja lõhkeaine jälgede avastamise seadmeid käsitlevate regulatiivsete nõuete osas COVID-19 pandeemia tõttu.*

reisijaid, posti või kaupa lennujaama või lennujaamast teise sihtkohta“.

Eelnõu kohaselt lisanduvad NIS2-direktiivi I lisa tõttu KüTSi (vt eelnõu KüTSi § 3 lõige 3 punkte 20–23) lennunduse valdkonnast järgmised üksused, kes peavad hakkama KüTSi nõudeid täitma (eeldusel, et on täidetud töötajate ja finantsnäitajate künnised):

- lennuettevõtja Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 300/2008 artikli 3 punkti 4 tähenduses, kes tegutseb kommertsvaldkonnas;
- lennujaama haldaja Euroopa Parlamendi ja nõukogu direktiivi 2009/12/EÜ artikli 2 punkti 1 tähenduses ning lennujaama abirajatiste käitaja;
- lennujaama haldaja lennundusseaduse tähenduses;
- lennujuhtimise teenust Euroopa Parlamendi ja nõukogu määruse (EÜ) nr 2024/2803 artikli 2 punkti 6 tähenduses osutav lennuliikluskorraldusettevõtja.

Lisaks eeltoodule on võimalus, et kui lennunduse valdkonnas määratakse üksus elutähtsa teenuse osutajaks hädaolukorra seaduse (tulevikus tsiviilkriisi ja riigikaitse seaduse) alusel, kohalduvad sellele üksusele samuti KüTSi nõuded (vt eelnõu KüTSi § 3 lõike 2 punkti 2).

Kui lennundusseaduse §-s 50^{25} viidatud maapealsed teenindajad ja omakäitlejad määratakse eelnõu kohaselt KüTSi teenuseosutajateks eelmainitud olukordade tõttu, peavad need üksused täitma KüTSi nõudeid kogu organisatsioonis. Isegi kui see ei ole seotud eelnõuga, ei reguleeri kõnealuse punkti kohaselt muudetav paragrahv olukorda, kus KüTSis nimetamata üksused peavad järgima kõiki KüTSis ja selle alusel sätestatud nõudeid. Sel juhul on muudetava sõnastusega paragrahvi puhul jätkuvalt tegemist sättega, mis säilitab maapealsete teenindajate ja omakäitlejate (lennundusseaduse tähenduses) kohustuse tagada turvameetmete kasutamine ulatuses, mis on seotud lennujaama haldaja võrgu- ja infosüsteemide turvalisusega, ning kohustuse teha lennujaama haldajaga koostööd. Tavapäraselt on taolised kohustused sätestatud lepingus, mis sõlmitakse KüTSi teenuseosutaja ning talle teenuseid osutava isiku vahel.

Kommenteeritava punktiga on kavas asendada kõnealuse paragrahvi esimeses lõikes tekstiosa „käesoleva seaduse §-s 59^{1} sätestatud“ sõnadega „kasutatava asjakohase“ ning muuta teises lõikes viidet ehk edaspidi viidata seal sama paragrahvi lõikele 1. Nende muudatustega luuakse seos nende lennujaama haldaja võrgu- ja infosüsteemidega, mida maapealne teenindaja ja omakäitleja kasutavad oma töös, ning sätestatakse nende üksuste ülesanne tagada küberturvalisuse nõuded ja teha koostööd lennujaama haldajaga. Seega on tegemist sama olukorra säilitamisega, mida on kirjeldatud 477 SE seletuskirjas.

Eeltoodu puhul tuleb arvestada ka võimalusega, et kui lennundusseaduses nimetatud maapealsetele teenindajatele ja omakäitlejatele kohalduvad praegu või tulevikus määrustes (EÜ) nr 300/2008 ja (EL) 2018/1139 ning nende määruste alusel vastu võetud asjakohastes delegeeritud õigusaktides (sh rakendusaktides) sätestatud turvanõuded, kohaldatakse nende üksuste teenustele viidatud määruste nõudeid, mistõttu ei kohaldata neile teenustele eelnõukohaseid KüTSi §-e 6, 6^{1} ja 7. Nende üksuste puhul ei kehti küberintsidentidest teavitamise nõude välistus (eelnõu KüTSi § 8), kuna sellele ei viita NIS2-direktiivi põhjendus 29 (vt ka eelnõu KüTSi § 1 lõike 4 selgitust).

Kuna Kliimaministeerium on algatamas lennundusseaduse revisjoni[185], on selle käigus võimalik analüüsida, kas ning milliseid küberturvalisuse nõudeid tuleks maapealsele teenindajale ja omakäitlejale kohaldada, sh mil määral tuleks eelnõuga lennundusseaduse § 50^{25} sõnastust säilitada või seda muuta.

Eelnõu § 7 punktiga 2 on kavandatud tunnistada kehtetuks lennundusseaduse § 59^{1}, § 60^{1} lõige 5 ja § 60^{56} lõige 3.

[185] Kliimaministeeriumi 25.06.2025. a kiri nr 19-3/25/4-6: https://adr.envir.ee/et/document.html?id=b3b06147-d39c-45ed-bf20-7ecad8eaeeb5.

Eelnõu kohaselt kehtetuks tunnistatavas paragrahvis (**lennundusseaduse § 59[1]**) on viide KüTSi §-dele 7 ja 8 (vt eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Lennundusseaduse § 60[1] lõige 5 kavandatakse tunnistada kehtetuks, kuna sama seaduse § 59[1] kehtetuks tunnistamisel tunnistatakse kehtetuks ristviide siin kommenteeritava punktiga eelnõu kohaselt kehtetuks tunnistatav lõige (lennundusseaduse § 60[1] lõige 5) sätestab eelmainitud lõigetes sätestatud nõuete täitmise üle järelevalve tegemise aspektid. Kui muudatust ei tehtaks, oleks nimetatud seaduses jätkuvalt nõue, et Riigi Infosüsteemi Amet teeb KüTSi alusel järelevalvet kommenteeritavas õigusnormis viidatud nõuete täitmise üle (vt ka eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Eelnõuga kavatsetakse kehtetuks tunnistada **lennundusseaduse § 60[56] lõige 3**, kuna see sätestab, et Riigi Infosüsteemi Amet on kohtuväline menetleja sama seaduse §-s 60[44] sätestatud väärteo (elektroonilise turvalisuse nõuete rikkumise) korral. Kuna viidatud väärteokoosseisu sisaldav säte on juba varem tunnistatud kehtetuks ja selle põhisisu on eelnõu kohaselt edaspidi KüTSis, tuleb ka menetluspädevuse määramisega seotud õigusnorm kehtetuks tunnistada.

§ 8. Raudteeseaduse muudatused

Eelnõu § 8 punktiga 1 kavatsetakse tunnistada kehtetuks raudteeseaduse § 8 ning § 143 lõike 1 punkt 6 ja lõige 8.
Raudteeseaduse § 8 tunnistatakse eelnõu kohaselt kehtetuks, kuna selles on viide KüTSi §-dele 7 ja 8 (vt eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).
Kommenteeritava punktiga on kavas kehtetuks tunnistada **raudteeseaduse § 143 lõike 1 punkt 6**, kuna eelnõuga on kavas tunnistada kehtetuks ristviide KüTSi §-dele 7 ja 8. Raudteeseaduse § 143 lõike 1 punkt 6 sätestab Riigi Infosüsteemi Ameti pädevuse teha riiklikku järelevalvet raudteeseaduse ja selle alusel kehtestatud õigusaktide nõuete täitmise üle. Kui seda muudatust ei tehtaks, oleks raudteeseaduses jätkuvalt nõue, et Riigi Infosüsteemi Amet teeb järelevalvet raudteeseaduse üle (vt ka eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).
Kommenteeritava punktiga on kavas kehtetuks tunnistada **raudteeseaduse § 143 lõige 8**, kuna eelnõuga on kavas tunnistada kehtetuks ristviide KüTSi §-dele 7 ja 8. Raudteeseaduse § 143 lõige 8 sätestab eelmainitud lõigetes sätestatud nõuete täitmise üle järelevalve tegemise aspektid. Siin on ka seos raudteeseaduse § 143 lõike 1 punkti 6 kehtetuks tunnistamisega. Kui siin kommenteeritava punktiga kavandatud muudatust ei tehtaks, oleks raudteeseaduses jätkuvalt nõue, et Riigi Infosüsteemi Amet teeb KüTSi alusel järelevalvet kommenteeritavas õigusnormis viidatud nõuete täitmise üle (vt ka eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Eelnõu § 8 punkt 2 on seotud ülejäänud §-s 8 kavandatavate muudatustega. Kuna eelnõu kohaselt eemaldatakse raudteeseadusest õigusnormid, mille järgi teeb raudteeseaduses oleva ühe nõude täitmise üle järelevalvet ka Riigi Infosüsteemi Amet, puudub vajadus säilitada samas seaduses ka nõue, et Riigi Infosüsteemi Amet on kohustatud tagama talle riikliku järelevalve tegemisel teatavaks saanud äri- ja tehnikaalase teabe konfidentsiaalsuse, kui seadus ei näe ette selle teabe avaldamist. See nõue kohaldub edaspidi eelnõukohase KüTSi § 12 lõikega 5 (vt selle sätte selgitusi).

§ 9. Sadamaseaduse muudatused

Eelnõuga kavatsetakse tunnistada kehtetuks **sadamaseaduse § 13 lõige 4,** kuna selles on viide KüTSi §-dele 7 ja 8 (vt eelnõu §-ga 3 Eesti Rahvusringhäälingu seaduses tehtava muudatuse

selgitusi). **Sadamaseaduse § 42 lõige 5** on kavas tunnistada kehtetuks, kuna eelnõuga on kavas tunnistada kehtetuks sama seaduse § 13 lõige 4 ehk ristviide KüTSi §-dele 7 ja 8. Sadamaseaduse § 42 lõige 5 sätestab eelmainitud lõigetes sätestatud nõuete täitmise üle järelevalve tegemise aspektid. Kui muudatust ei tehtaks, oleks sadamaseaduses jätkuvalt nõue, et Riigi Infosüsteemi Amet teeb KüTSi alusel järelevalvet kommenteeritavas õigusnormis viidatud nõuete täitmise üle (vt ka eelnõu § 3 punktiga 1 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

§ 10. Tervishoiuteenuste korraldamise seaduse muudatused

Eelnõuga kavandatakse tunnistada kehtetuks **tervishoiuteenuste korraldamise seaduse § 10 lõige 2, § 17 lõige 1^2 ja § 22 lõige 4^2**, kuna nendes kõigis on viide KüTSi §-dele 7 ja 8 (vt eelnõu § 3 punktiga 1 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

Tervishoiuteenuste korraldamise seaduse § 60 lõige 2 sätestab eelmainitud lõigetes sätestatud nõuete täitmise üle järelevalve tegemise aspektid, kuid kuna need sätted kavatsetakse tunnistada kehtetuks, siis tuleb kehtetuks tunnistada ka selle seaduse § 60 lõige 2. Kui muudatust ei tehtaks, oleks nimetatud seaduses jätkuvalt nõue, et Riigi Infosüsteemi Amet teeb KüTSi alusel järelevalvet kommenteeritavas õigusnormis viidatud nõuete täitmise üle (vt ka eelnõu §-ga 3 1 Eesti Rahvusringhäälingu seaduses tehtava muudatuse selgitusi).

§ 11. Seaduse jõustumine

Eelnõu § 11 näeb ette seaduse jõustumise.

NIS2-direktiivi artikli 41 (ülevõtmine) lõikes 1 on ette nähtud:

„1. Liikmesriigid võtavad [NIS2-direktiivi] järgimiseks vajalikud meetmed vastu ja avaldavad need hiljemalt 17. oktoobriks 2024. Liikmesriigid teatavad nendest viivitamata [Euroopa Komisjonile].

Nad kohaldavad kõnealuseid meetmeid alates 18. oktoobrist 2024.“

Kuna nimetatud kuupäev on möödunud, siis saaks seaduse jõustumise määrata ka üldises korras. Samas leiavad eelnõu koostajad, et õiguskindluse ja ettenägevuse tagamiseks on kasulikum määrata jõustumise konkreetne kuupäev, mistõttu on jõustumise kuupäevaks määratud 2026. aasta 1. jaanuar. See jätab piisavalt aega, et ette valmistada Vabariigi Valitsuse ja ministrite määruste muudatused.

Eelnõu menetluse käigus saab hinnata, kas seda kuupäeva on vaja muuta hilisemaks.

3.2. Eelnõu põhiseaduspärasuse analüüs

Seletuskirja selles alapeatükis ei analüüsita eelnõuga lisanduvaid õigusnorme, mis on seotud Euroopa Liidu õiguse ülevõtmisega, vaid KüTSi § 3^1 lisatava lõike 3 vastavust Eesti Vabariigi põhiseadusele. Lõikes 3 sätestatakse juurdepääsupiirangu alus tunnistada teenuseosutajate ja domeeninimede registreerimise teenuse osutajate nimekiri asutusesiseseks kasutamiseks mõeldud teabeks. Lõike selgituses on kirjeldatud kavandatava juurdepääsupiirangu aluse seost ametlikele dokumentidele juurdepääsu Euroopa Nõukogu konventsiooni artikli 3 lõike 1 esimese tekstilõigu punktides a („tagada riigi julgeolek ja riigikaitse ning kaitsta rahvusvahelisi suhteid“) ja b („tagada avalik julgeolek“) sätestatud võimalustega piirata juurdepääsu ametlikele dokumentidele.

Põhiseaduse § 44 esimene, teine ja neljas tekstilõik sätestavad:

„Igaühel on õigus vabalt saada üldiseks kasutamiseks levitatavat informatsiooni.

Kõik riigiasutused, kohalikud omavalitsused ja nende ametiisikud on kohustatud seaduses sätestatud korras andma Eesti kodanikule tema nõudel informatsiooni oma tegevuse kohta, välja arvatud andmed, mille väljaandmine on seadusega keelatud, ja eranditult asutusesiseseks kasutamiseks mõeldud andmed.

[...]

Kui seadus ei sätesta teisiti, siis on käesoleva paragrahvi lõigetes kaks ja kolm nimetatud õigused võrdselt Eesti kodanikuga ka Eestis viibival välisriigi kodanikul ja kodakondsuseta isikul.“
Põhiseaduse kommenteeritud väljaandes[186] on esimese tekstilõigu kohta selgitatud p-s 17 järgmist:
„17. PS § 44 lg-s 1 sätestatud põhiõigus on reservatsioonita põhiõigus ja seega peavad selle põhiõiguse piirangud olema õigustatavad teiste põhiseaduslike väärtustega või teiste põhiõigustega (vt eesmärgi konkreetsusega seoses RKÜKo 30.06.2017, 3-3-2-1-16, p-d 22–24; RKHKo 15.12.2017, 3-13-2425/53, p-d 21–22). Soorituspõhiõiguse kontrolliskeemi kohta vt II ptk sissejuhatuse komm-d.“
Põhiseaduse kommenteeritud väljaandes on teise tekstilõigu kohta selgitatud p-s 30 järgmist:
„30. Õigus saada infot avaliku võimu organite ja ametiisikute tegevuse kohta ei ole piiramatu. Juurdepääs ei laiene PS § 44 lg 2 kohaselt andmetele, mille väljaandmine on seadusega keelatud, ja eranditult asutusesiseseks kasutamiseks mõeldud andmetele. Seega on tegemist lihtsa seadusereservatsiooniga põhiõigusega, mis võimaldab käsitletavat õigust küllaltki ulatuslikult piirata – eeldusel, et seadusega kehtestatud piirangul on legitiimne eesmärk ning piirang on proportsionaalne. Andmete seadusega väljaandmise piirangud tulenevad näiteks RSVS-st, IKS-st, AvTS-st, ArhS-st, RStS-st, ATS-st jne. Väärtused, mis osutuvad sellisel juhul kaalukamateks kui isikute õigus informatsioonile, on näiteks Eesti Vabariigi julgeolek, isikuandmete kaitse jne.“
Eelmainitud põhiõigust sisustavad ennekõike avaliku teabe seaduse õigusnormid, kuid ka muudes eriseadustes võib olla sätestatud juurdepääsupiirangu aluseid. Samas ei ole kehtivas õiguses juurdepääsupiirangu alust. Eelnõu tulemusena lisandub KüTSi § 3^1 lõikega 3 sellekohane juurdepääsupiirangu alus, piirates igaühe õigust saada avalike ülesannete täitmise käigus saadud või loodud teavet. Kuna KüTSi § 3^1 lisatava lõike 2 kohaselt peab Riigi Infosüsteemi Amet koostama teenuseosutajatest ja domeeninimede registreerimise teenuse osutajatest nimekirja, siis on tegemist avaliku ülesande täitmisega. Selle nimekirja koostamise näeb ette NIS2-direktiiv (vt artikli 3 lõiget 2), kuid direktiiv ei sätesta, kuivõrd avalik on kõnealune nimekiri või kuidas seda tuleks kaitsta (st piirata sellele juurdepääsu).

Juurdepääsupiirangu kehtestamise eesmärk on tagada teenuseosutajate ja domeeninimede registreerimise teenuse osutajate nimekirja kui tundliku andmekogumi konfidentsiaalsus. Kõnealune nimekiri sisaldab osaliselt andmeid, mis on juurdepääsupiiranguga ka mõne muu õigusakti alusel (tsiviiltoetuse registri andmed). Seda nimekirja tuleb käsitada asutusesiseseks kasutamiseks mõeldud teabena, et kaitsta nimekirjas olevat koondteavet ning ka nimekirjas olevaid üksusi. Näiteks selleks, et pahatahtlikel isikutel oleks keerulisem mõjutada ühiskonna toimimise seisukohast vajalike üksuste kasutatavaid võrgu- ja infosüsteeme ning neid teenuseid, mis neid süsteeme kasutavad. See omakorda aitab tagada laiapindse riigikaitse eesmärke[187], sh ühiskonna toimimist.
Juurdepääsupiirangu aluse sätestamisega tekib selgus, et nimekirja kui kogumi puhul on tegemist teabega, mida tuleb kaitsta, kasutades asjakohaseid turvameetmeid. Piirangut tekitamata on võimalik seda teavet kaitsta, kasutades asjakohaseid turvameetmeid, kuid puudub võimalus keelduda selle (terve) nimekirja väljastamisest teabenõude korras. Seetõttu on juurdepääsupiirang sobiv ning vajalik püstitatud eesmärgi saavutamiseks. Riive on ka mõõdukas, kuna see ei riiva muid põhiõigusi ning võimaldab saavutada soovitud eesmärki.
Juurdepääsupiirang ei tähenda, et õigustatud isikul ei oleks võimalik teadmisvajaduse korral saada selle nimekirja kohta või nimekirjast endast soovitud teavet, näiteks kui nimekirja kantud üksus (KüTSi teenuseosutaja või domeeninimede registreerimise teenuse osutaja) soovib teada, milliseid andmeid on tema kohta sellesse nimekirja kantud. Sel juhul on võimalik teha asjakohane väljavõte

[186] https://pohiseadus.ee/sisu/3515/paragrahv_44
[187] https://kaitseministeerium.ee/et/eesmargid-tegevused/laiapindne-riigikaitse

ning väljastada teave avaliku teabe seaduse § 38 lõikes 4 sätestatud korras. Nimetatud lõike järgi võib asutuse juht „otsustada asutuseväliste isikute juurdepääsu võimaldamise asutusesiseseks tunnistatud teabele, kui see ei kahjusta riigi või omavalitsusüksuse huve“.
Arvestades eeltoodut on kavandatava juurdepääsupiirangu aluse loomine kooskõlas põhiseadusega.

4. Eelnõu terminoloogia

Mõistete „üksus“, „teenuseosutaja“, „ülioluline üksus“, „oluline üksus“ ja „domeeninimede registreerimise teenuse osutaja“ olemust ning omavahelist suhestumist selgitab joonis 2 (vt eelnõu KüTSi § 3 selgitust). Allpool on selgitatud eelnõukohase KüTSi §-des 2, 3 ja 8 kasutatavaid mõisteid.

