RAHANDUSMINISTEERIUM

Justiits- ja Digiministeerium
info@just.ee

Teie 09.12.2024 nr 2-2/3131-1;
MKM/24-1266/-1K
Meie 17.02.2025 nr 1.1-11/5510-4

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

Austatud proua justiits- ja digiminister

Rahandusministeerium kooskõlastab küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu järgmiste märkustega.

1. Eelnõu § 1 punktiga 24 täiendatakse küberturvalisuse seadust (edaspidi *KüTS*) §-ga $6^{1,}$ mille lõigetega 2 ja 3 võetakse üle NIS2 direktiivi artikli 20 lõige 2, mis on seotud NIS2 direktiivi põhjenduspunktiga 137, mille kohaselt peaksid elutähtsate ja oluliste üksuste juhtorganid kiitma küberturvalisuse riskijuhtimismeetmed heaks ja jälgima nende rakendamist. Seletuskirja kohaselt võiks teenuse osutaja juhtorgani liikmete erikoolituste sisu ehk õpiväljundid olla järgmised: küberturvalisusega seotud riskid, ohud, levinumad rünnakutüübid kui ka riskide haldamine. Samuti ootab eelnõu koostaja tagasisidet, kas taoline välp tuleks reguleerida ning kui jah, siis mis võiks olla sobiv välba pikkus. Teeme ettepaneku, et välba pikkus võiks olla kaks aastat.

Palume eelnõus selgelt sätestada ja seletuskirjas selgitada, mida peetakse silmas erikoolituse all (miks mitte lihtsalt koolitus), millistele nõuetele peavad vastama erikoolituse läbiviimiseks pädevad koolitusasutused ja mis on koolituse läbimist tõendavaks dokumendiks.

Ühtlasi palume normitehniliselt täpsustada uue § 6^1 asukohta, sest oma olemuselt kuulub uus § 6^1 1. peatükki alla, kuna ei peaks kohalduma nendele finantssektori ettevõtjatele, kellele KüTS 2. peatükk ei kohaldu (krediidiasutustele krediidiasutuste seaduse § 82^4 lõige 3, registripidajatele väärtpaberite keskregistri seaduse § 30^2 lõige 2 ja reguleeritud turu korraldajale § 124^6 lõike 3 kohaselt).

2. Eelnõu § 1 punktiga muudetakse KüTS § 1 lõiget 4.
Teeme ettepaneku seletuskirjas välja tuua, et näiteks on see säte asjakohane seoses määruse (EL) 2022/2554 (DORA) nõuete kohaldamisega finantssektoris. DORA määruse põhjenduspunktis nr 16 on selgitatud, et DORA määrus on NIS2 suhtes *lex specialis*. NIS2 direktiivi põhjenduspunkt 28 selgitab lisaks, et NIS2 direktiivi sätete asemel tuleks kohaldada

DORA määruse sätteid, mis käsitlevad 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, DORA määruse kohaldamisalasse jäävate finantssektori ettevõtjate suhtes kohaldada.

Palume selgitada, kas/kuidas tuleks kohaldada KüTS § 17^5 nii KüTS kui ka DORA kohaldamisalasse jäävatele finantssektori ettevõtjatele. Eelosutatud NIS2 põhjenduspunkti 28 kohaselt tuleks NIS2 direktiivi sätete asemel kohaldada DORA määruse sätteid, mis käsitlevad mh teabevahetuse kokkuleppeid. NIS2 artikli 4 lõike 1 sõnastus on kitsam, viidates ainult küberturvalisuse riskijuhtimismeetmete võtmisele või olulistest intsidentidest teatamisele (nagu on ka KüTS § 1 lg 4). DORA määruses on teabevahetus reguleeritud artiklis 45, kuid hõlmab ainult finantssektori ettevõtjate omavahelist teabevahetamist ja kokkuleppeid. Kui näiteks kaks finantssektori ettevõtjat (nt kaks ETO panka) soovivad omavahel vahetada teavet, siis kas teabevahetusele kohalduvad topelt normid?

3. Eelnõu § 1 punktiga 26 kohustatakse teenuse osutajat turvameetmete rakendamisel koostama ja kehtestama varade halduse põhimõtted ja seotud protseduurijuhendid (p 12). Kuigi ilmselt on enamus teenuse osutajatel kehtestatud vara halduse põhimõtted ja protseduurijuhised mistahes vara puhuks, ei ole küberturvalisuse vaatenurgast selline ulatuslik nõue KüTSis siiski asjakohane. Palume sättes varad piiritleda KÜTS § 1 lõikest 1 lähtuvalt.

4. Seletuskirja punktis 6.2.3 on hinnatud eelnõu mõju majandusele. Üldistatult saab kokku võtta, et olemasolevaid subjekte on 3537 ning uusi subjekte on ligikaudu 2000 ehk kokku on ligikaudu 5500 subjekti, kellele KüTSi nõuded hakkavad kohalduma.

