SISEMINISTEERIUM

Liisa Pakosta
Justiits- ja Digiministeerium

Teie: 25.05.2026 nr JDM/26-0608/-1K

Meie: 14.07.2026 nr 1-7/160-6

Siseministeeriumi vastuskiri määruse „Eesti infoturbestandardi“ eelnõule

Lugupeetud justiits- ja digiminister

Siseministeerium (edaspidi *SIM*) on tutvunud kooskõlastamiseks esitatud justiits- ja digiministeeriumi määruse „Eesti infoturbestandard“ muutmise eelnõuga ning kooskõlastab selle alljärgnevate märkustega.

1. **E-ITS lahti sidumine ISO standardist**
   Seletuskirjas rõhutatakse E-ITSi lihtsustamist ja nõuete arusaadavuse parandamist. Samas toob ISO standardist eemaldumine kaasa ühe rahvusvaheliselt tunnustatud võrdlusraamistiku kadumise. See võib praktikas muuta nõuete tõlgendamise ja rakendamise keerukamaks, mitte lihtsamaks. Selgema arusaadavuse tagamiseks ning koostöö hõlbustamiseks (sh rahvusvaheliste partnerite, audiitorite ja teenuseosutajatega) oleks otstarbekas lisada E-ITSi ja ISO/IEC 27001 põhimõtete vaheline vastendamine või suunav juhendmaterjal. Samuti võib vastavustabeli või juhendite puudumine kaasa tuua organisatsioonides dubleerivat tööd - näiteks nõuete tõlgendamisel, turvameetmete valikul ja rakendamisel, teenuslepingute tingimuste kujundamisel.

2. **Ohupilt ja dünaamiline küberturvalisuse keskkond**
   Tänapäevase kiiresti muutuva ohupildi kontekstis võiks standard käsitleda senisest selgemalt dünaamilist ohuteavet ja selle kasutamist. See hõlmab eelkõige:
   a. CERT-EE hoiatuste ja ohuhinnangute süsteemsemat kasutamist,
   b. tarkvara ja teenuste tarneahela küberturvalisuse riske (sealhulgas arvestades, et sertifikaadid üksi ei pruugi olla piisavad),
   c. pilveteenustega seotud spetsiifilisi riske,
   d. tehisintellekti kasutamisega kaasnevaid riske ja muutusi küberkeskkonnas.

   Kuigi eelnõu on tehnoloogianeutraalne, on tehisintellekti mõju küberdomeenis juba märkimisväärne ning selle käsitlemine vähemalt põhimõttelisel tasemel suurendaks regulatsiooni ajakohasust. Samuti võiks tugevamalt rõhutada organisatsioonide vahelise koostöö rolli, sealhulgas koostööd CERT-EE-ga.

3. **Auditeerimise tsükkel**

   Kehtivas määruses on kasutusel mõiste „auditeerimise tsükkel“. Uues määruse eelnõus ei ole seda mõistet otseselt sätestatud ega piisavalt selgitatud. Kuigi seletuskirjas on auditeerimise loogika osaliselt esitatud skeemina, ei ole kolmeaastane tsükkel normatiivsel tasandil üheselt arusaadav. Selline ebamäärasus võib praktikas kaasa tuua erinevaid tõlgendusi. Ettepanek on sätestada auditeerimise tsükkel selges ja üheselt mõistetavas vormis kas määruses või auditeerimiseeskirjas.

4. **Eelnõus nimetatud rollid**

   Eelnõu § 3 lõige 2 sätestab, et infoturbe halduse süsteemi toimimiseks tuleb määrata sealsamas punktides 1-4 nimetatud rollid, milleks on „hankejuht“, „infoturbejuht“, „kasutaja“ ja „äriüksuse juht“. Rollidega külgnevalt on eelnõu seletuskirja lk 6 kolmandas ja neljandas lõigus selgitatud, et „*Roll ei tähenda, et seda peab täitma sama ametinimetusega töötaja, vaid tegemist on tegevustega, millega organisatsioon peab arvestama.*“ ning „*Hankejuhi all ei mõisteta eelnõus ostujuhti või riigihanke eest vastutajat. Hankejuhi ülesanne on kontrollida, kas turvameetmed on planeeritud kogu elutsüklis (nii teenuste kui ka varade puhul), enne kui mõni uus teenus kasutusele võetakse või võrgu- ja infosüsteemi turvalisuse tagamisega seotud tegevusi tehakse. Näiteks peab ta välja selgitama vajaduse tulekustutussüsteemi järele serveriruumis, nii et õnnetuse korral ei oleks tagatud mitte ainult tuleohutus, vaid ka teabe säilimine. Hankejuhi rollis ei pea olema üks töötaja, vaid seda rolli võib täita mitu töötajat.*“.