4.1. Andmekeskusteenus – teenus, mis seisneb selliste struktuuride või struktuurirühmade pakkumises, mis on ette nähtud andmete talletamiseks, töötlemiseks ja edastamiseks kasutatavate infotehnoloogia- ja võrguseadmete keskseks majutamiseks, omavahel sidumiseks ja käitamiseks, sealhulgas kõiki elektrivarustuse ja majutuskeskkonna kontrolliga seotud vahendeid ja taristuid.

4.2. Digitaalse teenuse osutaja – üksuse üldnimetus, mille puhul on mõeldud domeeninimede süsteemi teenuse osutajat, tippdomeeninimede registrit, domeeninimede registreerimise teenuse osutajat, pilvandmetöötlusteenuse osutajat, andmekeskusteenuse osutajat, sisulevivõrguteenuse osutajat, haldusteenuse osutajat, infoturbeteenuse osutajat, internetipõhise kauplemiskoha pidajat, veebipõhise otsingumootori või sotsiaalmeedia platvormi pakkujat.

4.3. Digitaalse teenuse osutaja esindaja – Euroopa Liidus asuv füüsiline või juriidiline isik, kes on määratud tegutsema väljaspool Euroopa Liitu asuva digitaalse teenuse osutaja nimel ja kelle poole võib Riigi Infosüsteemi Amet pöörduda seoses digitaalse teenuse osutaja kohustustega.

4.4. Domeeninimede registreerimise teenuse osutaja – tippdomeeninimede registri pidaja või selle registri pidaja nimel tegutsev isik, näiteks registreerimisega seotud privaatsusteenuse või proksiteenuse osutaja või edasimüüja.

4.5. Domeeninimede süsteem – hierarhiline ja hajus nimesüsteem, mis võimaldab tuvastada internetiteenuseid ja -ressursse, tehes lõppkasutaja seadmetel võimalikuks kasutada internetimarsruutimise ja ühenduvuse teenuseid, et jõuda nende teenuste ja ressurssideni.

4.6. Domeeninimede süsteemi teenuse osutaja – üksus, kes osutab interneti lõppkasutajatele üldsusele kättesaadavat domeeninime rekursiivse teisendamise teenust või kes osutab kolmandatele isikutele kasutamiseks mõeldud domeeninime autoriteetse teisendamise teenust, välja arvatud juurnimeserverid teenust.

4.7. Esmane teade – teade, mille teenuseosutaja (välja arvatud julgeolekuasutus) esitab Riigi Infosüsteemi Ametile viivitamata, kuid hiljemalt 24 tundi pärast sellisest küberintsidendist teada saamist:
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.
Selle teavituse sisu on sätestatud eelnõus KüTSi § 8 lõikes 4^1.

4.8. Haldusteenuse osutaja – üksus, kes osutab teenuseid, mis on seotud IKT-toodete, võrkude, taristu, rakenduste või muude võrgu- ja infosüsteemide paigaldamise, haldamise, käitamise või hooldamisega toe või aktiivse haldamise kaudu kas kliendi ruumides või kaugjuhtimise teel.

4.9. IKT-protsess – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 14 määratletud IKT-protsess. Selle mõiste sisu: tegevused, mille käigus projekteeritakse või töötatakse välja IKT-toode või -teenus, seda tarnitakse või hallatakse.

4.10. IKT-teenus – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 13 määratletud IKT-teenus. Selle mõiste sisu: teenus, mis koosneb täielikult või peamiselt võrgu- ja infosüsteemide kaudu teabe edastamisest, säilitamisest, väljavõtmisest või töötlemisest.

4.11. IKT-toode – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 12 määratletud IKT-toode. Selle mõiste sisu: võrgu- või infosüsteemi element või elementide rühm.

4.12. Infoturbeteenuse osutaja – haldusteenuse osutaja, kes viib ellu riskide juhtimist või pakub selleks tuge.

4.13. Interneti sõlmpunkt – ühenduspunkt, mis võimaldab mitme sõltumatu võrgu omavahelist ühendamist ja internetiliiklust nende vahel; see võimaldab üksnes autonoomsete süsteemide omavahelist ühendamist ega nõua, et internetiliiklus kahe osaleva autonoomse süsteemi vahel toimuks mõne kolmanda autonoomse süsteemi kaudu, ei muuda sellist liiklust ega sekku sellesse mingil muul viisil.

4.14. Internetipõhine kauplemiskoht – internetipõhine kauplemiskoht tarbijakaitseseaduse tähenduses.

4.15. Intsidenditeade – teade, mille teenuseosutaja (välja arvatud julgeolekuasutus) edastab Riigi Infosüsteemi Ametile viivitamata, kuid hiljemalt 72 tundi pärast olulise mõjuga küberintsidendist teada saamist, et ajakohastada esmast teavet. Erandina reeglist peab usaldusteenuse osutaja teate edastama hiljemalt 24 tundi pärast olulise mõjuga küberintsidendist teada saamist ning see peab sisaldama teavet, mis on sätestatud eelnõus KüTSi § 8 lõikes 4^1. Julgeolekuasutus esitab teate asjakohasele julgeolekuasutusele.

4.16. Keskvalitsuse avaliku halduse üksus – Eesti Pank, kohtuasutus, riigi valimisteenistus, Riigikogu Kantselei, Riigikontroll, Vabariigi Presidendi Kantselei, valitsusasutus, valitsusasutuse hallatav riigiasutus ja Õiguskantsleri Kantselei.

4.17. Kohaliku omavalitsuse avaliku halduse üksus – kohaliku omavalitsuse üksus, valla või linna ametiasutus, valla või linna ametiasutuse hallatav asutus, osavald, linnaosa, osavalla või linnaosa ametiasutus, osavalla või linnaosa ametiasutuse hallatav asutus ning kohaliku omavalitsuse üksuste ühisamet ja –asutus.

4.18. Kvalifitseeritud usaldusteenuse osutaja – Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 3 punktis 20 määratletud kvalifitseeritud usaldusteenuse osutaja. Selle mõiste sisu: usaldusteenuse osutaja, kes osutab üht või mitut kvalifitseeritud usaldusteenust ning kellele järelevalveasutus on andnud kvalifitseeritud staatuse.

4.19. Küberintsidendi käsitlemine – toimingud ja menetlused, mille eesmärk on küberintsidenti ennetada, tuvastada, analüüsida, ohjata või lahendada ja sellest taastuda.

4.20. Küberintsident – võrgu- ja infosüsteemis toimuv sündmus, mis ohustab või kahjustab võrgu- ja infosüsteemi turvalisust.

4.21. Küberintsidentide käsitlemise üksus – ekspertide grupp, kelle ülesanne on teha küberintsidendi käsitlemist toetavad toimingud.

4.22. Küberoht – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 8 määratletud küberoht. Selle mõiste sisu: võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada.

4.23. Küberturvalisus – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 2 punktis 1 määratletud küberturvalisus. Selle mõiste sisu: tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest.

4.24. Lõppraport – teade, mille teenuseosutaja (välja arvatud julgeolekuasutus) edastab Riigi Infosüsteemi Ametile ühe kuu jooksul pärast intsidenditeate esitamist, mis sisaldab teavet küberintsidendi tekkepõhjuste, selle lahendamiseks kulunud aja ja rakendatud abinõude ning küberintsidendi mõju, sealhulgas asjakohasel juhul piiriülese mõju kohta. Kui olulise mõjuga küberintsidenti ei ole lõppraporti esitamise ajaks veel lahendatud, käsitatakse esitatud lõppraportit vahearuandena ja teenuseosutaja esitab uue lõppraporti ühe kuu jooksul pärast olulise mõjuga küberintsidendi lahendamist. Julgeolekuasutus esitab teate asjakohasele julgeolekuasutusele.

4.25. Oluline küberoht – küberoht, mille tehniliste näitajate põhjal võib eeldada, et sellel võib olla suur mõju üksuse võrgu- ja infosüsteemile või üksuse võrgu- ja infosüsteemi kasutajatele, tekitades märkimisväärset varalist või mittevaralist kahju.

4.26. Oluline üksus – eelnõus KüTSi § 3 lisatavates lõigetes 4 ja 5 loetletud üksused (näiteks Arenguseire Keskus, kohaliku omavalitsuse üksuste liit, Riigimetsa Majandamise Keskus).

4.27. Pilvandmetöötlusteenus – infoühiskonna teenus, mis võimaldab nõude põhjal hallata skaleeritavaid ja paindlikke jagatavaid andmetöötlusressursse ning ulatuslikku kaugpääsu neile, sealhulgas juhul, kui need ressursid paiknevad hajutatult eri kohtades.

4.28. Risk – küberintsidendist tingitud kahju või häire tekke võimalus, mis väljendub kahju või häire ulatuse ja küberintsidendi esinemise tõenäosuse kombineeritud näitajana.

4.29. Sisulevivõrk – geograafiliselt hajutatud serverite võrk, mille eesmärk on tagada digisisu ja infoühiskonna teenuste laialdane kättesaadavus, juurdepääsetavus või kiire edastamine internetikasutajatele sisu- ja teenusepakkujate nimel.

4.30. Sotsiaalmeediaplatvorm – platvorm, mis võimaldab lõppkasutajatel vastastikku ühendust pidada, sisu jagada, teavet otsida ja suhelda mitme seadme kaudu, eelkõige vestluste, postituste, videote ja soovituste vormis.

4.31. Teadusasutus – üksus, kelle peamine tegevus on teha rakendusuuringuid või tootearendust eesmärgiga kasutada selliste uuringute või arenduste tulemusi ärilistel eesmärkidel, kuid kes ei ole haridusasutus.

4.32. Tippdomeeninimede register – üksus, kelle vastutusel on Eesti maatunnusega seotud tippdomeen ning kes vastutab selle tippdomeeni haldamise eest, sealhulgas tippdomeeni alamdomeeninimede registreerimise eest ja tippdomeeni tehnilise toimimise eest, sealhulgas nimeserverite käitamise ja andmebaaside hooldamise eest ning tippdomeeni tsoonifailide jaotamise eest nimeserverite vahel, olenemata sellest, kas mõne neist toimingutest teeb üksus ise või ostetakse mõni toiming sisse, kuid välja arvatud juhul, kui register kasutab tippdomeeninimesid ainult enda tarbeks.

4.33. Turvahaavatavus – IKT-toote või IKT-teenuse nõrkus, vastuvõtlikkus või viga, mida küberoht võib ära kasutada.

4.34. Turvameetmed – rakendatavad organisatsioonilised, füüsilised ja infotehnilised toimingud või vahendid andmete ning võrgu- -ja infosüsteemide turvalisuse saavutamiseks ning säilitamiseks.

4.35. Ulatuslik küberintsident – küberintsident, mille põhjustatud häired on niivõrd laialdased, et üks Euroopa Liidu liikmesriik ei suuda nendega toime tulla, või millel on märkimisväärne mõju vähemalt kahele Euroopa Liidu liikmesriigile.

4.36. Usaldusteenuse osutaja – Euroopa Parlamendi ja nõukogu määruse (EL) nr 910/2014 artikli 3 punktis 19 määratletud usaldusteenuse osutaja. Selle mõiste sisu: füüsiline või juriidiline isik, kes osutab üht või mitut usaldusteenust kas kvalifitseeritud või kvalifitseerimata usaldusteenuse osutajana.

4.37. Vahearuanne – teade, mille Riigi Infosüsteemi Ameti taotlusel teenuseosutaja (välja arvatud julgeolekuasutus) edastab ametile enne lõppraporti esitamist, et anda ülevaade küberintsidendi lahendamise seisu kohta. Vahearuandes esitatakse eelnõus KüTSi § 8 lõikes 4^1 sätestatud andmed ja asjakohasel juhul ka ameti taotletud lisateave. Julgeolekuasutus esitab teate asjakohasele julgeolekuasutusele.

4.38. Veebipõhine otsingumootor – Euroopa Parlamendi ja nõukogu määruse (EL) 2019/1150 artikli 2 punktis 5 määratletud veebipõhine otsingumootor. Selle mõiste sisu: digitaalne teenus, mis võimaldab kasutajatel sisestada päringuid, et teha otsinguid üldjuhul kõikidel veebisaitidel või teatavas keeles kõikidel veebisaitidel mis tahes teemal võtmesõna, häälkäskluse, fraasi või muu sisendi vormis tehtud päringu alusel, ning saadab vastuseks mis tahes vormingus tulemused, kust võib leida teavet taotletud sisu kohta.

4.39. Võrgu- ja infosüsteem – elektroonilise side võrk elektroonilise side seaduse § 2 punkti 8 tähenduses, seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt digitaalsete andmete automaatne töötlemine, või digitaalsed andmed, mida eelnimetatud komponendid nende töö, kasutamise, kaitsmise või hooldamise jaoks salvestavad, töötlevad, saavad päringuga või edastavad.

4.40. Võrgu- ja infosüsteemi turvalisus – süsteemi võime osutada vastupanu mis tahes sündmusele, mis ohustab süsteemis töödeldavate andmete või süsteemi kaudu osutatavate või

juurdepääsetavate teenuste käideldavust, autentsust, terviklust ja konfidentsiaalsust.

4.41. Üksus – juriidiline isik, kes on asutatud ja keda tunnustatakse tema tegevuskohajärgse riigi õiguse kohaselt ning kellel võivad olla õigused ja kohustused, või füüsiline isik.

4.42. Üldkasutatav elektroonilise side teenus – üldkasutatav elektroonilise side teenus elektroonilise side seaduse tähenduses.

4.43. Üldkasutatav elektroonilise side võrk – üldkasutatav elektroonilise side võrk elektroonilise side seaduse tähenduses.

4.44. Ülioluline üksus – KüTSi § 3 lõigetes 1 ja 2 loetletud üksused (näiteks elutähtsa teenuse osutaja, kvalifitseeritud usaldusteenuse osutaja, tippdomeeninimede registri pidaja, domeeninimede süsteemi teenuse osutaja, keskvalitsuse avaliku halduse üksus, kohaliku omavalitsuse avaliku halduse üksus).

5. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu järgib õigusnormide loomisel järgmisi ELi õigusakte::

1) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152);
2) Euroopa Komisjoni delegeeritud määrus (EL) 2024/1366, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta (ELT L, 24.5.2024, lk 1–44).

Eelnõu vastab Euroopa Liidu õigusele, nendele aktidele vastavuse tabel on seletuskirja lisas 1. Kehtiva õiguse suhtes (mida nt ei muudeta) kohaldub ka NIS2-direktiivi artikkel 5, mis näeb ette järgmist: „[NIS2-direktiiv] ei takista liikmesriike tarbijate kaitseks vastu võtmast või kehtima jätmast sätteid, millega tagatakse kõrgem küberturvalisuse tase, tingimusel et sellised sätted on kooskõlas liikmesriikide kohustustega, mis on sätestatud liidu õiguses.“ Iga eelnõukohase seadusega tehtava muudatuse juures on võrreldud muudetava sätte vastavust Euroopa Liidu õigusele, sh tuuakse vajaduse korral välja ka võimalikud sõnastusalternatiivid.

6. Seaduse mõjud

Seadusega võetakse Eesti õigusesse üle NIS2-direktiiv ning sätestatakse õigusnormid, mis on vajalikud delegeeritud määruse (EL) 2024/1366 rakendamiseks.

Delegeeritud määruse (EL) 2024/1366 ettevalmistamisel peeti avalik konsultatsioon, samuti eelkonsultatsioonid.[188] Nende sisu seletuskirjas ei analüüsita ega korrata. Delegeeritud määruse (EL) 2024/1366 kohaldamisalasse kuuluvaid subjekte uuesti KüTSis ei korrata, kuna tegemist on otsekohalduva määrusega. Samuti ei analüüsita nende subjektidega seotud nõuete ja kohustuste mõjusid.

NIS2-direktiivi ettevalmistamisel hinnati eraldi ka selle mõjusid kogu liidule ning esitati näitajad, kuidas hinnatakse hiljem selle edusamme.[189] Nende dokumentide kuupäevad on 16.12.2020. NIS2-

[188] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13101-ELi-elektrivarustus-kuberturvalisust-kasitlevad-sektoripohised-normid-vorgueeskiri-_et ja https://www.entsoe.eu/network_codes/nccs/.

[189] Kättesaadav https://eur-lex.europa.eu/legal-content/ET/HIS/?uri=uriserv:OJ.L_.2022.333.01.0080.01.EST;

direktiivi algatuse[190] 7. lisa (finantsselgitus – ametid) punktis 1.4.3 on selgitatud:
1.4.3. Oodatavad tulemused ja mõju
Ettepanek peaks tooma märkimisväärset kasu: hinnanguliselt võib see vähendada küberturvalisuse intsidentidega seotud kulusid 11,3 miljardi euro võrra. Küberturvalisuse raamistikuga laiendataks sektoripõhist kohaldamisala märkimisväärselt, kuid lisaks mainitud eelistele kaasneb küberturvalisuse nõuetega koormus (eelkõige järelevalve aspektist), mida tasakaalustataks nii uute hõlmatud üksuste kui ka pädevate asutuste jaoks. Seda tänu asjaolule, et uue küberturvalisuse raamistikuga kasutataks kahetasandilist lähenemisviisi, keskendudes suurtele ja võtmetähtsusega üksustele ning rakendades diferentseeritud järelevalvekorda, mis võimaldab suure hulga üksuste, nimelt olulisena (mitte elutähtsana[191]) käsitatavate üksuste suhtes kohaldada järelevalve järelkontrollimeetmeid.
Kokkuvõttes saavutataks selle ettepaneku toel soodsad kompromissid ja tõhusad sünergiad ning selle toetataval poliitikavariandil oleks suurim potentsiaal tagada võtmetähtsusega üksuste kübervastupidavusvõime kõrgem ja ühtlasem tase kogu liidu ulatuses, mis lõppkokkuvõttes tähendaks nii ettevõtjate kui ka ühiskonna jaoks kulude kokkuhoidu.
Ettepaneku elluviimine tähendaks asjaomaste liikmesriikide ametiasutustele ka teatavaid nõuete järgimise ja täitmise tagamisega seotud kulusid (hinnanguliselt suureneb ressursivajadus kokku ligikaudu 20–30 %). Samas tooks uus raamistik märkimisväärset kasu ka selle kaudu, et tagaks olulistest ettevõtjatest parema ülevaate ja nendega tõhusama suhtlemise, tulemuslikuma piiriülese operatiivkoostöö ning vastastikuse abistamise ja vastastikuse hindamise mehhanismid. Selle tulemusena tõuseks liikmesriikide küberturvalisuse alase suutlikkuse üldine tase.
Küberturvalisuse raamistiku kohaldamisalasse hõlmatavad ettevõtjad peaksid esimestel aastatel pärast küberturvalisuse raamistiku jõustumist suurendama oma IKT-turbega seotud kulutusi maksimaalselt 22 % võrra (need ettevõtjad, kes juba kuuluvad [küberturvalisuse direktiivi (EL) 2016/1148] kohaldamisalasse, 12 % võrra). IKT-turbega seotud kulutuste keskmine suurenemine tooks samas kaasa proportsionaalse investeeringukasu, eelkõige tänu küberturvalisuse intsidentidega seotud kulude märkimisväärsele vähenemisele (hinnanguliselt 118 miljardit eurot kümne aasta jooksul).
Väike- ja mikroettevõtjad jäetaks küberturvalisuse raamistiku kohaldamisalast välja. Keskmise suurusega ettevõtjate IKT-turbega seotud kulutused esimestel aastatel pärast uue küberturvalisuse raamistiku kasutuselevõttu eelduste kohaselt suurenevad. Samas soodustaks nende üksuste turvanõuete taseme tõstmine ka nende küberturvalisuse alase suutlikkuse suurenemist ja aitaks tõhustada nende IKT-alast riskijuhtimist.
Oodatav mõju liikmesriikide eelarvetele ja haldusasutustele: lühikese ja keskpika perspektiivi prognoosi kohaselt suureneb ressursivajadus hinnanguliselt ligikaudu 20–30 %.
Muud olulist negatiivset mõju ei ole ette näha. Ettepaneku elluviimine peaks suurendama küberturvalisuse alast suutlikkust ning vähendama seega oluliselt intsidentide, sealhulgas andmetega seotud rikkumiste arvu ja nende raskusastet. Samuti avaldab see tõenäoliselt positiivset mõju kõikide küberturvalisuse raamistiku kohaldamisalasse kuuluvate üksuste jaoks võrdsete tingimuste tagamisele kõigi liikmesriikide ulatuses ning vähendab küberturvalisuse teabega seotud

konkreetsemalt Euroopa Komisjoni ettepaneku rubriigi alt, dokumentidest numbritega 52020PC0823, 52020SC0345 ja 52020SC0344. Lisaks: https://eur-lex.europa.eu/legal-content/EN/PIN/?uri=celex:52020PC0823 ja https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Kuberturvalisus-vorgu-ja-infosusteemide-turvalisust-kasitlevate-ELi-oigusnormide-labivaatamine_et.