Üks osa Eesti infoturbestandardi rakendamisest on ka Eesti infoturbestandardi vastavusauditi tegemine iga kolme aasta järel, mis on eelduslikult ühe suurema kulu allikas uutele KüTSi subjektidele. Auditi maksumus jääb seletuskirja kohaselt 4500–20 000 euro vahemikku. Eelnõu koostajad märgivad, et nimetatud summa on kajastatud hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (426 SE) seletuskirjas ning antud eelnõu koostamise hetke seisuga ei olnud võimalik kontrollida, kas mainitud maksumuste suurusjärk on jätkuvalt sama või on siin mingeid muudatusi toimunud.

Juhime tähelepanu, et hädaolukorra seaduse muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse (426 SE) eelnõu saadeti ministeeriumidele EIS-i kaudu esimesele kooskõlastusringile septembris 2023. a. Seega on auditi maksumuse andmed ilmselgelt vananenud. Palume seletuskirjas olevad auditeerimise hinnad korrigeerida. Värskemaid andmeid on võimalik saada riigihangete registrist või tehes päringuid audiitorfirmadele (Audiitorkogule). Lisaks palume seletuskirjas realistlikult hinnata subjektidele kaasnevat mõju (nii halduskoormusele kui ka kuludele) seoses Eesti infoturbestandardi rakendama hakkamisega.

5. Seletuskirjas on puudu andmed, kui paljud audiitorfirmad (audiitorid) IT-auditeerimise teenust pakuvad. Arvestades seda, et Eesti infoturbestandardi auditeerimisjuhendi kohaselt koosneb E-ITS audit minimaalselt põhiauditist ja vaheauditist (viiakse läbi hiljemalt üks aasta pärast põhiauditit või eelmist vaheauditit), on eeldatavasti juba praegu olemasolevad IT-auditeerimise teenuse pakkujad väga hõivatud. Seega võivad lisanduvad 2000 subjekti nõuetekohaste auditite läbiviimise muuta võimatuks ja/või tõsta

auditeerimise teenuse hinna kõrgeks. Seega palume seletuskirja täiendada IT-auditeerimise teenust pakkuvate audiitorite andmetega, kaaluda auditeerimistsükli pikendamist või esitada seletuskirjas muud olukorra leevendamise meetmed. Väheste audiitorite ja kulu suurendamise olukorras pannakse kohustatud isikutele üle jõu käivad kohustused.

6. Eelnõu § 1 punktis 1 (lisatav KüTS § 1 lg 1^6), § 1 punktis 5 (KüTS § 1 lg 4^1) ja § 1 punktis 49 (KüTS § 13^3 lg 1) ei ole normi sõnastusest võimalik aru saada, kas mõeldud on pädevusnormi või määruse andmise volitusnormi, seega palume sõnastuste vastavust HÕNTE-le kontrollida.

7. Eelnõu § 1 punktiga 58 täiendatakse KüTS vastutuse osa, lisades seaduse nõuete rikkumise eest karistused ka füüsilisest isikust üksustele. Palume seletuskirjas tuua näiteid Eestis olevatest füüsilistest isikust elutähtsast, olulisest ja komisjoni delegeeritud määruse (EL 2024/1366 nimetatud üksustest.

8. Eelnõus pannakse kohustatud isikutele mitmeid teavituskohustusi, mida ja millal ja kuidas peab kohustatud subjekt Riigi Infosüsteemi Ametit teavitama. Samas pole täpsustatud, kas ja kuidas peaks Riigi Infosüsteemi Amet nendele teavitustele vastama.

9. Palume lisada eelnõusse üleminekusätted, mille kohaselt antakse uutele kohustatud isikutele piisav üleminekuaeg Eesti infoturbestandardi ja sellest tulenevate turvameetmete rakendamiseks. Eesti infoturbestandardi rakendamisega seonduv tööhulk ja kulud (eelarvelised piirangud) võivad olla arvestatavad ja ei pruugi arvestades seaduse eelnõus sätestatud seaduse jõustumise aega olla tehtavad. Seejuures tuleks eelnevalt analüüsida, kas kõikidele kohustatud subjektidele ühetaolise Eesti infoturbestandardi või ISO27002 standardi rakendamise kohustuse panemisele on võimalik leida väiksemat halduskoormust (ja kulu) kaasa toov alternatiiv.

10. Palume üle kontrollida eelnõuga kasutusele võetavate ja kehtivas seaduses kasutatavate terminite kasutus (et sama mõiste jaoks ei kasutataks erinevaid termineid). Näiteks kasutatakse eelnõus intsidentide avastamise ja halduse termineid läbisegi, samuti on eelnõu tekstis korduvalt kasutatud loetelusid stiilis „küberriskide-, -ohtude, -intsidentide…“, kus selline üldistamine ei loo selgust ning jätab liigselt tõlgendusruumi nii seaduse täitmiseks kui järelevalveks.

11. Eelnõus esineb palju keelevigu, seega palume eelnõu enne selle edasist menetlemist keeleliselt toimetada.

Lugupidamisega

(allkirjastatud digitaalselt)

Jürgen Ligi
rahandusminister

Virge Aasa 5885 1493 Virge.Aasa@fin.ee

Kristiina Kubja 5885 1398 Kristiina.Kubja@fin.ee