JUSTIITS- JA DIGIMINISTEERIUM

Katrin Talihärm
tegevjuht
Eesti Pangaliit
pangaliit@pangaliit.ee

Teie 30.04.2026 nr 26

Meie 15.05.2026 nr 8-4/3523-2

Vastus selgitustaotlusele

Lugupeetud Katrin Talihärm

Saime Teie selgitustaotluse seoses 01.01.2026. a jõustunud küberturvalisuse seaduse (edaspidi *KüTS*) tõlgendamisega seoses krediidiasutustega. Selgitustaotlusega esitatud küsimused ja neile esitatud selgitused on järgnevad.

1. Millistele teenustele peab krediidiasutus kohaldama KüTS-i?
Vastus küsimusele nr 1:
Eeldame, et nii siinse kui ka järgnevate küsimuste puhul on krediidiasutuste puhul mõeldud krediidiasutust Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 artikli 4 punkti 1 tähenduses. Krediidiasutuste põhiteenustele ja neid toetavatele IKT-süsteemidele ei kohaldata KüTSi sisulisi küberturvalisuse nõudeid (st 2. peatükki), sest neile kohaldub Euroopa Parlamendi ja nõukogu määrus (EL) 2022/2554 ehk DORA määrus. Neile kohalduvad aga muudes KüTSi peatükkides toodud nõuded, mis ei ole seotud konkreetse teenusega (vt järgnevad selgitused). KüTS võib krediidiasutustele kohalduda täiendavas ulatuses nende teenuste suhtes, mida DORA määrus ei kata, kuid mis on nimetatud Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 ehk NIS2-direktiivi artiklis 2 või sama direktiivi I või II lisas.
Krediidiasutus on ennekõike KüTSi kohaldamisalas (st KüTSi tähenduses teenuseosutaja) seetõttu, et tegemist on kas elutähtsa teenuse osutajaga hädaolukorra seaduse tähenduses (vt ka KüTS § 3 lõike 2 punkti 2) või on tegemist eelviidatud määruse kohase krediidiasutusega, mis on suurem kui keskmise suurusega ettevõtja Euroopa Komisjoni soovituse 2003/361/EÜ tähenduses (vt ka KüTS § 3 lõike 3 punkti 18 ning lõike 4 punkti 8). EI ole välistatud, et krediidiasutus on KüTSi kohaldamisalas ka mõne muu teenuse või tegevusala tõttu – kuid see tuleb selgeks teha juhtumipõhiselt.
NIS2-direktiivi üle võtnud seaduseelnõu (739 SE)[1] seletuskirjas on KüTS § 3 lõike 3 punkti 18 selgitustes selgitatud määruse (EL) nr 575/2013 artikli 4 punkti 1 sisu ning selles on ka esitatud järgnev selgitus:
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.
Samas seletuskirjas on KüTS § 1 lõike 4 selgitused järgmised (väljavõte):
***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. ….*

[1] https://www.riigikogu.ee/tegevus/eelnoud/eelnou/4429a2b9-e6e2-41cf-991d-f6955c6c4a69/kuberturvalisuse-seaduse-ja-teiste-seaduste-muutmise-seadus-kuberturvalisuse-2.-direktiivi-ulevotmine/

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).[2]

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. ….

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[3] *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, 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.*

Enne kui on võimalik anda selgitust, millistele teenustele peab krediidiasutus kohaldama KüTSi, on kasulikum selgeks teha, mis on need sätted, mis talle KüTSist võivad üldse kohalduda (teenuste ja teemade osas, mis on DORA määrusega kaetud). Krediidiasutuste seaduse § 82[4] lõike 3 ning kaudselt ka KüTS 1 lõike 4 tõttu (neist esimene välistab KüTSi 2. peatüki kohaldumise) on need sätted ennekõike KüTSi 1. peatükis (vt KüTS § 1 lõiget 4 ning §-e 3–4[1] ja 6). KüTSi 3. ja 3[1] peatükid on seotud ennekõike ametiasutuste või vastavushindamisasutuste tegevusega ehk need peatükid pole eelduslikult krediidiasutuste kontekstis asjakohased. KüTSi 4. ja 5. peatükid on ennekõike seotud KüTSi 2. peatükiga, mistõttu pole ka need peatükid konkreetsel juhul asjakohased. KüTSi 4[1]. peatükist kohaldub