[190] Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020PC0823.

[191] Kõnesolevas eelnõus „üliolulistena“.

ebaühtlust.
Direktiivi (EL) 2016/1148 toimivuse hindamises[192] analüüsiti NIS2-direktiivi koostamise puhul järgmisi asjaolusid:
C. Eelistatud poliitikavariandi mõju

- *Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) eelised?*

Eelistatud poliitikavariant tooks märkimisväärset kasu: hinnangute kohaselt, mis põhinevad küberturvalisuse direktiivi [(EL) 2016/1148] läbivaatamise toetuseks korraldatud uuringu raames välja töötatud majandusmudelil, võib eelistatud poliitikavariant vähendada küberturvalisuse intsidentidega seotud kulusid 11,3 miljardi euro võrra.
Küberturvalisuse raamistikuga laiendataks sektoripõhist kohaldamisala märkimisväärselt, kuid lisaks mainitud eelistele kaasneb küberturvalisuse nõuetega koormus (eelkõige järelevalve aspektist), mida tasakaalustataks nii uute hõlmatud üksuste kui ka pädevate asutuste jaoks. Seda tänu asjaolule, et uue küberturvalisuse raamistikuga kasutataks kahetasandilist lähenemisviisi, keskendudes suurtele ja peamistele üksustele ning rakendades diferentseeritud järelevalvekorda, mis võimaldab suure hulga üksuste, nimelt olulisena (mitte elutähtsana[193]) käsitatavate üksuste suhtes kohaldada järelevalve järelkontrollimeetmeid (nn ex-post-järelevalve, mis tähendab reageerivat lähenemist ega hõlma üldist kohustust nõuetele vastavust süstemaatiliselt dokumenteerida).
Kokkuvõttes saavutataks selle poliitikavariandiga soodsad kompromissid ja tõhusad sünergiad ning sellel oleks kõigist analüüsitud poliitikavariantidest suurim potentsiaal tagada, et kogu liidu ulatuses saavutatakse võtmetähtsusega üksuste kübervastupidavusvõime kõrgem ja ühtlasem tase, mis lõppkokkuvõttes tähendaks nii ettevõtjate kui ka ühiskonna jaoks kulude kokkuhoidu.

- *Millised on eelistatud poliitikavariandi (kui see on olemas, vastasel korral peamiste poliitikavariantide) kulud?*

Eelistatud poliitikavariandi rakendamine tähendaks asjaomaste liikmesriikide ametiasutustele teatavaid nõuete järgimise ja täitmise tagamisega seotud kulusid (hinnanguliselt suureneb ressursivajadus kokku ligikaudu 20–30 %). Samas tooks uus raamistik märkimisväärset kasu ka selle kaudu, et tagaks olulistest ettevõtjatest parema ülevaate ja nendega tõhusama suhtlemise, tulemuslikuma piiriülese operatiivkoostöö ning vastastikuse abistamise ja vastastikuse hindamise mehhanismid. Selle tulemusena tõuseks liikmesriikide küberturvalisuse alase suutlikkuse üldine tase.
Küberturvalisuse raamistiku kohaldamisalasse hõlmatavad ettevõtjad peaksid esimestel aastatel pärast küberturvalisuse raamistiku jõustumist suurendama oma IKT-turbega seotud kulutusi maksimaalselt 22 % võrra (need ettevõtjad, kes juba kuuluvad [küberturvalisuse direktiivi (EL) 2016/1148] kohaldamisalasse, 12 % võrra). IKT-turbega seotud kulutuste keskmine suurenemine tooks samas kaasa proportsionaalse investeeringukasu, eelkõige tänu küberturvalisuse intsidentidega seotud kulude märkimisväärsele vähenemisele (hinnanguliselt kuni 11,3 miljardit eurot kümne aasta jooksul).

- *Milline on mõju VKEdele ja konkurentsivõimele?*

Väike- ja mikroettevõtted jäetaks eelistatud poliitikavariandi puhul küberturvalisuse raamistiku kohaldamisalast välja. Keskmise suurusega ettevõtjate IKT-turbega seotud kulutused esimestel aastatel pärast uue küberturvalisuse raamistiku kasutuselevõttu eelduste kohaselt suurenevad.

[192] Euroopa Komisjoni talituste töödokument mõju hindamise aruande kommenteeritud kokkuvõte; lisatud dokumendile: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148. C osa: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020SC0344.
[193] Kõnesolevas eelnõus „üliolulistena".

Samas soodustaks nende üksuste turvanõuete taseme tõstmine ka nende küberturvalisuse alase suutlikkuse suurenemist ja aitaks tõhustada nende IKT-alast riskijuhtimist.

- *Kas on ette näha märkimisväärset mõju riigieelarvetele ja ametiasutustele?*

Oodatav mõju liikmesriikide eelarvetele ja haldusasutustele: lühikese ja keskpika perspektiivi prognoosi kohaselt suureneb ressursivajadus hinnanguliselt ligikaudu 20–30 %.

- *Kas on oodata muud olulist mõju?*

Muud olulist negatiivset mõju ei ole ette näha. Eelistatud poliitikavariandi rakendamisega peaks saavutatama suurem küberturvalisuse alane suutlikkus ning seeläbi peaks oluliselt vähenema intsidentide, sealhulgas andmetega seotud rikkumiste arv ja raskusaste. Samuti avaldab see tõenäoliselt positiivset mõju kõikide küberturvalisuse raamistiku kohaldamisalasse kuuluvate üksuste jaoks võrdsete tingimuste tagamisele kõigi liikmesriikide ulatuses ning vähendab küberturvalisuse alase teabega seotud ebaühtlust.

Eelmainitud mõjude analüüsimisel tuleb arvestada, et tegemist on Euroopa Komisjoni koostatud hinnanguga, mis hindas ennekõike NIS2-direktiivi sõnastusettepanekute mõju võrreldes nende õigusnormidega, mis direktiiv (EL) 2016/1148 ette nägi. Eesti puhul on NIS2-direktiivi rakendamise kulud väiksemad, sest esimese direktiivi (direktiiv (EL) 2016/1148) üle võtmisel rakendasime miinimumist rohkem nõudeid ning KüTSi muudeti ka 2022. aastal.

NIS2-direktiivi algatuse 7. lisa (finantsselgitused – ametid) punktis 1.4.4 on märgitud, milliste näitajate abil jälgitakse NIS2-direktiivi edusamme ja saavutusi:

1.4.4. Tulemusnäitajad

Näitajaid hindab komisjon ENISA ja koostöörühma toetusel kolm aastat pärast uue küberturvalisust käsitleva õigusakti jõustumist. Järgnevalt on loetletud mõned seirenäitajad, mille alusel küberturvalisuse alast edukust läbivaatamisel hinnatakse.

- *Tõhusam intsidentide käsitlemine. Küberturvalisuse meetmete võtmisega parandavad ettevõtjad mitte ainult oma võimet teatavaid intsidente täielikult vältida, vaid ka oma suutlikkust intsidente lahendada. Edunäitajad on seega i) intsidendi tuvastamiseks kuluv keskmine aeg (selle lühenemine), ii) keskmine aeg, mis kulub organisatsioonidel intsidendist taastumiseks, ja iii) intsidendi põhjustatud kahju keskmine maksumus.*
- *Ettevõtete tippjuhtkonna suurem teadlikkus küberturvalisusega seotud riskidest. Ettevõtjatelt meetmete võtmise nõudmise kaudu aitaks [NIS2-direktiiv] suurendada tippjuhtkonna teadlikkust küberturvalisusega seotud riskidest. Seda saab mõõta, uurides, kuivõrd prioriseerivad küberturvalisuse raamistikuga hõlmatud ettevõtjad küberturvalisust oma ettevõtte sise-eeskirjades ja -protsessides (mida tõendavad ettevõtte sisedokumendid, asjakohased koolitusprogrammid ja töötajate teadlikkuse suurendamiseks võetavad meetmed) ning seda, kuivõrd prioriseeritakse küberturvalisusse tehtavaid IKT-investeeringuid. Kõigi elutähtsate[194] ja oluliste üksuste juhtkond peaks samuti olema teadlik [NIS2-direktiivis] sätestatud eeskirjadest.*
- *Valdkonnapõhiste kulutuste ühtlustumine. IKT-turvalisusega seotud kulutused on ELi eri sektorites väga erinevad. Kui nõuda meetmete võtmist suurema arvu sektorite ettevõtjatelt, peaksid kõrvalekalded sektoripõhistest keskmisest IKT-turbega seotud kulutustest (mida väljendatakse protsendina IKT-valdkonda tehtavatest kõigist kulutustest) vähenema nii sektorite kui ka liikmesriikide tasandil.*
- *Tugevamad ja pädevamad asutused ning ulatuslikum koostöö. [NIS2-direktiiviga] võidakse määrata pädevatele asutustele lisaülesandeid. Sellel oleks mõõdetav mõju küberturvalisusega tegelevatele asutustele riiklikul tasandil eraldatavatele rahalistele ja inimressurssidele ning see peaks avaldama positiivset mõju ka pädevate asutuste võimele ennetavalt koostööd teha ja seega suurendama selliste juhtumite arvu, mille puhul pädevad asutused suhtlevad üksteisega, et*

[194] Kõnesolevas eelnõus „üliolulised“.

lahendada piiriüleseid intsidente või teha ühist järelevalvet.

- *Ulatuslikum teabevahetus: [NIS2-direktiiviga] parandataks ka teabevahetust ettevõtjate vahel ja teabevahetust pädevate asutustega. Üks muutmise eesmärke võiks olla nende üksuste arvu suurendamine, kes teabevahetuse eri vormides osalevad.*

Esimene küberturvalisuse direktiiv ehk direktiiv (EL) 2016/1148, mis sillutas paljudes liikmesriikides teed mõtteviisi olulisele muutusele ning pani aluse institutsioonilise ja regulatiivse lähenemisviisi kujunemisele küberturvalisuse valdkonnas, on andnud küll märkimisväärseid tulemusi, kuid selle võimalused on osutunud piiratuks. Ühiskonna digiüleminek (mida võimendas COVID-19 kriis) on ohumaastikku laiendanud ning toonud kaasa uusi probleeme, mis nõuavad kohandatud ja uuenduslikke lahendusi. Küberrünnete arv kasvab endiselt, need on üha keerukamad ning pärinevad paljudest eri allikatest nii Euroopa Liidus kui ka mujal. Tuginedes [direktiivi (EL) 2016/1148] toimivuse hindamisele, tuvastati mõjuhinnanguga järgmised probleemid: Euroopa Liidus tegutsevate ettevõtjate kübervastupidavusvõime madal tase; ebaühtlane vastupidavusvõime tase liikmesriikide ja sektorite tasandil ning ühise olukorrateadlikkuse madal tase ja ühistegevuse puudulikkus kriisidele reageerimisel.[195]

NIS2-direktiivi ettevalmistamisel analüüsiti ka võrreldes direktiiviga (EL) 2016/1148 sektorite ja subjektide lisandumist, mistõttu seda seletuskirjas eraldi ei analüüsita ega korrata.[196]

NIS2-direktiivi ettevalmistamisel oli soov välistada olukord, kus mikro- ja väikeettevõtjad satuvad NIS2-direktiivi kohaldamisalasse. Seetõttu ongi peamiseks lävendiks määratud keskmise suurusega ettevõtja, arvestades soovituse 2003/361/EÜ lisa artikli 2 kriteeriume. Samas ei ole seda siiski suudetud välistada – näiteks juhul, kui on sõnaselgelt ette nähtud, et mingi üksus kuulub NIS2-direktiivi kohaldamisalasse, olenemata selle suurusest (nt elutähtsa teenuse osutajad), mis võib kaasa tuua ka mikro- ja väikeettevõtjate lisandumise KüTSi kohaldamisalasse.

Järgnevalt analüüsitakse eelnõukohase seaduse sätete mõju Eestis.

Seaduseelnõus kavandatud muudatustest on seletuskirja mõjuanalüüsis (või seletuskirja mõju osas) käsitletud üksnes need muudatused, millele on tuvastatud oluline mõju. Ülejäänud muudatustel olulist mõju ei tuvastatud ning seetõttu neid seletuskirjas ei käsitleta. Eelnõu toob kaasa muudatusi ennekõike KüTSis olevatele kui ka sinna lisanduvatele üksustele NIS2 direktiivi tõttu, kuid olenevalt konkreetsest ülesandest võib konkreetne mõju olla ainult osadel või kõigil üksustel ehk subjektidel. KüTSi §-s 3 tehtavate muudatuste tulemusena määratakse kindlaks, millised üksused on KüTSi kohaldamisalas, sh kas need on käsitatavad ülioluliste üksustena või oluliste üksustena. Lisaks sätestatakse ka mõned kohustused domeenimede registreerimise teenuse osutajatele. Osa eelmainitud üksustest on ka kehtiva KüTSi kohaldamisalas ehk siin säilitatakse kehtiv õigus.

Seetõttu saab järgmisena esitatud muudatuste kirjelduste juures jaotada mõjud üldjoontes kahe rühma vahel: (1) need üksused, mis on praegu ja ka edaspidi KüTSi subjektid, ning (2) need üksused, mis saavad KüTSi subjektiks NIS2-direktiivi tõttu. Kui allpool esitatud muudatuse juures ei ole konkreetse mõju valdkonna kontekstis tehtud vahetegu nende kahe rühma puhul, siis mõju ilmneb mõlema grupi suhtes, kui mõju valdkonna juures esitatud analüüs viitab KüTSiga seotud üksustele.

Praegu on KüTSi kohaldamisalas umbes 3500 üksust ning eelnõu järgi lisandub neile umbes 3000 (+/- 10%) ehk kokku on umbes 6500 subjekti (üksust), kellele KüTSi uuendatud nõuded hakkavad kohalduma. Nende arvude puhul tuleb arvestada asjaoluga, et ilmselt osa subjekte vastab mitmele

[195] Euroopa Komisjoni talituste töödokument mõju hindamise aruande kommenteeritud kokkuvõte; lisatud dokumendile: Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148. A osa: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020SC0344.

[196] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020SC0345

tunnusele: näiteks on tegemist nii keskvalitsuse avaliku halduse üksusega kui ka avaliku teabe seaduse tähenduses andmekogu vastutava töötlejaga või volitatud töötlejaga; või näiteks on tegemist elutähtsa teenuse osutajaga ning samal ajal ka üldkasutatava elektroonilise side võrgu teenuse osutajaga; või on tegemist vee-ettevõtjaga, kes samal ajal tegutseb ka reovee valdkonnas. Samuti tuleb arvestada võimalusega, et esialgne subjektide arv toetub poolikutele algandmetele või eeldustele.

Nimetatud arvude puhul tuleb ka arvestada, et domeeninimede registreerimise teenuse osutajatele ei kohaldata kõiki KüTSi nõudeid (vt eelnõukohase KüTSi § 2 punkti 4 selgitust).

Eeltoodut iseloomustab ka järgnev tabel nr 2, mis iseloomustab eelnõukohase seadusega KüTSi lisatavate või juba KüTSis olevate üksuste arvu võrreldes sihtrühma ehk samas õiguslikus vormis tegutsevate juriidiliste isikute arvuga. Eraõiguslike isikute puhul on sihtrühmaga seotud arvud ühendatud ehk tabelis olev arv sisaldab aktsiaseltse, osaühinguid, välismaa äriühingu filiaale, sihtasutusi ja füüsilisest isikust ettevõtjaid ehk FIEsid (vastavad arvnäitajad on: 2123 + 269 990 + 480 + 785 + 25 272). Riigi ja kohaliku omavalitsuse asutusena on mõeldud kohaliku omavalitsuse asutust, täidesaatva riigivõimu asutust või muud institutsiooni ning avalik-õiguslikku juriidilist isikut, põhiseaduslikku institutsiooni või nende asutust (vastavad arvnäitajad on 1569 + 147 + 38) ehk eelnõu sõnastuse kohaselt keskvalitsuse avaliku halduse üksust ja kohaliku omavalitsuse avaliku halduse üksust. Tabelis on õigusliku vormi puhul kasutatud andmete allika – e-äriregistri portaalis oleva registri seisu statistika[197] – sõnastust. Mõjutatavate eraõiguslike isikute hulga puhul on arvestatud eeldusega, et lisanduvate üksuste hulk suureneb umbes 3000 võrra ehk see arv ei arvesta võimalikku veaprotsenti (+/- 10%). Seega võib see arv olla suurem või väiksem umbes 300 üksuse võrra. Sama arvu hulgas on ka need üksused, mis peavad kohaldama kehtiva KüTSi nõudeid ehk tegemist on seaduse mõttes teenuseosutajatega.

Tabel 2. Eelnõukohase seadusega mõjutatavate üksuste arv juriidilise isiku vormina võrreldes kõikide sama liiki juriidiliste isikutega

Õiguslik vorm	**Koguarv (10.07.2025 seisuga) (arv)**	**Eelnõukohase seadusega mõjutatud üksuste hulk (arv)**	**Eelnõukohase seadusega mõjutatud üksuste arv võrreldes üksuste koguarvuga (%)**
Eraõiguslikud isikud (aktsiaselts, osaühing, filiaal, sihtasutused ja FIEd)	298 650	umbes 4700	umbes 1,5737%
Riigi- ja kohaliku omavalitsuse asutused	1754	1754	100%
Kokku üksusi		umbes 6500	

Andmeallikas: e-äriregistri portaal (seis 10.07.2025)

Eeltoodu põhjal on eelnõukohase seadusega mõjutatavate eraõiguslike isikute sihtrühm väike võrreldes kogu sihtrühmaga. Riigi ja kohaliku omavalitsuse asutuste puhul tuleb arvestada, et kõnealused üksused on juba praegu KüTSi subjektid kõikide võrgu- ja infosüsteemide ning tegevuste osas, mistõttu on seaduse tegelik mõju neile ennekõike minimaalne. KüTSi subjektiks saavate üksuste lõplik arv selgub, kui Riigi Infosüsteemi Amet koostab esitatud andmete põhjal

[197] https://ariregister.rik.ee/est/statistics

subjektide nimekirja (vt eelnõus KüTSi § 3^1).
Kokkuvõtlikult on eelnõu mõjud (st kas haldus- või töökoormus väheneb, suureneb või jääb samaks) järgmised:

a) halduskoormus tabelis viidatud eraõiguslikele isikutele: eelnõu mõjutab ainult nende eraõiguslike isikute halduskoormust, kes on juba praegu KüTSi kohaldamisalas, ning neid, kes eelnõuga KüTSi lisanduvad; neist esimeste halduskoormus lühiajaliselt suureneb seaduse jõustumise järel, kuna need peavad edaspidi kõigi oma teenuste ja tegemiste puhul lähtuma täiendatud KüTSi nõuetest, kuid kuna sarnased nõuded kehtisid ka varem (nt konkreetse teenuse kohta), siis halduskoormuse suurenemine ei ole eelduslikult märkimisväärne; teistel halduskoormus suureneb ennekõike kohe eelnõu seadusena jõustumise järel, kuna kehtima hakkavate õigusnormide rakendamine võtab teatava aja, pärast seda halduskoormus enam ei suurene.
b) halduskoormus elanikele ja kodanikele: mõju puudub, st sellele rühmale ei ole kehtiva õiguse kohaselt küberturvalisuse valdkonnas halduskoormust ning kehtestatava seadusega seda ka ei tekitata;
c) avaliku sektori töökoormus ei suurene.

6.1. Kavandatav muudatus: riskijuhtimismeetmete ehk turvameetmete rakendamise nõue

Muudatus on seotud NIS2-direktiivi artikliga 21, mis võetakse üle KüTSi §-ga 7, ennekõike selle lõikega 2 ning sama paragrahvi lõike 5 alusel kehtestatud Vabariigi Valitsuse määrusega. Artiklis 21 on kasutatud sõnastust „küberturvalisuse riskijuhtimismeetmed“, kuid seaduses on selle puhul mõeldud turvameetmete rakendamise nõuet.
Seadusel puuduvad muud otsesed või kaudsed mõjud, mis on olulised Vabariigi Valitsuse 22. detsembri 2011. a määruse nr 180 „Hea õigusloome ja normitehnika eeskiri“ § 46 lõike 2 kohaselt.

6.1.1. Sotsiaalne, sealhulgas demograafiline mõju

Kommenteeritav muudatus ei tekita ettevõtjale märkimisväärset sotsiaalset mõju. KüTSi subjektide vajadus tööturul sobiva kvalifikatsiooniga küberturbe ekspertide järele küberturvalisuse tagamiseks jääb püsima.
Seadusel on positiivne mõju isikutele (füüsilistele ja juriidilistele), kelle andmed asuvad nii olemasolevate kui ka uute subjektide võrgu- ja infosüsteemides. Muudatus võib mõjutada ka inimeste karjäärivalikuid tegelemaks infotehnoloogia sektoriga, sh suurendab inimeste teadlikkust küberturvalisuse valdkonnast ning küberturvalisuse tagamise olulisusest, kuna üks osa ette nähtud nõuetest on küberturvalisuse koolitused.
IKT areng toob kaasa teenuste parema kättesaadavuse ja kasutusmugavuse. Tehnoloogia suureneva osatähtsusega kaasneb ühiskonna, majanduse ja riigi sõltuvus juba harjumispärastest e-lahendustest ning kinnistub ootus tehnoloogia tõrgeteta toimimisele. Selle tõttu on ka väga oluline, et oleks tagatud kodanikele oluliste teenuste katkematu toimimine.
Muudatusel on positiivne mõju ka isikuandmete kaitse tagamisele, kuna paraneb uute subjektide teadlikkus vajadusest kaitsta võrgu- ja infosüsteeme, milles on inimeste isikuandmed.
Eeltoodu tõttu on muudatuse mõju ulatus, sagedus ja ebasoovitavate mõjude risk väike.

6.1.2. Mõju riigi julgeolekule ja välissuhetele

Valmisolek küberintsidentide ennetamiseks, tõrjumiseks ja lahendamiseks on seotud ka riigikaitse ja julgeolekuga. Eesti julgeolekupoliitika alustes on kirjas: „Eesti ühiskonna turvalisus ja majandusedu sõltuvad digiühiskonna kestlikust arengust. Digipöördes ja tehnoloogilistes valikutes peavad riik ja erasektor võtma arvesse julgeolekukeskkonda ning üleilmseid tehnoloogilisi suundumusi. Digitaalses ruumis peame läbivalt kõigis infosüsteemides, organisatsioonides ja

protsessides planeerima küber- ja infoturvet.“[198] Seadus mõjutab riigi julgeolekut küberturvalisuse taseme tõusu kaudu, millega tagatakse süsteemide järjepidev ja võimalikult väheste tõrgetega toimimine.
Muudatusel on positiivne mõju riigi julgeolekule ja välissuhetele, kuna see annab selguse, millistele sektoritele ja valdkondadele on ette nähtud ühised küberturvalisuse riskijuhtimise nõuded, mis on samaväärsed teistes Euroopa Liidu liikmesriikides kehtestatud nõuetega.
Seadusega luuakse piiriülesed mehhanismid küberintsidentide tõhusamaks lahendamiseks ning suurendatakse riikidevahelist koostööd, millel on mõningane mõju ka piiriüleselt tegutsevatele ettevõtetele.
Paralleelset mõjutab muudatus ka Eesti kui e-ühiskonna ja küberturvalisuse positiivset kuvandit ning suurendab koostööd nii riigi ja ettevõtete vahel kui ka rahvusvahelisel tasandil. Välissuhete vaatepunktist aitab muudatus säilitada ning arendada Eesti riigi kui küberturvalisuse eestvedaja kuvandit.
Võrgu- ja infosüsteemide paremal kaitstusel võiks olla teatav mõju kodanike turvatundele, kuna Eesti riik ja ühiskond sõltub e-lahenduste toimimisest, rahvas usaldab e-teenuseid ning vajab turvalisi küberteenuseid.
Eeltoodu tõttu on muudatuse mõju ulatus, sagedus ja ebasoovitavate mõjude risk väike.

6.1.3. Mõju majandusele

Võrgu- ja infosüsteemide turvalisusel on vahetu mõju majanduskeskkonna toimimisele. Seetõttu on seaduse kehtestamise üks eesmärke edendada selgema raamistiku kaudu võrgu- ja infosüsteemide turvalisust. Vastus Eesti majanduse proovikiviks peetud küsimusele, kas suudetakse pakkuda suurema lisandväärtusega tooteid ja teenuseid, seisneb suuresti digilahenduste kasutuselevõtus või uute digitaalsete toodete pakkumises. Oodatav konkurentsieelis realiseerub vaid juhul, kui digitaalsete lahenduste toimepidevus, terviklus ja konfidentsiaalsus on tagatud, sest need määravad otseselt toote või teenuse usaldusväärsuse. E-teenuste toimimine sõltub nende turvakindlusest (nii tegelikust kui ka tajutavast), mis vahetult mõjutab inimeste usaldust teenuste vastu. Teenuste suurenev turvalisus suurendab omakorda kodanike ja elanike usaldust digitaalsete teenuste vastu ning suunab neid rohkem kasutama, tagades selle kaudu ka nende teenuste toimimise jätkusuutlikkuse. Kodanike ja elanike halduskoormust seadus ei mõjuta. E-teenuste pideva toimimise parem tagamine aitab kokku hoida riigi või erasektori ettevõttega suhtlemiseks kuluvat aega.
Eestis on palju ettevõtjaid, kelle teenuste toimimine sõltub oluliselt info- ja kommunikatsioonitehnoloogiast ning kes on ka juba praegu planeerinud vahendeid turvameetmete rakendamiseks. Risk, et ettevõtjad ei soovi uute reeglite tõttu Eestis tegutseda, on väike, sest NIS2-direktiivi vastuvõtmise korral on kõikidel Euroopa Liidu liikmesriikidel kohustus uus kord jõustada. Küll aga tuleb leida koostöös ettevõtjatega parimad lahendused, mis lihtsustaks neil oma kohustusi täita parimal võimalikul moel.
Muudatuse mõju sõltub mitmest asjaolust, sh sellest, kas konkreetne üksus kuulub kehtiva KüTSi kohaldamisalasse või see on uus subjekt. Mõlema variandi puhul võib tähtsust omada ka konkreetse üksuse vastavus kehtestatava seaduse nõuetele, kuid seletuskirjas saab analüüsida ainult mõju nõuete muudatuste kontekstis.
Küberturvalisusega seotud kulutused võib jaotada peamiselt kaheks: i) kulutused, mida tehakse küberturvalisuse tagamiseks organisatsioonis (pädeva personali palkamine, teenuste ja süsteemide kaardistamine, riskianalüüs, meetmete rakendamine), ning ii) kulutused, mida tehakse küberintsidendi tagajärgede likvideerimiseks (lunavara nõuded, andmebaaside taastamine, riistvara

[198] Riigikogu 22.02.2023. a otsus „Eesti julgeolekupoliitika alused“ heakskiitmine, lk 12: https://dhs.riigikantselei.ee/avalikteave.nsf/documents/NT003B6B36/.

väljavahetamine, info- ja võrgusüsteemide uuesti arendamine, teenuse osutamata jätmisega tekkinud kahju kandmine (sh esitatud kahjunõuded ja leppetrahvid jne)).
Alati on võimalik, et üksus, mis on teinud küberturvalisuse tagamisele olulisi kulutusi, ei suuda vältida kahjulikke küberintsidente ega nendega kaasnevaid kulutusi, ning üksus, mis ei ole teinud kulutusi küberturvalisuse tagamiseks, ei lange küberintsidendi ohvriks ega kanna ka sellest põhjustatud kulutusi, kuid üldjuhul tähendab küberturvalisuse tagamiseks tehtavate kulutuste suurendamine küberintsidendi juhtumise tõenäosuse vähenemist. Samas näitab Riigi Infosüsteemi Ameti statistika, millega on võimalik tutvuda iga kuu ilmuva väljaande „Olukord küberruumis“[199] vahendusel, et küberintsidendi ohvriks langemise puhul on küsimus pigem ajas, millal see juhtub, ning toimunud küberintsidendi mõju ulatuses. Seega ei saa pidada mõistlikuks lähenemist, et küberturvalisuse tagamiseks jäetakse kulutused tegemata põhjendusel, et loodetavasti KüTSi subjekt ei lange küberintsidendi ohvriks.

Seaduse eesmärk on tekitada kommenteeritava muudatusega nõuded ennekõike keskmise suurusega ning suurematele organisatsioonidele, kuid ei saa välistada, et kohustused tekivad ka mikro- või väikeettevõtjatele. Seetõttu on nõuete täitmiseks ette nähtud üleminekuaeg – vt KüTSi § 28^1 sisu ja seletuskirja.
Kehtiva KüTSi kohaldamisalasse kuuluva subjekti puhul ei ole muudatused märkimisväärsed, kuna ka eelnõu KüTSi § 7 lõike 2 selgitustes on märgitud, et NIS2-direktiivi artikli 21 lõikes 2 sätestatud küberturvalisuse riskijuhtimismeetmed on samaväärsed nende nõuetega, mida näeb ette Eesti infoturbestandard või selle alternatiiviks olev rahvusvaheline standard ISO/IEC27001.

Kui tegemist on stsenaariumiga, kus KüTSi uue subjekti suhtes ei ole ette nähtud küberturvalisuse riskijuhtimismeetmeid, kuid seadusemuudatusega need tekivad, siis nendele üksustele võib mõningane mõju avalduda. Kui arvestada asjaoluga, et seaduse küberturvalisuse riskijuhtimismeetmete nõuete sisu on samaväärne Eesti infoturbestandardi nõuetega, siis saab välja tuua paralleeli Eesti infoturbestandardi rakendamisega seotud mõjude ja tähelepanekutega.
Ennetavalt tuleb mainida, et seaduse ja sellega seotud määruste kavandite kõrval on Justiits- ja Digiministeeriumil ettevalmistamisel ka KüTSi § 7 lõike 5 alusel antud Vabariigi Valitsuse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muudatus (eelnõude infosüsteemi toimik 25-0715),[200] mis sätestab (1) üldised turvameetmete nõuded, millest kõik KüTSi teenuseosutajad peavad lähtuma (v.a kui tegemist on KüTSi suhtes *lex specialis*’ega ehk eelnõujärgse KüTSi § 1 lõike 4 olukorraga või kui tegemist on NIS2-direktiivi artikli 21 lõike 5 alusel antava rakendusaktiga – vt eelnõukohase KüTSi § 7 lõike 7 sõnastust ja selgitusi), ning (2) muudab lävendit, millal peab teenuseosutaja rakendama Eesti infoturbestandardit (koos selle auditeerimisega) või alternatiivset rahvusvahelist standardit ISO/IEC 27001.

Üksuse puhul, mille suhtes pole veel ette õigusaktiga nähtud küberturvalisuse riskijuhtimismeetmeid ehk turvameetmeid, tuleb arvestada infoturbega tegelevate inimeste ajakuluga, et koostada Eesti infoturbestandardi ülevõtmiseks vajalik dokumentatsioon. Ajakulu on suurem, kui dokumentatsioon, sh vajalikud protsesside, varade ja muude ressursside kaardistused, tuleb koostada esimest korda.
Seadus võib kaudselt mõjutada KüTSi uue subjekti osutatavate teenuste kvaliteeti, kuna teenuste kaardistamine ja riskipõhine lähenemine aitab üksusel tuvastada tehnoloogilisi mahajäämusi või paremaid arendussuundi. Eesti infoturbestandardi rakendamise eelduseks olev selge ülevaade üksuse äriprotsessidest ja nendega seotud teenustest aitab hinnata üksuse toimimiseks vajalikke

[199] https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/olukord-kuberruumis
[200] https://eelnoud.valitsus.ee/main/mount/docList/7d3ea848-35b2-47d8-8eb8-fa2f735c3da6

ressursse.
Isikutel, kes ei ole varem turvameetmete rakendamiseks kulutusi teinud, tekib ilmselt lisaressursi vajadus (näiteks personalikulu, IT-süsteemide arendamise kulu, riskianalüüsi koostamise kulu). Majanduslik mõju on sellisel juhul igale üksusele väga erinev ning ei ole täpselt hinnatav, kuna üksuste tegevusalad ja vajadused on erinevad. Näiteks on ilmselgelt erinevad vajadused kohalikus omavalitsuses olevate sõiduteede sõidetavust tagaval üksusel, mis on saanud elutähtsa teenuse osutajaks, ja üksusel, mis on üldkasutatava elektroonilise side teenuse osutaja. Turvameetmete rakendamiseks vajalik rahaline kulu sõltub konkreetse üksuse kasutatavate süsteemide hulgast, keerukusest ning nendele nii enne kasutamist rakendatud turvameetmete olemasolust (sõltub üksuse vastutustundlikkusest oma IT-lahenduste kasutamisel või muudest seaduslikest nõuetest, näiteks kui isikuandmete töötlemiseks on rakendatud tehnilisi ja korralduslikke meetmeid isikuandmete turvalisuse tagamiseks) kui ka turvameetmete rakendamisega seotud personali olemasolust või vajadusest leida selleks spetsialiste juurde. Rakendamiseks vajaliku kulu majanduslik mõju üksusele sõltub omakorda selle kulu osakaalust üksuse eelarves (näiteks IT-lahendustega seotud eelarves). Kui üksus on otsustanud või edaspidi otsustab mingi osa oma turvameetmete haldamisest anda üle muule isikule (näiteks teenus tellitakse infoturbeteenuse osutajalt), on üksuse enda tegevusvaldkonna ja sellega seotud teenuse ning eelkirjeldatud muude asjaolude põhjal üksusele avalduvat majanduslikku mõju keeruline hinnata.
Selle stsenaariumi korral võib muudatuste tõttu mõnele üksusele tekkida oluline majanduslik mõju, kui üksus kasutab oma tegevuses ulatuslikult keerukaid süsteeme, millele turvameetmeid varem rakendatud ei ole ning mille eelarve ei võimalda nende IT-lahenduste toimepidevuse tagamiseks vajalikke ressursse. Küll aga ei mõjuta see olukord majandusliku mõju hinnangut uute KüTSi subjektide mõttes tervikuna, kuivõrd tegemist oleks ühe osaga väga piiratud subjektide ringist.
KüTSi subjektist juhtkond ise määrab, milliseid objekte ja protsesse on tarvis kaitsta. Etalonturve seab kaitstavad objektid ja protsessid vastavusse etalonturbe kataloogi tüüpmoodulitega. Eesti infoturbestandardi etalonturbe kataloogis leiduvad tüüpmoodulid kirjeldavad tüüpilisi ohte ja neile vastavaid, riskianalüüsi põhjal valitud turvameetmeid. Seetõttu on selle sisu üsnagi mahukas, kuid selle rakendamine ei ole võimatu ülesanne. Turvameetmete rakendamine vähendab küberohtude realiseerumise tõenäosust. Etalonturve võimaldab KüTSi subjektil kasutada infoturbe järjest paremaid lahendusi ning kokku hoida infoturbele kuluvaid vahendeid.
Üks osa näiteks Eesti infoturbestandardi rakendamisest on ka Eesti infoturbestandardi vastavusauditi tegemine iga kolme aasta järel, mis on eelduslikult ühe suurema kulu allikas uutele KüTSi subjektidele, kellele laieneb Eesti infoturbestandardi rakendamise kohustus. Eelnõu nr 426 SE seletuskirjas on lk-l 56 mõjude osas võrgu- ja infosüsteemide riskianalüüsi ning Eesti infoturbestandardi auditi kohta märgitud järgmist: „KüTSi järgi on kohustus koostada võrgu- ja infosüsteemide riskianalüüs, mille võib turult saada olenevalt ettevõttest 2000–20 000 euro eest. Selliseid analüüse saab ettevõte teha ka ise, st kohustust tellida neid ei ole, see on üksnes ettevõtte võimalus. Kõik vähemalt kümne töötajaga ja aasta bilansimahuga või aastakäibega üle 2 miljoni euro elutähtsa teenuse osutajad on KüTSi kohaselt kohustatud tellima sisse võrgu- ja infosüsteemide auditi. Tegemist on ainukese kohustusega, mida ettevõtja ei saa ise täita ja mida tuleb tellida sisse. Auditi maksumus jääb 4500–20 000 euro vahemikku. Maksumus oleneb ettevõtte suurusest ja infosüsteemidest.“ Riigi Infosüsteemi Ameti hinnangul algavad auditi hinnad 10 000 eurost kolmeaastase auditiperioodi kohta. Audit sisaldab eelauditit, põhiauditit, vaheauditit ja järelauditit. Avalike andmete kohaselt leiab nii Eesti infoturbestandardi kui ka rahvusvahelise standardi ISO/IEC 27001 auditeerivate organisatsioonide andmed siit: https://eisay.ee/e-its-ja-iso-27001-alaste-teenustega-tegelevate-ettevotete-loetelu.
On võimalik, et Eesti infoturbestandardi auditeerimiskulud on majanduslikult koormavamad üksustele, mille IKT korraldus on oluliselt väiksema mahuga, kuna lävend on kõigile sama, seega

ka auditi minimaalne kulu (sõltub protseduuri enda kulust, audiitori kvalifikatsiooninõuetest ning auditi käigus koostatava dokumentatsiooni nõuetest). Arvestada tuleb ka asjaoluga, et ettevalmistamisel on Vabariigi Valitsuse määruse muudatus, mis muudab Eesti infoturbestandardi järgimise (koos selle auditeerimisega) lävendit (vt eespool olevat selgitust). Seega mõjutab too muudatus ka seda, millised üksused peavad läbima Eesti infoturbestandardi kohase auditeerimise. Lisaks toetab Riigi Infosüsteemi Amet Eesti infoturbestandardile üleminekut koolituste korraldamisega.[201] Amet on avaldanud tehnoloogilise rakenduse, mis abistab Eesti infoturbestandardi rakendamist. Sel teemal vt allpool seletuskirja järgmist peatükki.
Siin tuleb arvestada asjaoluga, et mõjude ulatus on eelduslikult väiksem, kuivõrd kohustusi uutele KüTSi subjektidele tehniliste ja korralduslike turvameetmete rakendamiseks on sätestatud ka muudes aktides: rakendada tuleb isikuandmete turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid isikuandmete kaitse üldmääruse artikli 32 lõike 1 alusel ning samuti lähtuma selle kohustuse täitmisel riskide analüüsist sama määruse artikli 32 lõike 2 alusel.
Lisaks on oluline märkida, et isegi kui kehtestatava seaduse järgi peab üksus võtma rahalisi kohustusi võrgu- ja infosüsteemide turvalisuse tagamiseks, võib nende kulude mõju olla üksusele majanduslikult positiivne. Süsteemide turvalisuse tagamiseks tehtavad kulutused vähendavad nii küberintsidendi tekkimise tõenäosust kui ka tekkinud küberintsidendi kahjulikku majanduslikku mõju. Arvestades küberruumis aina sagedamini esinevaid rünnakuid[202] ning nende laastavat mõju ohvri süsteemide kasutatavusele, ei ole õigustatud vaadelda süsteemide turvalisuse tagamiseks tehtavaid kulutusi rangelt kahjuliku majandusliku mõjuna.
Mõnele üksusele on muudatusega seotud täpsustused ette nähtud NIS2-direktiivi artikli 21 lõike 5 alusel kehtestatud delegeeritud määruses. Viidatud lõige näeb ette, et Euroopa Komisjon peab vastu võtma rakendusaktid, milles „sätestatakse sama artikli lõikes 2 osutatud meetmete tehnilised ja metoodilised nõuded seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, [haldusteenuse osutajate], [infoturbeteenuse osutajate], internetipõhiste kauplemiskohtade, [veebipõhiste otsingumootorite] ning sotsiaalvõrguteenuse platvormide ja usaldusteenuse pakkujatega.“ Seetõttu on komisjoni rakendusmääruses (EL) 2024/2690[203] täpsustatud eelmainitud üksuste suhtes kehtivaid küberturvalisuse riskijuhtimismeetmete nõudeid ehk nende üksuste puhul ilmneb mõju rakendusmäärusest, mitte kehtestatavast seadusest. Seetõttu ei ole võimalik viidatud rakendusmäärusega seotud mõjusid siin analüüsida.