[2] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52023XC0918%2801%29&qid=1726668543740

[3] 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/112022026002)].

krediidiasutustele ainult KüTS § 17^5 (vt allpool). KüTSi 6. peatükist kohaldub krediidiasutustele ainult § 28^1 (vt allpool). Seetõttu on hetke teadmiste kohaselt krediidiasutuste puhul asjakohased järgmised KüTSi sätted (valdkondade või teenust korral, mis on hõlmatud DORA määrusega):

- KüTS § 1 lõige 4 (*nö samaväärse õigusakti kohaldumine*): tegemist on kaudselt krediidiasutustega seotud sättega, kuna see on seotud krediidiasutuste seaduse § 82^4 lõikega 3 – samas selgitatav lõige ei erista konkreetset teenust või (tegevus)valdkonda, vaid teatavaid kohustusi ja nõudeid;
- KüTS § 3 (*teenuseosutaja*): vt eespool viidatud sätteid, mille alusel on krediidiasutused ennekõike KüTSi teenuseosutajad; meile on teadmata, kas krediidiasutus saab (st kas on lubatud) üldse osutada ka muid teenuseid, mis on tolle paragrahvi erinevates lõigetes nimetatud ning meil puudub hetkel ka teadmine, milliseid teenuseid konkreetne krediidiasutus osutab või võib osutada, mistõttu on keeruline anda selgitust, mil määral see paragrahv kohaldub üksusele, kes tegutseb krediidiasutusena;
- KüTS § 3^1 (*teavitamiskohustus ja nimekiri*): kuigi 739 SE seletuskirjas on märgitud, et nimetatud paragrahvi ei kohaldata DORA määruse kohastele finantssektori üksustele, ei ole KüTSis taolist välistust ette nähtud ning seda paragrahvi ei ole meile teadaolevalt välistatud ka mõnes muus seaduses (st ennekõike krediidiasutuste seaduses), mistõttu tegemist on sättega, mis kohaldub ka krediidiasutustele;
- KüTS § 4 (*digitaalse teenuse osutajaga seonduvad nõuded*): selle paragrahvi kohaldamise võimalikkus sõltub sellest, kas krediidiasutustele on võimalik käsitada digitaalse teenuse osutajana (vt KüTS § 2 punkti 2). Meil hetkel puudub taoline teadmine, kuid kui taoline lähenemine on võimalik, siis peab krediidiasutus esitama enda kohta käivad andmed ja uuendama neid viivitamata, kuid hiljemalt kolme kuu jooksul pärast muudatuse tegemise kuupäeva. Teataval juhul peab ta ka määrama endale esindaja (vt ka KüTS § 2 punkti 3) ja tegema selle esindaja kontaktid avalikult kättesaadavaks;
- KüTS § 4^1 (*nõuete ja kohustuste esmakordne täitmine*): määratleb ära, mis tähtajaks peab alates 01.01.2026. a jõustunud KüTSi muudatustega lisandunud üksus esmakordselt täitma näiteks KüTS §-des 3^1 ja 4^1 olevad kohustused (milleks on aega kuni kolm kuud);
- KüTS § 6 (*küberturvalisuse tagamise põhimõtted*): kuigi 739 SE seletuskirjas on märgitud, et nimetatud paragrahvi ei kohaldata DORA määruse kohastele finantssektori üksustele, ei ole KüTSis taolist välistust ette nähtud ning seda paragrahvi ei ole meile teadaolevalt välistatud ka mõnes muus seaduses (st ennekõike krediidiasutuste seaduses), mistõttu tegemist on sättega, mis kohaldub ka krediidiasutustele;
- KüTS § 17^5 (*küberturvalisusalase teabevahetuse kokkulepped*): tegemist on paragrahviga, mis reguleerib nii KüTSis subjektide kui ka muude üksuste vahelist küberturvalisuse alast teabevahetust ja seotud kokkulepete korraldust. Vastava kokkuleppega ühinemine on vabatahtlik, kuid kui krediidiasutus taolise kokkuleppega ühineb, siis tuleb lähtuda selles paragrahvis ette nähtud nõuetest;
- KüTS § 28^1 (*nn üleminekusätted neile üksustele, kes olid KüTSi subjektid enne 01.01.2026. a*): nende sisu ja tähtajad on põhimõtteliselt sama, mis on ette nähtud KüTS §-s 4^1.