Muudatusel on eelduslikult mõju majanduskeskkonnale ja seega ka ettevõtlusele, kuna tekib teatav nõudlus küberturvalisuse tagamise valdkonnas pakutavate teenuste järele. See omakorda võib suurendada ettevõtete arvu või olemasolevate ettevõtete osutatavate teenuste arvu – näiteks võib tekkida uusi konsultatsioonide, auditeerimise või koolitamise teenuse osutajaid või teenuseid. Kuid mõju ettevõtluse toimimisele on keeruline hinnata, kuna ei ole teada, kui palju uusi ettevõtteid võidakse nende teenuste osutamiseks luua või kui palju olemasolevad ettevõtted võivad täiendada oma teenuste nimekirja.

Muudatuse mõju ulatus seaduse jõustumise järel on keskmine, kuna muudatus avaldab mõju ennekõike neile üksustele, kes saavad KüTSi järgi teenuseosutajateks (võrreldes kõikide üksuste arvuga, kellele muudatus hakkab edaspidi kohalduma). Olemasolevate teenuseosutajate korral on muudatuse mõju samuti kuni keskmine siis, kui nad peavad edaspidi turvameetmeid rakendama

[201] https://eits.ria.ee/et/avalehe-menueue/suendmused
[202] Riigi Infosüsteemi Ameti ööpäeva ülevaade Eesti küberruumi kohta: https://www.ria.ee/et/kuberturvalisus/olukord-kuberruumis/oopaeva-ulevaated.html.
[203] https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX:32024R2690&qid=1732094006135

kõikide oma võrgu- ja infosüsteemide suhtes, mitte ainult konkreetse teenuse osutamisega seotud süsteemidele.
Muudatuse mõju sagedus on kuni keskmine ennekõike uutele üksustele, kuna turvameetmete rakendamine nõuab alguses rohkem aega ja pühendumust. Mõne aja pärast muutub mõju korrapärasemaks, kui üksused on suutnud küberturvalisuse meetmetega seotud protsessid evitada ning käigus hoida. Kuna muudatusega seotud teemal on olemas juhendeid (mida ka ajakohastatakse) ning toimub koolitusi ja teabepäevi, on muudatusega seotud ebasoovitavate mõjude risk pigem väike.[204]

6.1.4. Mõju elu- ja looduskeskkonnale
KüTSi kohaldamisalasse lisandub üksusi, mille põhitegevus on mitmel moel seotud tegevustega, mis võivad kahjustada või häirida elu- ja looduskeskkonda. Kehtestatav seadus ise ei avalda otsest mõju elu- ja looduskeskkonnale. Kaudselt võib positiivset mõju elu- ja looduskeskkonnale aga avaldada vastupanuvõime suurendamine küberrünnakute suhtes, mis saaksid põhjustada elukeskkonnale või looduskeskkonnale kahjulikke tagajärgi (nt veepuhastusprotsessi sekkumine ja kasutatavate kemikaalide koguste muutmine). Kuna kehtestatava seadusega lisandub ka muid uusi üksusi, mis peavad KüTSi nõudeid järgima, võimaldab see omakorda ennetada keskkondlikke õnnetusi, mis võivad kaasneda näiteks energeetikasektoris tegutsevate ettevõtete IT-süsteemidesse ebaseadusliku sisenemisega. Selle tagajärjel võidakse rivist välja lüüa olulised süsteemid, mis omakorda toovad kaasa energiatootmise vähenemise või täieliku peatumise. Uued KüTSi subjektid peavad rakendama oma võrgu- ja infosüsteemide kaitseks turvameetmeid, mis võimaldab vähendada selliste stsenaariumite tekkimise riski, mis võivad ühiskonna igapäevaelu pärssida. Selliste sündmuste tekkimise võimalus on väga väike.
Kokkuvõttes otsene mõju loodus- ja elukeskkonnale puudub, mistõttu pole mõju sihtrühmade kaupa välja toodud, kuid siiski peab riskide hindamisel sellega arvestama. Eeltoodu põhjal on muudatuse mõju ulatus, sagedus ja ebasoovitavate mõjude risk väike.

6.1.5. Mõju regionaalarengule
Muudatuste mõju regionaalarengule on väike ja pigem kaudne, seetõttu ei ole mõju sihtrühmade kaupa eraldi analüüsitud. Erasektori osutatavate teenuste kättesaadavus, mis tagatakse lisaturvameetmete kaudu, aitab kaasa ühiskonna toimimisele igas Eesti piirkonnas. Piirkondlik koostöö IT-turvalisust tagavate ettevõtetega võib suureneda, samuti võivad teoreetiliselt mõned töökohad juurde tekkida nii suurlinnadesse kui ka väiksematesse piirkondadesse, kuid mõju ei ole kindlasti märkimisväärne.
Eeltoodu põhjal on muudatuse mõju ulatus, sagedus ja ebasoovitavate mõjude risk väike.

6.1.6. Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele
Siinse muudatuse mõju sõltub mitmest asjaolust, sh sellest, kas tegemist on kehtiva KüTSi kohaldamisalasse kuuluva subjektiga või on tegemist uue subjektiga. Avalik sektor on juba praegu kehtiva KüTSi kohaldamisalas, mistõttu tehtavad muudatused ei ole neile niivõrd suur mõjuga. Siin võib olla tähtis ka konkreetse üksuse reaalne vastavus kehtestatavatele nõuetele, kuid seletuskirjas saab analüüsida ainult mõju nõuete muudatuste kontekstis.
Kehtiva KüTSi kohaldamisalasse kuuluva üksuse puhul ei ole muudatused märkimisväärsed, kuna ka KüTSi § 7 selgitustes on märgitud, et NIS2-direktiivi artikli 21 lõikes 2 sätestatud küberturvalisuse riskijuhtimismeetmed on samaväärsed nende nõuetega, mida näeb ette Eesti

[204] Vt: https://ria.ee/kuberturbe-nouanded/nouanded-internetikasutajale, https://ria.ee/kuberturbe-nouanded/nouanded-asutusele-ja-ettevottele, https://ria.ee/kuberturbe-nouanded/infomaterjalid-ja-kirjutised/kuberturvalisuse-infomaterjalid, https://www.itvaatlik.ee/ ja https://eits.ria.ee/.

infoturbestandard või rahvusvaheline standard ISO/IEC27001. Seetõttu ei too kommenteeritav muudatus kaasa suurt mõju riigiasutuste ja kohaliku omavalitsuse korraldusele. Muudatuste järgimine ei nõua asutuse töökorralduse muutmist ega töökoormuse olulist suurendamist või muid muudatusi.
Kehtestatavad küberturvalisuse riskijuhtimismeetmed mõjutavad järelevalveasutustest Riigi Infosüsteemi Ametit, kuna KüTSi lisanduvad uued üksused (ennekõike erasektorist, mitte avalikust sektorist), mida tuleb nõustada ning mille üle tehakse järelevalvet. See tekitab vajaduse palgata töötajaid juurde, millega omakorda kaasnevad lisakulud (vt seletuskirja järgmist peatükki). Samas saab Riigi Infosüsteemi Amet suurema ja selgema pildi küberturvalisuse tasemest Eestis. Julgeolekuasutusest järelevalveasutusele oluline mõju puudub, kuna nendele kehtivaid nõudeid ei muudeta.
Eeltoodu põhjal on muudatuse ulatus, sagedus ja ebasoovitavate mõjude risk väike.

6.2. Kavandatav muudatus: küberintsidentidest teatamise nõue

Muudatuse sisu on seotud NIS2-direktiivi artikliga 23, mis võetakse üle KüTSi §-dega 8 ja 12 – need sätted reguleerivad vastavalt kohustuslikku küberintsidendist teatamist ning Riigi Infosüsteemi Ameti tegevust ja volitusi teadete menetlemisel. Samas on muudatusega kaudselt seotud ka NIS2-direktiivi artikkel 30 (vabatahtlik küberintsidentidest teatamine), mis võetakse üle KüTSi §-ga 8^1.
Muudatusega täpsustatakse kehtivaid nõudeid: mis etapil millist infot ning mis aja jooksul tuleb esitada. Üldreegel jääb samaks: olulise mõjuga küberintsidendist või muust samaväärsest küberintsidendist tuleb teavitada hiljemalt 24 tundi pärast sellest teada saamist (esitada esmane teade). Täpsustatakse teavet, mis tuleb esitada küberintsidendi kohta esmase teatega, millal tuleb esmast teadet uuendada (esmase teate uuendus ehk intsidenditeade tuleb esitada 72 tundi pärast küberintsidendist teadasaamist), mida käsitatakse vahearuandes ning mis tähtajaks tuleb esitada küberintsidendi lahendamise lõppraport (kehtivas õiguses ei ole see kindlaks määratud, kuid NIS2-direktiiv sätestab siin konkreetsema tähtaja). Usaldusteenuse osutajate puhul tehakse erand – nad peavad esitama intsidenditeate 24 tunni jooksul.
Muudatus saab ennekõike mõjutada neid üksusi, mis lisanduvad KüTSi, kui neile juba mõni muu õigusakt (sh muu valdkondlik õigusakt) ei ole kehtestanud samalaadset teavituskohustust. Kehtiva KüTSi subjektidele need nõuded juba kohalduvad, mistõttu muudatus neid ei mõjuta. Lisaks kommenteeritavale muudatustele tuleb arvestada ka asjaoluga, et sarnane nõue on ka isikuandmete kaitse valdkonnas, mistõttu ei ole tegemist oma olemuselt uue nõudega KüTSi uutele subjektidele.[205]
Eelnõul puudub oluline mõju regionaalarengule ning muud otsesed või kaudsed mõjud.

6.2.1. Sotsiaalne, sealhulgas demograafiline mõju

Küberintsidendist teatamise nõude täpsustamine ei tekita ettevõtjale sotsiaalset mõju.
Kuna KüTSi subjektide arv suureneb, suureneb ka nende organisatsioonide arv, mis peavad olulise mõjuga küberintsidendist teavitama Riigi Infosüsteemi Ametit. See võimaldab aegsasti ja kiiresti tegeleda küberintsidendi lahendamisega. KüTSi subjektil võib tekkida vajadus teavitada ka isikut, keda olulise mõjuga küberintsident või oluline küberoht võib mõjutada; või avalikkust, kui mõjutatud isikuid ei ole võimalik eraldi teavitada. Teates annab üksus võimaluse korral teada olulisest küberohust ja meetmetest, mida mõjutatud isik saab olulisele küberohule reageerimiseks võtta (vt eelnõukohane KüTSi § 8 lõige 5). See suurendab ka inimeste teadlikkust küberohtudest

[205] Vt Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679, mis käsitleb füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta, artiklit 33 ja isikuandmete kaitse seaduse § 44.

ning nende võimalikest maandamise või ennetamise meetmetest – seda ka seetõttu, et sageli on küberintsidendid seotud isikuandmetega (nt toimub isikuandmete teatavaks saamine selleks õigustamata isikule). Seetõttu on teavitamisnõudel kaudne positiivne sotsiaalne mõju.
Isiku (sh isikuandmete kaitse valdkonna mõttes andmesubjekti) vaatest on muudatuse mõju ulatus pigem keskmine, kuna see võimaldab isikul parandada enda käitumist võrgu- ja infosüsteemide ning ka näiteks enda isikuandmete või muude digitaalse vara kaitsmisel, kui neile antakse teada, milliseid meetmeid on võimalik kasutusele võtta olulisele küberohule reageerimiseks. Muudatuse mõju sagedus on eelduslikult pigem väike, kuid ei ole välistatud, et see on ka kuni keskmine, kuna olulise mõjuga küberintsidentide arv on igal aastal suurenenud.[206] Kuna inimesed on üha enam teadlikud küberohtudest, siis on muudatusega seotud ebasoovitavate mõjude risk pigem väike.[207]

6.2.2. Mõju riigi julgeolekule ja välissuhetele
Muudatusel on positiivne mõju riigi julgeolekule ja välissuhetele, kuna küberintsidentidest teavitamine võimaldab tekkinud või tekkivate probleemidega kiiremini tegeleda nii riigisiseselt kui ka koostöös teiste riikidega. Muudatusega tõhustatakse olemasolevaid piiriüleseid koostöömehhanisme, et piiriüleseid küberintsidente lahendada, ning suurendatakse riikidevahelist koostööd, mis mõjutab mõneti ka piiriüleselt tegutsevaid ettevõtteid, kuna hõlbustab ning ühtlustab nõudeid, kuidas piiriüleseid küberintsidente lahendada.
Küberintsidentidest teavitamine võimaldab kindlaks teha ka küberohtudega seotud laiemat seisu, kuna küberohust võib välja kasvada olulise mõjuga küberintsident. Seetõttu on vaja teavitada küberintsidentidest, eriti olulise mõjuga küberintsidentidest.
Muudatuse kaudseks mõjuks on ka Eesti kui e-ühiskonna positiivse kuvandi edendamine, samuti suurendab see meie koostööd nii riigi tasandil riigi ja ettevõtete vahel kui ka rahvusvahelisel tasandil.
Muudatuse mõju ulatus lõppkokkuvõttes on pigem väike ning selle sagedus kuni keskmine. Kuna juba praegu toimub koostöö teiste riikidega ning muudatus aitab suurendada selgust piiriüleste küberintsidentide käsitlemisega seotud nõuetest, siis ebasoovitavate mõjude risk on väike.

6.2.3. Mõju majandusele
Muudatusel on positiivne mõju, kuna suureneb uute KüTSi subjektide teadlikkus vajadusest tegeleda küberintsidentide lahendamisega. Paraneb arusaam sellest, mis on üldse küberintsident ning mida tuleb teha, kui selline sündmus aset leiab. See aitab läbi mõelda ning õppustel ka läbi harjutada kriisis tegutsemist, konkreetsemalt küberintsidendi lahendamist.
Muudatuse tulemusena suureneb Riigi Infosüsteemi Ameti ja KüTSi uue subjekti vaheline suhtlus, kui see subjekt pole ise varem küberintsidentidest vabatahtlikult ametit teavitanud. Selle koormuse määra on keeruline analüüsida, kuna see sõltub omakorda sellest, mis on KüTSi uute subjektide küberturvalisuse riskijuhtimismeetmete rakendamise tase ning kuivõrd on üldse mõeldud küberintsidentidele või tegeldud nende haldusega.
Kuna KüTSi subjektide ring suureneb, võimaldab see saada ka laiema pildi ohtudest ja probleemidest, mis üksuste küberturvalisuse tagamisel esinevad, kuna samad probleemid või küberintsidendid võivad esineda ka muudes valdkondades.
Kui olulise mõjuga küberintsidendist teavitatakse Riigi Infosüsteemi Ametit, on ametil võimalik aegsasti reageerida teavitusele ning anda võimaluse korral ka vastus, mis sisaldab esialgset

[206] Riigi Infosüsteemi Amet. Küberturvalisuse aastaraamat 2025: https://www.ria.ee/veel-uks-rekordiaasta-mida-polnud-vaja.
[207] Vt: https://ria.ee/kuberturbe-nouanded/nouanded-internetikasutajale, https://ria.ee/kuberturbe-nouanded/nouanded-asutusele-ja-ettevottele, https://ria.ee/kuberturbe-nouanded/infomaterjalid-ja-kirjutised/kuberturvalisuse-infomaterjalid ja https://www.itvaatlik.ee/.

tagasisidet olulise mõjuga küberintsidendi kohta ja teavituse esitanud üksuse taotluse korral ka suuniseid olulise mõjuga küberintsidendi lahendamise meetmete rakendamiseks. See võimaldab intsidenti kiiremini lahendada. Lisaks sellele saab amet edastada ka küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid (vt kehtiva KüTSi § 12 lõige 3). Eeltoodu aitab saada ametil ka parema ülevaate küberturvalisuse tagamise seisust Eestis.
Analüüsitaval muudatusel koosmõjus eespool mainitud muudatusega (küberturvalisuse riskijuhtimismeetmete rakendamine) on eelduslikult ka positiivne mõju KüTSi uuele subjektile. Küberintsidendid on ebaregulaarsed sündmused, mille põhjustavad enamasti pahatahtlikud kolmandad isikud, seega ei saa ka ennustada, kui palju konkreetne üksus küberturvalisuse meetmete rakendamisest majanduslikult võidab või kaotab. Arvestades küberruumis aina sagedamini esinevaid rünnakuid[208] ning nende laastavat mõju ohvri süsteemide kasutatavusele, ei ole õigustatud vaadelda süsteemide turvalisuse tagamiseks tehtavaid kulutusi rangelt kahjuliku majandusliku mõjuna. Samas on positiivne see, kui KüTSi uued subjektid on aegsasti läbi mõelnud tegevused küberintsidendi haldamiseks, ning kui neid ka tehakse ning rakendatakse asjakohaseid ja ajakohaseid turvameetmeid, võimaldab see vähendada küberintsidendi esinemise tõenäosust.
Muudatusel on eelduslikult mõju majanduskeskkonnale, sh ettevõtlusele, kuna see tekitab teatava nõudluse küberturvalisuse tagamise valdkonnas pakutavate teenuste järele – konkreetsemalt küberintsidendi halduse ja lahendamise kontekstis. See omakorda võib suurendada ettevõtete arvu või olemasolevate ettevõtete osutatavate teenuste arvu – näiteks võib tekkida uusi konsultatsioonide, küberintsidendi lahendamisega seotud või küberintsidentide ennetusele suunatud koolitusteenuse osutajaid jm teenuseid. Siiski on muudatuse mõju ettevõtete toimimisele keeruline hinnata, kuna ei ole teada, kui palju uusi ettevõtteid võidakse nende teenuste osutamiseks luua või kui paljud ettevõtted võivad täiendada osutatavate teenuste nimekirja.

Muudatuse mõju ulatus seaduse jõustumise järel on keskmine, kuna muudatuse mõju avaldub ennekõike neile üksustele, kellest saavad siis teenuseosutajad (võrreldes kõikide üksuste arvuga, kellele muudatus hakkab edaspidi kohalduma). Muudatuse mõju sagedus võib olla kuni keskmine, kuna olenevalt poliitilistest või muudest asjaoludest võidakse üha enam sooritada ettevõtjate vastu erinevaid küberrünnakuid või nende katseid, millest tuleb või tasuks ka Riigi Infosüsteemi Ametit teavitada. Lõpptulemusena kujuneb muudatusest osa uute teenuseosutajate argitegevusest ja tööprotsessidest. Seda enam, et muudatusega seotud nõude täitmiseks on olemas asjakohased abimaterjalid ja selgitused, mil moel on ettevõtjal võimalik nii (olulise mõjuga) küberintsidentidest kui ka muudest küberohtudest teavitada Riigi Infosüsteemi Ametit.[209] Seetõttu on pikemas vaates muudatuse ebasoovitavate mõjude risk väike.

6.2.4. Mõju elu- ja looduskeskkonnale

Muudatused ei avalda otsest mõju elu- ja looduskeskkonnale, mistõttu nende mõju ulatus, sagedus ja ebasoovitavate mõjude risk on väike. Kaudselt võib positiivne mõju elu- ja looduskeskkonnale aga avalduda küberrünnakutele vastupanuvõime suurenemise kaudu, näiteks selliste intsidentide puhuks, mis saaksid põhjustada elu- või looduskeskkonnale kahjulikke tagajärgi (nt veepuhastusprotsessi sekkumise ja kasutatavate kemikaalide koguste muutmise või kemikaalide tootmisega seotud protsessidesse sekkumise korral). Selliste kahjulike tagajärgede tekkimise võimalust vähendab küberrünnakust ning selle põhjustatud küberintsidendist teada saamine,

[208] Riigi Infosüsteemi Ameti ööpäeva ülevaade Eesti küberruumi kohta: https://www.ria.ee/et/kuberturvalisus/olukord-kuberruumis/oopaeva-ulevaated.html.
[209] https://ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee/kuberintsidendist-teavitamine ja https://raport.cert.ee/.

mistõttu on küberintsidendist teatamise nõude täpsustamisel positiivne mõju. Intsidentidest teatamise korral on Riigi Infosüsteemi Ametil võimalik teatele aegsasti reageerida ning anda võimaluse korral esialgne tagasiside olulise mõjuga küberintsidendile ning teate esitanud üksuse taotluse korral ka suuniseid olulise mõjuga küberintsidendi lahendamiseks.

6.2.5. Mõju riigiasutuste ja kohaliku omavalitsuse korraldusele

Muudatusel ei ole otsest mõju KüTSi praegustest subjektidest riigiasutuste ja kohaliku omavalitsuse korraldusele, kuna nende puhul ei muutu kehtiv õigus niivõrd oluliselt. Muudatuse mõju ulatus ja ebasoovitavate mõjude risk on väike, kuna tegemist on juba tavapärase nõudega, mida tuleb järgida. Muudatuse mõju sagedus võib olla kuni keskmine, kuna olenevalt poliitilistest oludest või muudest asjaoludest võidakse üha enam sooritada ametiasutuste vastu küberrünnakuid või nende katseid, millest tuleb või tasuks ka Riigi Infosüsteemi Ametit teavitada.

Teatav mõju on Riigi Infosüsteemi Ametile kui järelevalveasutusele, ennekõike seetõttu, et KüTSi üksuste arv suureneb, samuti tegevuste hulk, mis on seotud edastatud küberintsidentide lahendamisega ametis. Seda enam, et NIS2-direktiivi alusel näeb KüTS ette, et amet annab olulise mõjuga küberintsidendi teadet saades teavitanud teenuseosutajale võimaluse korral 24 tunni jooksul vastuse, mis sisaldab esialgset tagasisidet olulise mõjuga küberintsidendi kohta ja teavitanud teenuseosutaja taotluse korral ka suuniseid olulise mõjuga küberintsidendi lahendamiseks. Riigi Infosüsteemi Ameti kodulehel ja eraldi portaalis on info, mil moel on võimalik küberintsidendist teatada.[210] IT-arenduse vajadust selleks praegu pole.

6.3. Kavandatav muudatus: teenuseosutaja juhatuse liikme kohustused

Muudatuse sisu on NIS2-direktiivi artiklis 20, mis on kavas võtta üle §-ga 6^1. Need kohustused on seotud organisatsiooni juhtorgani tasandil (st juhatuse liikme) suurema ja selgema rolli võtmisega küberturvalisuse tagamisel.

Ka NIS2-direktiivi algatuse[211] 7. lisas (finantsselgitused – ametid) on punktis 1.4.4 märgitud, milliste näitajate abil jälgitakse NIS2-direktiivi edusamme ja saavutusi. Üks neist (teine alapunkt) on ka seotud üksuse juhtkonna kohustustega:

1.4.4. Tulemusnäitajad

Näitajaid hindab komisjon ENISA ja koostöörühma toetusel kolm aastat pärast uue küberturvalisust käsitleva õigusakti jõustumist. Järgnevalt on loetletud mõned seirenäitajad, mille alusel küberturvalisuse alast edukust läbivaatamisel hinnatakse.

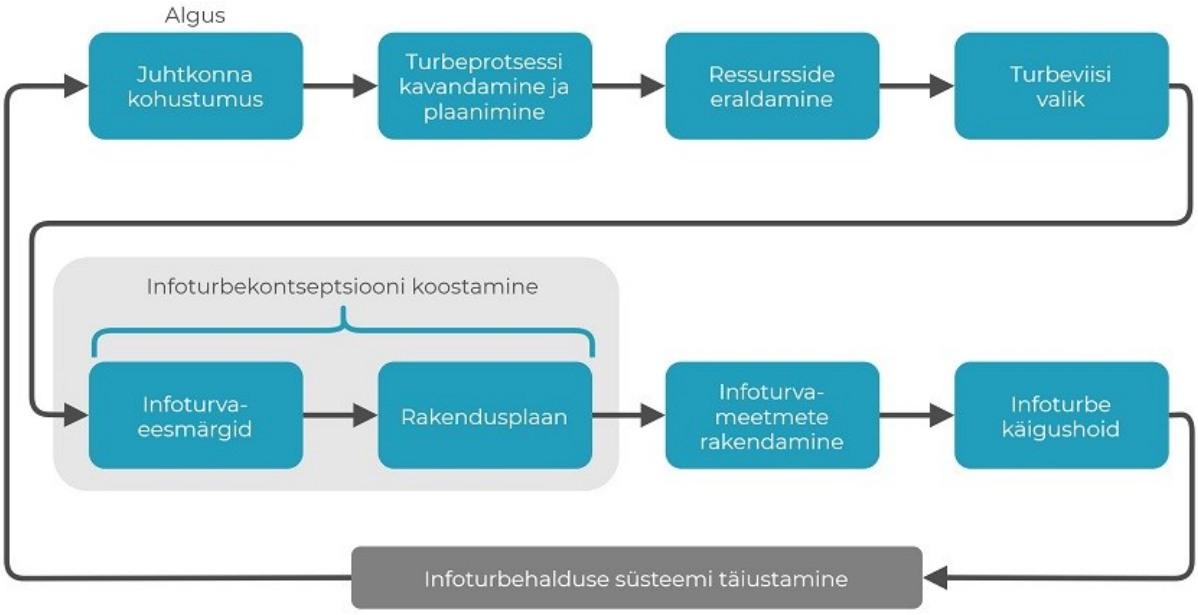
Ettevõtete tippjuhtkonna suurem teadlikkus küberturvalisusega seotud riskidest. Ettevõtjatelt meetmete võtmise nõudmise kaudu aitaks muudetud küberturvalisuse direktiiv suurendada tippjuhtkonna teadlikkust küberturvalisusega seotud riskidest. Seda saab mõõta, uurides, kuivõrd prioriseerivad küberturvalisuse raamistikuga hõlmatud ettevõtjad küberturvalisust oma ettevõtte sise-eeskirjades ja -protsessides (mida tõendavad ettevõtte sisedokumendid, asjakohased koolitusprogrammid ja töötajate teadlikkuse suurendamiseks võetavad meetmed) ning seda, kuivõrd prioriseeritakse küberturvalisusse tehtavaid IKT-investeeringuid. Kõigi elutähtsate ja oluliste üksuste juhtkond peaks samuti olema teadlik küberturvalisuse direktiivis sätestatud eeskirjadest.

Muudatus laieneb nii praegustele kui ka uutele KüTSi subjektidele, kuid selle muudatuse mõju on suurem neile üksustele, mis alles saavad KüTSi subjektiks, sest see on seotud turvameetmete heakskiitmise ja nende rakendamise jälgimisega. KüTSi § 6^1 lõikes 1 sätestatud nõuded on

[210] Vastavalt https://ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee/kuberintsidendist-teavitamine ja https://raport.cert.ee/.

[211] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020PC0823

samaväärsed, mis on näiteks ette nähtud Eesti infoturbestandardi osaks oleva infoturbe halduse süsteemi[212] protsessiga – selle sammud on tolle dokumendi peatükis 4.1 oleva joonise nr 1 kohaselt (seletuskirjas joonis nr 3) järgmised:



Joonis 3. Infoturbe halduse süsteemi käivitamise ja uuendamise tegevused

Eesti infoturbestandardi võrgulehel olev asjakohane vastavustabel[213] kinnitab, et joonise sisu on nõuete mõttes sama, mille näeb ette ka rahvusvaheline standard ISO/IEC 27001.
Kehtiva KüTSi subjektide puhul on juhtorgani liikmetel sama nõue juba seetõttu, et neile kohaldub kas Eesti infoturbestandard või selle alternatiiviks olev rahvusvaheline standard ISO/IEC 27001. Valitsusasutuste (mis on kehtiva õiguse kohaselt KüTSi subjektid) puhul on samalaadne nõue ka Vabariigi Valitsuse 15.03.2012. a määruse nr 26 „Infoturbe juhtimise süsteem“ §-s 3. Seetõttu ei ole muudatusel nendele üksustele olulist mõju. Kui mõnele nendest üksustest avaldub oluline mõju, siis on see seotud kehtivate nõuete täitmata jätmise, mitte muudatusega.
Lisaks infoturbe halduse süsteemi kui juhtimisprotsessi tagamisele on muudatuse mõju seotud ka juhtorgani liikme enda koolitamisega ehk ta peab käima asjakohatel koolitustel. Koolituste sisu ehk siis ootused, mida korraldatavad koolitused peaksid sisaldama, on kirjeldatud KüTSi § 6[1] selgitustes, mida siin ei korrata.
Muudatusel on mõningane mõju sotsiaalsest vaatenurgast, sh töösuhete kontekstis, kuid samuti kõigile KüTSi subjektidele (nii praegustele kui ka uutele). Kaudselt avaldub sel teel mõju ka riigi julgeolekule. Nimetatud mõjud on positiivse loomuga.
KüTSi uute subjektide puhul on infoturbe halduse süsteemi kui protsessi tagamisega seotud juhtorgani liikme ülesanded positiivse mõjuga, kuna annavad juhtorgani liikmele parema selguse, milliseid varasid (nt infosüsteeme, andmeid, intellektuaalomandit ja muid ärisaladusi jne) kaitstakse. KüTSi subjekt saab soovi korral planeerida ja arendada uusi teenuseid, mille vajadus olemasolevate äriprotsesside ja teenuste kaardistamise järel ilmneb. Samuti ei ole välistatud, et

[212] Infoturbe halduse süsteem (ingl *Information Security Management System*, ISMS) on organisatsiooni juhtimise osa, mis tegeleb infoturbe rajamise, evitamise, käigushoiu ja pideva täiustamisega. Allikas: https://eits.ria.ee/et/versioon/2023/eits-poohidokumendid/eits-noouded-infoturbe-halduse-suesteemile, peatükk 4.1.
[213] Eesti infoturbestandardi võrguleht. Juhendid ja näidised. Vastavustabelid. Allikas: https://eits.ria.ee/et/avalehe-menueue/juhendid.

kaardistamise järel leitakse ka optimeerimise võimalusi, mis võivad subjekti kulu vähendada. Kuna KüTSi lisanduvad üksused on erineva profiili ja tegevusalaga, siis ei ole siinses analüüsis võimalik ega mõistlik hinnata eri valdkondade võimalikke kokkuhoiuga seotud mõjusid.
Koolitusnõudega tagatakse, et ühiskonnas suureneb teadlikkus küberturvalisuse valdkonnast ning selle tagamise vajadusest, samuti inimeste teadlikkus nii küberohtudest ning nende võimalikest maandamise või leevendamise meetmetest kui ka nendega tegelemise vajadustest. Kaudselt suureneb ka inimeste teadlikkus isikuandmete kaitse valdkonnast, kuna mõned küberohud on seotud isikuandmetega, mida on tarvis kaitsta.

Muudatusel on eelduslikult mõju ka majanduskeskkonnale ja ettevõtlusele, kuna tekib teatav nõudlus küberturvalisuse tagamise valdkonnas pakutavate konsultatsioonide ja koolituste ning teenuste järele. See omakorda võib suurendada ettevõtete arvu või olemasolevate ettevõtete osutatavate teenuste hulka. Praegu ei ole teada, kui palju uusi ettevõtteid võidakse koolitusteenuste pakkumiseks luua või kui paljud olemasolevad ettevõtted võivad täiendada oma koolitusteenuseid. Samalaadne positiivne mõju võib ilmneda ka haridussektoris, kui mõni õppeasutus soovib pakkuda näiteks koolitusi juhtorgani liikmetele või ka KüTSi subjektiks olevatele ametnikele ja töötajatele. Kaudne mõju on seotud riigi julgeolekuga, sest mida teadlikumaks muutub tööandja küberturvalisuse tagamise vajadusest, seda paremini on hoitud ja tagatud ühiskonna toimimine. See omakorda aitab tagada seda, mis on ette nähtud Eesti julgeolekupoliitika alustes (vt seletuskirja punkt 6.1.2.).
Eesti infoturbestandardi suunised ja juhendid on asjakohases portaalis, vt https://eits.ria.ee/et/avalehe-menueue/koolitusvideod, https://eits.ria.ee/et/avalehe-menueue/juhendid, https://eits.ria.ee/et/avalehe-menueue/kogukond ja https://eits.ria.ee/et/avalehe-menueue/suendmused. Küberturvalisuse veebikoolitusi pakub Digiriigi Akadeemia (https://digiriigiakadeemia.ee/) kuhu on peatselt lisandumas ka koolitusmaterjal, mida saaks kasutada ka kommenteeritava muudatuse ehk koolitusnõude täitmiseks.
Muudatusel puudub oluline mõju elu- ja looduskeskkonnale, regionaalarengule, muud otsesed või kaudsed mõjud.
Muudatuse mõju ulatus on keskmine seaduse jõustumise järel, kuna muudatus puudutab ennekõike neid üksusi, mis saavad KüTSi teenuseosutajateks (võrreldes kõikide üksuste arvuga, kellele siinne muudatus hakkab edaspidiselt kohalduma). Mõju sagedus on keskmine samuti seaduse jõustumise järel, kuid pärast muutub nõude täitmine igapäevase tööprotsessi osaks. Seda enam, et muudatusega seotud nõude täitmiseks on olemas või peatselt tulemas asjakohased abimaterjalid. Seetõttu on pikemas vaates muudatuse ebasoovitavate mõjude risk väike.

6.4. Kavandatav muudatus: järelevalveasutuse teavitamine üksuse andmetest

Muudatus on seotud NIS2-direktiivi artikli 3 lõike 4 ja artikli 27 lõike 2 täitmisega, mis võetakse üle KüTSi § 3^1 lõikega 1 ja § 4 lõikega 1.
Kohustus mõjutab KüTSi subjekti ja Riigi Infosüsteemi Ameti koormust. Inimestele siin lisatööd ei kaasne.
Mõlema kohustuse sisu on samalaadne – KüTSi subjekt (nii praegune kui ka uus) annab Riigi Infosüsteemi Ametile teada oma andmetest. Eelnõu koostamisel ei analüüsitud, kas teavitada on võimalik ka mõnd IT-lahendust kasutades ning lähtudes andmete ühekordse küsimise põhimõttest ja riigi andmekogudes olevate andmete taaskasutamisest, kuid edaspidi tasub seda kaaluda. Seda enam, et tegemist ei ole n-ö ühekordse kohustusega, vaid kui mingites andmetes on toimunud muudatusi, tuleb nendest ka ametit ettenähtud tähtajal teavitada. Tähtaja pikkus sõltub sellest, kas tegemist on teenuseosutaja, digitaalse teenuse osutaja või domeeninimede registreerimise

teenuseid osutava üksusega. Eelduslikult ei tehta nendes andmetes muudatusi sageli, mistõttu tegemist ei ole kohustusega, mida tuleb liiga tihti täita. Seetõttu on muudatuse mõju väike, kuna andmeid tuleb uuesti esitada siis ja ainult selles ulatuses, kui palju on varem teavitatud andmed muutunud.
Esitatavate andmete maht ei ole suur ega nõua üksustelt ülemääraseid pingutusi. Seetõttu on muudatuse mõju ulatus ja sagedus väike. Samuti on muudatuse ebasoovitavate mõjude risk väike. Samuti on Euroopa Komisjon koostanud suunised, kuidas nimetatud kohustust täita – need leiab komisjoni teatisest „Komisjoni suunised direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) artikli 3 lõike 4 kohaldamise kohta 2023/C 324/02“.[214]
Muudes valdkondades muudatus olulist mõju ei avalda, mistõttu pole mõjusid sihtrühmade kaupa eraldi välja toodud.