Nagu eelnevalt selgitasime, puudub Justiits- ja Digiministeeriumil teadmine, kas ja milliseid muid teenuseid krediidiasutused praktikas osutavad või milliseid teenuseid on neil lubatud osutada. Seetõttu on ka keeruline anda soovitud selgitusi. Sellest hoolimata, näitab eeltoodud ülevaade, et krediidiasutusele saab kohalduda (valdkondade või teenust korral, mis on hõlmatud DORA määrusega) KüTSist valdavalt üksikud nõuded ning need ei ole ennekõike seotud konkreetse teenusega.

2. Kas krediidiasutused peavad Riigi Infosüsteemi Ametile esitama KüTS § 3^1 kohase teavituse?
Seaduse tekst ei näe ette erisusi teavitamiskohustuse täitmisele, kuid seletuskirja kohaselt ei kohaldata DORA kohaldamisalas oleva finantssektori üksuse osutatavale DORA kohaldamisalasse kuuluvale teenusele KüTS-i §-i 3^1 . Vastamisel palun võtke arvesse ka vastust küsimusele nr 1.
Vastus küsimusele nr 2: krediidiasutused peavad tegema KüTS § 3^1 kohase teavituse Riigi Infosüsteemi Ametile. Vt siin ka vastust küsimusele nr 1.

3. Kas saame õigesti aru, et pangad ei pea Riigi Infosüsteemi Ametile esitama KüTS § 6^1 kohase info? Krediidiasutuste seaduse § 82^4 lõige 3 järgi ei kohaldata krediidiasutustele küberturvalisuse seaduse 2. peatükis sätestatud küberturvalisuse tagamise nõudeid ja hädaolukorra seaduse § 4^1 lõiget 1 (jõustunud 17.01.2025). Alates 2026. aastast on KüTS 2. peatükki lisatud § 6^1. Teenuseosutaja juhatuse liikme kohustused, mis sätestab vastutava juhatuse liikme määramise ning esitama Riigi Infosüsteemi Ameti taotlusel vastava nime ja kontaktandmed.
4. Kas krediidiasutused peavad esitama Riigi Infosüsteemi Ametile KüTS § 6^1 alusel vastutava juhatuse liikme andmed?
Arvestada tuleb krediidiasutuste seaduse KAS § 82^4 lõikes 3 sätestatut, et krediidiasutustele ei kohaldata KüTS 2. peatüki nõudeid. Alates 2026. aastast lisandub § 6^1 samasse peatükki. Palume

ministeeriumi seisukohta, kas krediidiasutused on sellest kohustusest vabastatud või ministeeriumi hinnangul rakendub § 6[1] siiski ka krediidiasutustele.
Vastus küsimustele 3 ja 4:
Eeldame, et mõlema küsimuse puhul on mõeldud sama organisatsiooni (üksust), st krediidiasutust. Kuna KüTS § 6[1] asub selle seaduse 2. peatükis, siis krediidiasutuste seaduse § 82[4] lõike 3 ning kaudselt ka KüTS § 1 lõike 4 tõttu ei pea krediidiasutus edastama Riigi Infosüsteemi Ametile tema taotluse korral tolles paragrahvis mainitud juhatuse liikme andmeid.

Täiendavate küsimuste korral oleme meeleldi nõus selgitusi andma.

Lugupidamisega

(allkirjastatud digitaalselt)
Taavi Viilukas
juhataja

Raavo Palu
raavo.palu@justdigi.ee

Lisaadressaadid: Rahandusministeerium
Riigi Infosüsteemi Amet
Finantsinspektsioon