6.5. Kavandatav muudatus: pädevate asutuste ja ülesannete määramine

NIS2-direktiivi mitu artiklit näevad ette pädevate asutuste ja nendele ülesannete määramise. Need võetakse üle KüTSi §-s 5 tehtavate täiendustega, samuti Justiits- ja Digiministeeriumi põhimääruse ning Riigi Infosüsteemi Ameti põhimääruse täiendamisega. NIS2-direktiivi artikkel 19 (vastastikune hindamine) ei täpsusta lõplikult, kes valitsusasutuste mõttes peab teatavaid ülesandeid täitma, mistõttu on KüTSi täiendatud §-ga 17^6 ning selles oleva volitusnormi alusel tuleb anda määrus vastastikuse hindamisega seotud täpsemate tingimuste ja korra kehtestamiseks. Delegeeritud määruse (EL) 2024/1366 artikli 4 lõige 1 näeb ette ka vajaduse täpsustada pädevat asutust riigi tasandil, mistõttu selle määramisega seotud volitusnorm võetakse üle KüTSi §-ga 5^2.
Nimetatud õigusaktides määratakse ülesanded ja volitused Vabariigi Valitsusele, Justiits- ja Digiministeeriumile, julgeolekuasutustele ning Riigi Infosüsteemi Ametile, sh viimase osaks olevale küberintsidentide käsitlemise üksusele. KüTSi §-s 5 selgituses märgitakse, miks on vaja ülesannete sisu (millega näiteks mainitud valitsusasutused juba tegelevad) eraldi sätestada. Seetõttu seda siin ei korrata. Samad põhjendused on mainitud põhimääruste muudatuste korral.
Muudatus mõjutab ennekõike riigiasutuste korraldust. Muudes valdkondades muudatus olulist mõju ei avalda, mistõttu pole mõjusid sihtrühmade kaupa eraldi välja toodud.
Vabariigi Valitsusele antav ülesanne (küberturvalisuse strateegia vastuvõtmine) ei ole olulise mõjuga ülesanne, kuna sellega seotud põhitöö ehk koordineerimise ülesanne on Justiits- ja Digiministeeriumil. Küberturvalisuse strateegia võetakse tavaliselt vastu digiühiskonna arengukava osana, selle uuendamine on plaanis 2025. aastal.
Mitu seaduses sätestatud ülesannet on sellised, millega nii Riigi Infosüsteemi Amet kui ka Justiits- ja Digiministeerium tegelevad praegugi kehtiva õiguse kohaselt. Seetõttu ei ole vaja nende ülesannete mõju analüüsida. Mõningane mõju võib Riigi Infosüsteemi Ametile kaasneda KüTSi lisanduvate üksuste tõttu, kuid see on seotud olemasolevate ülesannete suuremas mahus täitmisega, mitte niivõrd uute ülesannetega. KüTSi lisanduvaid subjekte saab näiteks nõustada ning nende üle tehakse järelevalvet. See tekitab vajaduse lisatööjõu järele, millega omakorda kaasnevad lisakulud (vt ka seletuskirja järgmist peatükki).
Vastastikuse hindamisega seotud ülesanded ja nende maht sõltub ennekõike asjaolust, kas Eesti soovib üldse osaleda NIS2-direktiiviga ette nähtud vastastikuses hindamises. Seetõttu ei ole eeldatavasti siin olulist mõju ei Justiits- ja Digiministeeriumile, Riigi Infosüsteemi Ametile ega ka muudele küberturvalisuse valdkonna ekspertidele, keda võidakse kaasata selle ülesande täitmisesse.
Julgeolekuasutusest järelevalveasutusele oluline mõju puudub, kuna tehtava muudatuse põhisisu on nende puhul olemas kehtivas õiguses ning siin sisulisi täiendusi või muudatusi ei tehta, vaid

[214] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0914%2801%29&qid=1748949142248.

muudatus on selguse loomiseks NIS2-direktiivi kontekstis.
Delegeeritud määruse (EL) 2024/1366 artikli 4 lõike 1 kohase ülesande andmine käskkirjaga Riigi Infosüsteemi Ametile ei too samuti kaasa olulist mõju, kuna ametil on praegu vajalik pädevus samas sektoris (piiriüleste energiavoogudega seotud ettevõtted) olemas. Kui muudatust ei tehtaks, oleks delegeeritud määruse (EL) 2024/1366 artikli 4 kohaselt nimetatud ülesande täitjaks Eestis Konkurentsiamet, kuid selle asutuse sobimatust on selgitatud KüTSi § 5^2 juures.
Muudatuse kaudne positiivne mõju avaldub selle kaudu, et õigusaktide tasandil on täpsemalt määratud või sätestatud volitusnormid, mille järgi määratakse valitsusasutused, mis tegelevad NIS2-direktiivi asjakohaste artiklite ja delegeeritud määruse (EL) 2024/1366 artikli 4 tähenduses küberturvalisuse valdkonnaga.
Seaduse ja sellega seotud rakendusaktidega tehtavate muudatuste mõju ulatus ning ebasoovitavate mõjude risk on väike, kuna mainitud valitsusasutused tegelevad kehtiva õiguse alusel suuremal või vähemal määral samade ülesannetega, mis on sätestatud muudetavas seaduses. Riigi Infosüsteemi Ametil, ennekõike kohe pärast seaduse jõustumist, tuleb olemasolevaid ülesandeid täita suuremas mahus kui varem, seega on muudatuse mõju mainitud ajal sage.

7. Seaduse rakendamisega seotud riigi ja kohaliku omavalitsuse tegevused, eeldatavad kulud ja tulud

Siinses peatükis analüüsitakse tegevusi, sh eeldatavaid kulusid, mida seadusemuudatused võivad kaasa tuua.
Delegeeritud määruse (EL) 2024/1366 artikkel 11 reguleerib kulude hüvitamist. Selle sisu on:
1. Iga liikmesriigi asjaomane reguleeriv asutus hindab käesolevas määruses sätestatud kohustustest tulenevaid kulusid, mida kannavad põhi- ja jaotusvõrguettevõtjad, kelle suhtes kohaldatakse võrgutariifide reguleerimist, sealhulgas kulusid, mida kannavad Euroopa elektri põhivõrguettevõtjate võrgustik ja ELi jaotusvõrguettevõtjate üksus.
2. Mõistlikuks, tõhusaks ja proportsionaalseks hinnatud kulud kaetakse võrgutariifide või muude asjakohaste mehhanismide kaudu, mille määrab kindlaks asjaomane riigi reguleeriv asutus.
3. Kui asjaomased riigi reguleerivad asutused seda nõuavad, esitavad lõikes 1 osutatud põhi- ja jaotusvõrguettevõtjad riigi reguleeriva asutuse määratud mõistliku aja jooksul teabe, mida on vaja, et tekkinud kulusid hõlpsamini hinnata.
Reguleerivaks asutuseks on asutus direktiivi (EL) 2019/944 artikli 57 lõike 1 tähenduses. Eestis on reguleeriv asutus Konkurentsiamet, mille ülesanded tulenevad delegeeritud määrusest (EL) 2024/1366, mistõttu selle määrusega seotud mõjusid ja kulusid siin pikemalt ei analüüsita.
NIS2-direktiivi algatuse[215] 7. lisa (finantsselgitus – ametid) punktis 1.4.3 on selgitatud direktiivi oodatavaid tulemusi ja mõjusid. Järgnev väljavõte käsitleb avaliku sektori, samuti uute üksuste kuludega seotut (eeldatavasti on mõeldud uute üksuste kulude kontekstis ettevõtjate kulude mõttes ka avaliku sektori üksuste kulusid):
1.4.3. Oodatavad tulemused ja mõju
Ettepaneku elluviimine tähendaks asjaomaste liikmesriikide ametiasutustele ka teatavaid nõuete järgimise ja täitmise tagamisega seotud kulusid (hinnanguliselt suureneb ressursivajadus kokku ligikaudu 20–30 %). Samas tooks uus raamistik märkimisväärset kasu ka selle kaudu, et tagaks olulistest ettevõtjatest parema ülevaate ja nendega tõhusama suhtlemise, tulemuslikuma piiriülese operatiivkoostöö ning vastastikuse abistamise ja vastastikuse hindamise mehhanismid. Selle tulemusena tõuseks liikmesriikide küberturvalisuse alase suutlikkuse üldine tase.
Küberturvalisuse raamistiku kohaldamisalasse hõlmatavad ettevõtjad peaksid esimestel aastatel pärast küberturvalisuse raamistiku jõustumist suurendama oma IKT-turbega seotud kulutusi

[215] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52020PC0823.

maksimaalselt 22 % võrra (need ettevõtjad, kes juba kuuluvad [küberturvalisuse direktiivi (EL) 2016/1148] kohaldamisalasse, 12 % võrra). IKT-turbega seotud kulutuste keskmine suurenemine tooks samas kaasa proportsionaalse investeeringukasu, eelkõige tänu küberturvalisuse intsidentidega seotud kulude märkimisväärsele vähenemisele (hinnanguliselt 118 miljardit eurot kümne aasta jooksul).
Väike- ja mikroettevõtjad jäetaks küberturvalisuse raamistiku kohaldamisalast välja. Keskmise suurusega ettevõtjate IKT-turbega seotud kulutused esimestel aastatel pärast uue küberturvalisuse raamistiku kasutuselevõttu eelduste kohaselt suurenevad. Samas soodustaks nende üksuste turvanõuete taseme tõstmine ka nende küberturvalisuse alase suutlikkuse suurenemist ja aitaks tõhustada nende IKT-alast riskijuhtimist.
Oodatav mõju liikmesriikide eelarvetele ja haldusasutustele: lühikese ja keskpika perspektiivi prognoosi kohaselt suureneb ressursivajadus hinnanguliselt ligikaudu 20–30 %.
Eeltoodud hinnangu puhul tuleb arvestada asjaoluga, et direktiivi (EL) 2016/1148 kohaldamisalas ei olnud avalikku sektorit. Kui Eesti tolle direktiivi üle võttis, lisati ka avalik sektor (tollases sõnastuses: riigi ja kohaliku omavalitsuse üksus) KüTSi kohaldamisalasse. Samuti tuleb arvestada, et avalikule sektorile kehtisid juba toona ning kehtivad praegugi KüTSis nõuded, mis on võrreldavad NIS2-direktiivi nõuetega (nt turvameetmete nõuded). Seetõttu ei ole seadusel ka näiteks eeldatavat mõju kohaliku omavalitsuse üksuste eelarvetele, kuna tegemist on kehtiva KüTSi subjektiga ning muudatused ei ole sedavõrd olulised, et neid siin analüüsida.

Ka NIS2-direktiivi algatuse kohta koostatud Eesti seisukohtades (eelnõude infosüsteemi toimik 20-3668, 18.02.2021. a kirjas olev fail „Seletuskiri_MKM.pdf“)[216] on lk-del 10 ja 11 märgitud:
„Ministeeriumid ning riigiametid peavad hakkama järgima [NIS2-direktiivist] tulenevaid kohustusi. Kuigi Eesti riigiasutuste küberturvalisus ületab praegugi EL-i poolt sätestatud miinimumstandardit, siis hiljutised küberrünnakud riigiasutuste suunal näitavad, et täielikku kindlust küberrünnete vastu ei ole võimalik saavutada, kuid parem ülevaade infosüsteemidest aitab probleeme ära hoida. Üldiselt võib eeldada, et [NIS2-direktiivi] laienemine avalikule sektorile toob suurema kasuteguri kaasa nendele [liikmesriikidele], kus konkreetseid meetmeid riigiasutuste küberturbele ette nähtud ei ole. [...]
Kuna ka avaliku sektori asutused kuuluvad [NIS2-direktiivi] subjektide hulka, siis eeldab komisjon, et avaliku sektori IKT-kulutused tõusevad praeguse EL-i keskmise 4% pealt 4,88% peale. [Riigi Infosüsteemi Ameti] hinnangul oleks riigiametitel ning ministeeriumitel praeguse infoturbealase inimressursiga võimalik direktiivist tulevad miinimumülesanded ära täita, kuid nendib, et pikas perspektiivis tuleks kõikides kõnealustes asutustes infoturbe ekspertide koosseisu laiendada.“
Eelnõuga ei prognoosita tulusid.

7.1. Vabariigi Valitsus ning Justiits- ja Digiministeerium

Valitsuse tasandi tegevused on seotud riikliku küberturvalisuse strateegiaga, mis kinnitatakse digiühiskonna arengukava osana. Arengukava peamine ettevalmistaja on Justiits- ja Digiministeerium. Digiühiskonna arengukava on plaanis muuta 2025. aastal.
Justiits- ja Digiministeeriumi ülesannetena sätestatakse osalemine NIS2-direktiivi artiklis 14 nimetatud koostöörühma ja artiklis 16 sätestatud võrgustiku töös koos Riigi Infosüsteemi Ametiga. Need ülesanded lisatakse mõlema valitsusasutuse põhimäärusesse. Ministeerium täidab neid ülesandeid juba praegu, mistõttu ei tohiks need tekitada lisakulutusi. Kui neid peaks siiski tekkima, analüüsitakse neid riigieelarve planeerimise protsessis.

[216] https://eelnoud.valitsus.ee/main/mount/docList/5c847e1d-42e5-46f8-99d8-d21d144bca61.

7.2. Riigi Infosüsteemi Amet

Riigi Infosüsteemi Ameti tegevused on seotud KüTSi uute subjektidega lisandumisega ning ennekõike nende nõustamise ja järelevalvega. Osa ülesandeid – üksuste kohta käivate andmete saamine, nende täpsustamine ja asjakohasel juhul edastamine Euroopa Liidu Küberturvalisuse Ametile või Euroopa Komisjonile jms – on seotud kõigi KüTSi subjektidega. See nõuab nii lisatööjõudu kui ka -raha.

NIS2-direktiivi algatuse kohta koostatud Eesti seisukohtades (eelnõude infosüsteemi toimik 20-3668, 18.02.2021. a kirjas olev fail „Seletuskiri_MKM.pdf“)[217] on sedastatud, et NIS2-direktiiv suurendab Riigi Infosüsteemi Ameti töökoormust koos pikemas perspektiivis vajadusega laiendada ameti koosseisu. Seisukohtades (lk 11) on märgitud:

Vastastikuste hindamiste praktika ning EL-i uue küberkriisihalduse mehhanismi rakendamine aitavad tõsta usaldust [liikmesriikide] vahel valdkonnas, kus riikliku julgeoleku tagamise põhimõttel ollakse tihtipeale teabevahetuse küsimustes ettevaatlikud. Eelmainitud uuendused ning [Euroopa Liidu Küberturvalisuse Ameti] hallatav turvanõrkuste register aitavad [liikmesriikidel] enda töö kvaliteeti tõsta, kasutamata olulisi rahalisi lisaressursse. Kuid tõenäoliselt toovad [liikmesriikidele] kaasa halduskoormuse ning rahaliste kulude tõusu mitmed teised muutused direktiivis, nagu seda on turvanõuete täitmise jälgimise kohustus ning üldine järelevalveprotseduur, tihe raporteerimise nõue ja üksustele suhtlusplatvormide loomine. Komisjon hindab sellega seonduvat (inim- ja rahaliste) ressursside kasvu riiklikele pädevatele asutustele 20-30%. CSIRTide koormus peaks tõusma 10-15%.

[Riigi Infosüsteemi Amet] hindab lisanduvate kohustuste täitmise ja lisanduvate subjektide üle teostatava järelevalvevõimekuse teostamiseks oleks hinnanguliselt vaja lisaks kolme järelevalveametnikku ning ühte riskijuhti. Järelevalve täiendavad vajadused peegelduvad järgnevalt: 4x (54 000€ palgafond ning 9000€ töökoha kulud) ja ca 5000€ muud majandamise kulud, s.o 275 000 eurot aastas. Seoses lisanduvate subjektidega laienevad ka [Riigi Infosüsteemi Ameti] kriitilise taristu infoturbe tööülesanded, mille katmiseks läheks vaja kahte eksperti lisaks. Kriitilise taristu infoturbe vajadused peegelduvad järgnevalt: 2x (54 000€ palgafond ja 9000€ töökoha kulud) ning 3000€ muud majandamise kulud, s.o 120 000 eurot aastas.

[NIS2 direktiiv] tooks ka lisakoormust [Riigi Infosüsteemi Ameti] CERT-ile, kehtestades oluliselt konkreetsemad nõuded IKT toodete turvanõrkuste koordineeritud avalikustamisele, kõrgkäideldavusele, küberohtude ja haavatavuse seirele (sh proaktiivne seire, teavitustööl ning tehniliste analüüside koostamine (direktiivi artikkel 6 ja artikkel 10)), mille katmiseks läheks vaja 4 küberturbe eksperdi ametikohta. Sellega seoses hindame CERT-EE täiendavaid vajadusi järgnevalt: aastane palgakulu – 4x (72250€ palgakulu ning 9000€ töökoha kulud) 325 000 eurot; aastane majanduskulu - 235 000 eurot; aastane investeeringute kulu - 185 000 eurot.

NIS koostöögrupi mandaadi tugevnemisega seotud ülesandeid, sh riskianalüüside EL-i tasemel koordineerimine, saab [Riigi Infosüsteemi Ameti] analüüsi- ja ennetusosakond olemasoleva inimressursiga tõenäoliselt ära katta. Kokku tooks [NIS2 direktiivi] rakendamine [Riigi Infosüsteemi Ametile] aastaseid lisakulusid riigieelarvesse 1 140 000 euro ulatuses. Viidatud kulusid menetletakse tulevikus vastavalt riigi majanduslikele võimalustele vastavate aastate riigi eelarvestrateegia ja riigieelarve protsessis. Antud tegevustele saab lisada ka projektipõhiseid arendusi, millele saaks rahastust taotleda Digitaalse Euroopa rahastust – nagu seda on praegu tehtud Euroopa Ühendamise rahastust[218].

Nende arvnäitajate puhul tuleb arvestada, et tegemist on 2021. aastal koostatud hinnanguga. Samuti

[217] https://eelnoud.valitsus.ee/main/mount/docList/5c847e1d-42e5-46f8-99d8-d21d144bca61.

[218] Seletuskirjas oli viide nr 14 tekstiga: *Allikas: https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme.*

tuleb arvestada, et praeguseks on Riigi Infosüsteemi Ametisse juba lisandunud uusi teenistuskohti. Kuni 31.12.2024 oli riikliku küberturvalisuse valdkond Majandus- ja Kommunikatsiooniministeeriumi valitsemisalas. 24.05.2024 taotles Majandus- ja Kommunikatsiooniministeerium Rahandusministeeriumilt Vabariigi Valitsuse reservi sihtotstarbelistest vahenditest raha eraldamist summas 297 332 eurot Riigi Infosüsteemi Ameti halduskulude (tööjõukulude) katteks 2024. a eelarves.[219] Rahavajaduse tingis NIS2-direktiivi ülevõtmisega seotud lisanduvate kohustuste täitmine. Rahandusministeerium tagastas 09.10.2024 taotluse soovitusega leida selleks võimalus Majandus-. Ja Kommunikatsiooniministeeriumi 2023. aasta ülekantud jääkide arvelt.[220] Kuna küberturvalisuse valdkond, sh Riigi Infosüsteemi Amet, liikus 2025. aastal Justiits- ja Digiministeeriumi valitsemisalasse, tuleb tagada eelarve olemasolu riigieelarve planeerimise käigus või esitades taotluse Rahandusministeeriumile Vabariigi Valitsuse reservi sihtotstarbelistest vahenditest raha eraldamiseks. Muudatustega seotud Riigi Infosüsteemi Ameti kulude suurus on vähemalt sama, mis oli 2024. aasta mais Rahandusministeeriumile esitatud taotluses. Kui mingil põhjusel on vaja lisaressursse, analüüsitakse seda eelarve planeerimise käigus.

7.3. Julgeolekuasutus

Julgeolekuasutustena on mõeldud Kaitsepolitseiametit ja Välisluureametit. Kuna julgeolekuasutustele kui järelevalveasutustele ei lisandu järelevalvatavaid, ei suurene nende töökoormus ega teki neil märkimisväärseid kulutusi. NIS2-direktiiviga ette nähtud meetmete rakendamisega (näiteks turvameetmete nõuded) seotud tegevused ja kulutused on isegi väiksemad võrreldes teiste KüTSi kohaldamisalas olevate üksustega, kuna KüTSi ei kohaldata riigisaladuse ja salastatud välisteabe töötlemisele ning sellise teabe töötlussüsteemide pidamisele.

7.4. Muu tugi, koolitus ja toetused

Siinses alapeatükis antakse ülevaade valitsusasutuste ja nende valitsemisalas olevate asutuste tegevustest (sh toetustest), mis aitavad siinse eelnõu ellu viimist ja rakendamist.

Justiits- ja Digiministeerium on ette valmistamas toetusmeedet KüTSi subjektidele ja ka muudele huvitatud osalistele, et neil oleks võimalik viia end vastavusse küberturvalisuse tagamise nõuetega (vt ka allpool olevat küberturvalisuse taseme kaardistamise ja arendamise toetust, mis on selle meetme eeskujuks). Meedet rahastab Eesti riik.

Riigi Infosüsteemi Ameti teenistujate osalusel on arendamisel Eesti infoturbestandardi järgimiseks tugirakendus, mis aitab rakendajal luua enda vajaduste põhjal turvameetmete rakendusplaani, seejuures vähendada vigade teket meetmete valimisel, ja suunab rakendaja kohe meetmete rakendamisele. Peamine eesmärk on vähendada Eesti infoturbestandardi rakendamise protsessi keerukust. See on interaktiivne rakendusjuhend, mis aitab läbida infoturbehalduse protsessi teatud samme ning annab võimaluse püsida standardi kataloogi uuendustega pidevalt kursis. Seejuures säilib siiski kogu standardi olemus ning meetmetes järeleandmisi ei tehta – küberruumi olukord nõuab vähemalt põhimeetmete rakendamist, NIS2-direktiivi artikli 21 nõuded on seejuures kõikehõlmavad. Riigi Infosüsteemi Amet ei hakka organisatsioonide turvet haldama ega hoidma haldamise teavet. Amet tegeleb standardi arendamisega ja püüab leida lahendusi, et aidata rakendajal leida Eesti infoturbestandardist oma organisatsioonile võimalikult ressursse säästvalt õiged meetmed, neid rakendama ja haldama peab KüTSi subjekt oma tööriistadega. Eesti infoturbestandardi tugirakenduse leiab siit: https://eits.ria.ee/et/abimaterjalid/tugirakendus. Eesti infoturbestandardi juhendid on asjakohases portaalis, vt https://eits.ria.ee/et/avalehe-menueue/koolitusvideod, https://eits.ria.ee/et/avalehe-menueue/juhendid,

[219] https://adr.rik.ee/mkm/dokument/15462072
[220] https://adr.rik.ee/mkm/dokument/16109492

https://eits.ria.ee/et/avalehe-menueue/kogukond ja https://eits.ria.ee/et/avalehe-menueue/suendmused.
Asjakohaseid veebikoolitusi pakub ka Digiriigi Akadeemia (https://digiriigiakadeemia.ee/), kuhu on lisandumas koolitusmaterjal, mida saaks kasutada KüTSi § 6[1] kohase koolitusnõude täitmiseks. Lisaks on ettevalmistamisel infoturbe audiitorite järelkasvu koolitused.

Kuni 2024. a septembrini oli Riigi Infosüsteemi Ametil koostöös Ettevõtluse ja Innovatsiooni Sihtasutusega avatud toetusmeede, mis aitas Eesti väike- ja keskmise suurusega ettevõtjatel välise nõustaja kaasabil selgitada välja oma IT-süsteemide küberturvalisuse tase ja teha vajalikke arendusi selle tõstmiseks, et kaitsta ennast küberrünnakute ja nendega kaasnevate (majandus)kahjude vastu. Toetusmeetme eelarve oli ligi 900 000 eurot, millest pool saadi Euroopa Liidu programmist Digital Europe. Täpsema info leiab siit: https://eis.ee/toetused/kybertoetus/. Projekt oli kaheastmeline, esimese etapi tegevussuund oli oma küberturvalisuse hetkeseisu hindamine, et saada ülevaade kõige põletavamatest puudustest ja olukorra parandamise võimalustest. Selle tulemuseks oli teekaart, milles anti hinnang ettevõtja küberturvalisusele, toodi välja puudujäägid, küberturvalisuse taseme tõstmiseks vajalikud tegevused ja ettepanekud tehniliste, füüsiliste ja organisatoorsete kaitsemeetmete parandamiseks. Lisaks esitati hinnang vajalike arendusmeetmete kestusele, tegevuste järjestus ning ühe aasta tegevuskava. Toetuse teises etapis oli teekaarti võimalik rakendada koos küberturbeteenust pakkuva ettevõtja abiga. Teise etapi elluviimise tähtaeg oli 28.02.2025 ning selle tulemus aitab ettevõtjatel olla konkurentsivõimeline ja usaldusväärne partner. Kuigi tegemist on juba suletud toetusega, on kavas avada sama või vähemalt sarnane toetusmeede nii olemasolevatele kui ka uutele KüTSi subjektidele (vt ka KüTSi § 28[2] sisu ja selgitusi ning sellega seotud määruse kavandit).
Kuni 19.05.2025 avatud ettevõtete digipöörde toetusmeetme (lisainfo https://eis.ee/toetused/digipoorde-toetus/) eelarve oli *ca* 56 miljonit eurot ning suurim toetus ettevõttele kuni 300 000 eurot ja ettevõtja omaosalus vähemalt 50%. Toetusmeedet rahastati Euroopa Liidu taasterahastu NextGenerationEU vahenditest. Kuigi selle toetuse nimetus ei olnud otse seotud küberturvalisuse valdkonnaga, oli digipöörde tegevuste käigus võimalik ellu viia tegevusi, mis on vajalikud küberturvalisuse tagamiseks (vt toetuse andmise tingimuste määruse[221] § 7 lõiget 3, sh punkte 1–3, 8 ja 10).
Perioodi 2021–2027 Euroopa Liidu ühtekuuluvus- ja siseturvalisuspoliitika fondide rakendamise seaduse[222] § 10 lõike 2 alusel antud käskkirjaga „Toetuse andmise tingimused valdkondlike digipöörete toetamiseks“[223] oli ette nähtud avalikus sektoris digilahenduste ja uuenduste väljatöötamise ning kasutuselevõtuga seotud tegevuste elluviimiseks toetuse andmised tingimused ja kord. Toetuse andmise eesmärk oli toetada valdkondlikke digipöördeid, tagada inimeste põhiõiguste kaitse, suurendada teadlikkust digiriigist ja selle võimalustest ning pakkuda kasutajale avalikke digiteenuseid mugavalt, küberturvaliselt, andmepõhiselt, etteaimavalt ja kättesaadavalt igas piirkonnas, lähtudes Vabariigi Valitsuse 23. detsembri 2021. a protokollilise otsusega kinnitatud „Eesti digiühiskonna arengukava 2030“ eesmärkidest.[224] Toetuse andmise eesmärk oli saavutada valdkondlike digipöörete toel kasutajakesksete avalike digiteenuste parim kogemus, kus keskendutakse riigi ja valitsemisalade strateegiliste äriliste eesmärkide saavutamisele ning

[221] https://www.riigiteataja.ee/akt/119082022005?leiaKehtiv
[222] https://www.riigiteataja.ee/akt/130062023056
[223] https://adr.rik.ee/mkm/dokument/14601782; käskkirja on muudetud https://adr.rik.ee/mkm/dokument/14798525, https://adr.rik.ee/mkm/dokument/15537817, https://adr.rik.ee/mkm/dokument/16117311 ja https://adr.rik.ee/jm/dokument/17090474. Muudatustes ei ole muudetud siinses seletuskirjas viidatud punkte.
[224] Vastava toetuse andmise käskkirja p 2.1.

kliendiväärtuse suurendamisele nüüdisaegse digitehnoloogia parima kasutuse abil, parandades sealjuures kasutajate teadlikkust.[225] Kui mingi tegevus panustas muu hulgas sellesse eesmärki või tulemusse, siis toetatavate tegevuste hulgas olid käskkirja punkti 3.1. kohaselt: „3.1.1. infotehnoloogiliste lahenduste väljatöötamine ja arendamine; 3.1.2. küberruumi hoidmine, arendamine ja juurutamine usaldusväärse ja turvalisena; 3.1.3. teadlikkuse tõstmine punktides 3.1.1., 3.1.2. ja 3.1.4. nimetatud tegevuste osas, sealhulgas elluviija ja partnerite teadlikkuse tõstmine; 3.1.4. valdkondliku digipöörde elluviimisega seotud tegevused.“ Toetuse kasutamiseks koostati konkreetse elluviija (ministeerium, Riigikantselei või Eesti Linnade ja Valdade Liit) valdkonnas tehtavate tegevuste kava. Seega oli ka selle toetuse puhul võimalik taotleda toetust küberturvalisuse tagamisega seotud tegevusteks.
Praegu saab taotleda digitaliseerimise teekaardi koostamise toetust. Toetuse eesmärk on suurendada ettevõtja teadlikkust tema ettevõtte digitaliseerituse ja automatiseerituse hetkeolukorrast ja küberturvalisuse esmasest tasemest ning luua eeldusi digiriigi lahenduste kasutuselevõtuks, parandades protsesside tulemuslikkust ning kasvatades seeläbi ettevõtja konkurentsivõimet ja võimet suurendada digitaliseerimisega oma toodete ja teenuste lisandväärtust. Toetuse eelarve on 2,5 miljonit eurot ning suurim toetus ettevõttele on kuni 10 000 eurot (digitaliseerimise teekaardi koostamine) või kuni 35 000 eurot (digitaliseerimise teekaardis esitatud kitsaskohtade lahendamiseks ja arenguvõimaluste elluviimiseks vajalik nõustamisteenus ja arendustegevus). Ettevõtja omaosalus on ettevõtja suuruse ja asukoha järgi 30–50%. Lisainfo selle toetuse kohta on siin: https://eis.ee/toetused/digitaliseerimise-teekaardi-toetus/ (vt ka majandus- ja infotehnoloogiaministri 29.02.2024. a määrust nr 8 „Ettevõtja digitaliseerimise teekaardi toetus“, https://www.riigiteataja.ee/akt/105032024001?leiaKehtiv).

8. Rakendusaktid

KüTSi muutmise tõttu ei muutu rakendusaktide volitusnormid kehtetuks.
Rakendusaktide ja teiste määruste muudatuste kavandid on lisatud seletuskirja lisana 2. Need on planeeritud jõustuma seadusega samal ajal.
KüTSi § 52 lõige 1 annab riikliku küberturvalisuse valdkonna eest vastutavale ministrile volituse kehtestada käskkiri, millega määratakse delegeeritud määruse (EL) 2024/1366 artikli 4 lõikes 1 nimetatud pädev asutus. Pädevaks asutuseks määratakse Riigi Infosüsteemi Amet.

8.1. Uued rakendusaktid

Seaduse jõustumisel tuleb ette valmistada järgmiste määruste terviktekstid.
8.1.1. Justiits- ja digiministri määrus „Riikliku küberturvalisuse strateegia koostamise ulatus, tingimused ja elluviimise kord“. KüTSi § 5 lõige 2 näeb ette, et riikliku küberturvalisuse strateegia ulatuse, tingimused ja elluviimise korra koos asjaomaste poliitikameetmete loeteluga kehtestab riikliku küberturvalisuse valdkonna eest vastutav minister määrusega.
Sel määrusel on seos KüTSi § 5 lõikega 1, mis näeb ette, et Vabariigi Valitsus võtab vastu NIS2-direktiivi artiklis 7 nimetatud riikliku küberturvalisuse strateegia, mis võib olla koostatud muu õigusakti kohase dokumendi osana. Riikliku küberturvalisuse strateegia koostamist koordineerib riikliku küberturvalisuse valdkonna eest vastutav minister.
KüTSi § 5 lõike 2 selgitustes on põhjendatud, miks määruse volitusnorm luuakse ning miks see on ministri tasandil. Neid selgitusi siin ei korrata.

8.1.2. Justiits- ja digiministri määrus „Sihipärase turvaauditi korraldamise täpsemad tingimused ja kord“.

[225] Vastava toetuse andmise käskkirja p 2.2.

Määrus kehtestatakse KüTSi § 16 lõike 1^2 ja § 17 lõike 1^2 alusel.
KüTSi § 16 lõige 1^2 näeb ette, et sama paragrahvi lõike 1^1 punktis 2 nimetatud sihipärase turvaauditi korraldamise täpsemad tingimused ja korra, sh loetelu olukordadest, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale turvaauditi kulu, ning turvaauditi kulu hüvitamise korra sätestab riikliku küberturvalisuse valdkonna eest vastutav minister määrusega.
KüTSi § 17 lõige 1^2 näeb ette, et sama paragrahvi lõike 1^1 punktis 2 nimetatud sihipärase turvaauditi korraldamise täpsemad tingimused ja korra, sh loetelu olukordadest, mille puhul Riigi Infosüsteemi Amet hüvitab teenuseosutajale turvaauditi kulu, ning turvaauditi kulu hüvitamise korra sätestab riikliku küberturvalisuse valdkonna eest vastutav minister määrusega.
Määrusel on kaks volitusnormi, kuna sama järelevalvemeedet on võimalik kasutada nii riiklikus kui ka haldusjärelevalves ning puudub vajadus kehtestada mõlema menetlusliigi jaoks eraldi samasisuline määrus. Kommenteeritavate paragrahvide selgitustes on põhjendatud, miks määruse volitusnorm luuakse ning miks see on ministri tasandil. Neid selgitusi siin ei korrata.

8.1.3. Justiits- ja digiministri määrus „Vastastikuse hindamise täpsemad tingimused".
Määruse kehtestamise alus on KüTSi § 17^6 lõige 3, mis näeb ette, et riikliku küberturvalisuse valdkonna eest vastutav minister võib kehtestada määrusega vastastikuses hindamises osalemise täpsemad tingimused ja korra, sh vastastikuse hindamise korralduse nõuded, selles osalevate asutuste ülesanded ja vastastikuses hindamises osalevad isikud.
Kommenteeritava paragrahvi selgitustes on põhjendatud, miks määruse volitusnorm luuakse ning miks see on ministri tasandil. Neid selgitusi siin ei korrata.
Kommenteeritava määruse aluseks olev volitusnorm ei eelda määruse kohest kehtestamist seaduse jõustumisel, kuna vastastikusel hindamisel osalemine on vabatahtlik ning eelnõu koostamise seisuga ei ole olnud arutelusid, kas Eesti võiks olla esimeste seas, keda vastastikku hinnatakse, või Eesti osaleks teise riigi suhtes tehtavas vastastikuses hindamises.

8.1.4. Justiits- ja digiministri määrus „Küberturvalisuse taseme tõstmise toetuse tingimused ja kord".
Määrus kehtestatakse eelnõukohase KüTSi § 28^2 lõike 3 ja riigieelarve seaduse § 53^1 alusel.
Eelnõukohane KüTSi § 28^2 lõige 1 näeb ette, et saavutada Eestis küberturvalisuse ühtlaselt kõrge tase, on teenuseosutajatel õigus taotleda enda küberturvalisuse taseme parandamiseks küberturvalisuse taseme tõstmise toetust. Toetust on võimalik taotleda ka muudel isikutel, kes soovivad KüTSi nõudeid täita või enda küberturvalisuse taset parandada.
Eelnõukohane KüTSi § 28^2 lõige 3 näeb ette, et selle toetuse taotlemise, andmise, kasutamise ja tagasinõudmise tingimused ning kord kehtestatakse riigieelarve seaduse §-s 53^1 sätestatud korras riikliku küberturvalisuse valdkonna eest vastutava ministri määrusega.
Riigieelarve seaduse § 53^1 lõige 1 näeb ette, et minister kehtestab määrusega tingimused ja korra ministeeriumi valitsemisala vahendite arvelt riigisisese toetusprogrammi elluviimiseks, toetusprogrammist vahendite saamiseks ning saadud vahendite kasutamiseks, kui nimetatud tingimused ja kord ei ole sätestatud muus õigusaktis.
Eelnõukohase KüTSi § 28^2 selgitustes on põhjendatud, miks määruse volitusnorm luuakse. Neid selgitusi siin ei korrata.

8.2. Muudetavad rakendusaktid

Seaduse jõustumisel tuleb muuta järgmisi määruseid:

- Vabariigi Valitsuse 23.12.1996. a määrus nr 319 „Justiits- ja Digiministeeriumi põhimääruse kinnitamine" (RT I, 29.12.2024, 46);
- Vabariigi Valitsuse 09.12.2022. a määrus nr 121 „Võrgu- ja infosüsteemide küberturvalisuse

nõuded“ (RT I, 19.06.2024, 12);[226]
- Vabariigi Valitsuse 03.01.2024. a määrus nr 1 „Võrgu- ja infosüsteemi turvameetmete nõuded ja nende kohaldamise ulatus pilvteenuse kasutamisel“ (RT I, 09.01.2024, 25);
- majandus- ja infotehnoloogiaministri 17.08.2023. a määrus nr 53 „Küberintsidentide registri põhimäärus“ (RT I, 24.08.2023, 3);
- majandus- ja kommunikatsiooniministri 25.04.2011. a määrus nr 28 „Riigi Infosüsteemi Ameti põhimäärus“ (RT I, 27.12.2024, 10);[227]
- majandus- ja taristuministri 28.06.2018. a määrus nr 37 „Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektriga varustamisel“ (RT I, 08.12.2023, 3).

9. Seaduse jõustumine

Seadus 2026. aasta 1. jaanuaril. Jõustumise kuupäeva on selgitatud eelnõu §-s 11.

10. Kaasamine

Eelnõu koostamisele eelnesid arutelud (kärajad), mis peeti 2023. a juunis nii avaliku sektori kui ka erasektoriga. Kärajatel osalesid huvirühmad järgmistest organisatsioonidest ja liitudest: Advokatuur / Advokaadibüroo Nove, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Eesti Jõujaamade ja Kaugkütte Ühing, Eesti Linnade ja Valdade Liit, Eesti Pank, Eesti Rahvusringhääling, Eesti Vee-ettevõtete Liit, Elektrilevi, Finantsinspektsioon, Greenergy Data Centres, Huawei Technologies Eesti, Kaitseministeerium, Kultuuriministeerium, Maksu- ja Tolliamet, Proud Engineers, Põhja-Eesti Regionaalhaigla, Rahapesu Andmebüroo, Registrite ja Infosüsteemide Keskus, Riigi Infosüsteemi Amet, Riigikantselei, Saaremaa vald, SEB Pank, Siseministeeriumi infotehnoloogia- ja arenduskeskus, SK ID Solutions, Swedbank, Tallinna Lennujaam, Tallinna Vesi, Tarbijakaitse ja Tehnilise Järelevalve Amet, Telia Eesti, Tori vald ja Viru Keemia Grupp.

Eelnõu koostamisel peeti arutelusid ka Eesti Interneti Sihtasutusega nii ennekõike NIS2-direktiivi artikli 28 kui ka muude nende tegevusvaldkonnaga seotud artiklite ülevõtmise kohta.

Majandus- ja Kommunikatsiooniministeerium saatis eelnõu 9. detsembril 2024 kooskõlastamiseks ja arvamuse avaldamiseks Riigikantseleile, ministeeriumitele, Eesti Linnade ja Valdade Liidule ning muudele küberturvalisuse valdkonnaga seotud osalistele ning huvirühmadele. Too eelnõu on eelnõude infosüsteemi toimikus 24-1266.[228]

Avalikul kooskõlastusringil olnud eelnõule esitasid tagasiside Kaitseministeerium, Kliimaministeerium, Majandus- ja Kommunikatsiooniministeerium, Rahandusministeerium, Regionaal- ja Põllumajandusministeerium, Siseministeerium, Sotsiaalministeerium, Välisministeerium, Riigikogu kantselei, Andmekaitse Inspektsioon, Finantsinspektsioon, Maa- ja Ruumiamet, Riigi Infosüsteemi Amet, Tarbijakaitse ja Tehnilise Järelevalve Amet, Transpordiamet, Eesti Advokatuur, Tervisekassa, Alkoholitootjate ja Maaletoojate Liit, Eesti Esmatasandi Tervisekeskuste Liit, Eesti Haiglate Liit, Eesti Infotehnoloogia ja Telekommunikatsiooni Liit, Eesti Jõujaamade ja Kaugkütte Ühing, Eesti Kaubandus-Tööstuskoda, Eesti Kaupmeeste Liit, Eesti Linnade ja Valdade Liit, Eesti Perearstide Selts, Eesti Proviisor Apteekide Liit, Eesti Põllumajandus-Kaubanduskoda, Eesti Ravimihulgimüüjate Liit, Eesti Vee-ettevõtete Liit, Advokaadibüroo RASK, AS Elenger Grupp, Baltic RCC OÜ, Eesti Energia AS,

[226] Eeldatavasti jõustuvad enne sama määruse muudatused (vt eelnõude infosüsteemi toimik 25-0715, mis on planeeritud jõustuma oktoobris 2025), mistõttu kõnesoleva eelnõu lisas esitatud määruste kavandis ette nähtud muudatused toimuvad tolle määruse redaktsiooni kohta.

[227] Justiits- ja Digiministeeriumil on kõnesoleva eelnõu kirjutamise ajal ettevalmistamisel sama määruse muudatus, mistõttu eelnõu lisas esitatud määruste kavandis ette nähtud muudatused toimuvad tolle määruse redaktsiooni kohta.

[228] https://eelnoud.valitsus.ee/main/mount/docList/c774c2e2-0c3e-4137-b24b-b49d1249f326.

Eesti Interneti SA, Guardtime, Riigimetsa Majandamise Keskus ning üks eraisik. Haridus- ja Teadusministeerium ning Kultuuriministeerium kooskõlastasid eelnõu märkusteta. Riigikohus ei soovinud arvamust avaldada. Esitatud tagasiside ja selle vastused on seletuskirja lisas 3.