   SIM nõustub seletuskirjas toodud käsitlusega, et eelnõus nimetatud roll ei peaks tähendama, et seda peab täitma sama ametinimetusega töötaja. SIM mõistab eelnõuga taotletavat eesmärki selliselt, et infoturbe süsteemi toimimise tagamiseks on eeskätt tähtis, et organisatsioon on siseselt läbi mõelnud ja paika pannud, kes antud organisatsioonis täidab rollide juures kirjeldatud tegevusi. Hetkel see eelnõu tekstist selliselt välja ei tule vaid üksnes seletuskirjast. Ühtlasi leiame, et eelnõu § 3 lõike 2 punktis 1 kirjeldatud tegevuste eest vastutavale rollile antud nimetus „hankejuht“ on rollile määratud tegevusi silmas pidades eksitav. Kuigi seletuskirjas on toodud, et eelnõus ei mõisteta rolli „hankejuht“ all ostujuhti või riigihanke eest vastutajat, siis märgime, et tavapäraselt seostub avalikus sektoris sõnaga „hankejuht“ just riigihangete valdkonna töötaja ehk riigihanke menetluste läbiviija.

   Ülaltoodust lähtuvalt palume üle vaadata, kas piisab kui eelnõus jätta välja rollide nimetused ja sätestada organisatsioonile üksnes kohustus siseselt määrata, kes täidab eelnõu § 3 lõike 2 punktides 1-4 toodud tegevusi. Või alternatiivselt, üle vaadata eelnõus kasutatud rollide nimetused ning seejuures tagada, et ka eelnõust endast tuleb välja, et roll ei tähenda, et seda peab täitma sama ametinimetusega töötaja.

5. **Isikuandmete kaitse käsitluse täpsustamine**

   Eelnõu lisas 1 on eraldi protsessimoodulina ette nähtud GRC.4 „Isikuandmete kaitse“, kuid määruse normatiivses osas ei ole selgitatud, kuidas see moodul suhestub infoturbe halduse süsteemiga ning isikuandmete kaitset reguleerivatest õigusaktidest tulenevate kohustustega. Erinevate tõlgenduste vältimiseks võiks seletuskirjas või juhendmaterjalis selgitada, et GRC.4 eesmärk ei ole luua organisatsioonis eraldiseisvat andmekaitse juhtimissüsteemi, vaid toetada Euroopa Parlamendi ja nõukogu määrusest (EL) 2016/679 (IKÜM) tulenevate kohustuste täitmist tehniliste ja korralduslike meetmete rakendamisel ning andmekaitse lõimimisel organisatsiooni üldisesse riskijuhtimisse.

6. **Riskihaldus ja andmekaitsealane mõjuhinnang**
   Eelnõus käsitletakse infoturberiskide hindamist, kuid ei selgitata selle seost IKÜM artikli 35 kohase andmekaitsealase mõjuhinnanguga. Seletuskirjas võiks selgitada infoturberiskide hindamise ja andmekaitsealase mõjuhinnangu omavahelist seost. Praktikas viiakse mõlemad hinnangud sageli läbi sama projekti või infosüsteemi arendamise käigus. Juhised nende omavaheliseks sidumiseks aitaksid vältida dubleerimist ning toetaksid terviklikku riskijuhtimist. Samal ajal võiks selgitada ka nende hinnangute erinevat eesmärki ja fookust, et oleks arusaadav, millised riskid ja asjaolud kuuluvad infoturbe riskihindamise ning millised andmekaitsealase mõjuhinnangu käsitlusalasse.

7. **Muud täpsustavad kommentaarid**
   Määruse seletuskirja lk 6 alguses olev lõik „*Võrreldes E-ITSi kehtiva versiooniga on loobutud erinevatest skaaladest (nt kõrge, keskmine, madal), sest normiga ei ole võimalik piiritleda kõikvõimalikke olukordi ja lahendusi, mis võivad organisatsioonides esineda. Organisatsioonil võib olla erinevaid kohustusi, need võivad tuleneda erinevatest õigusaktidest. Neist mõnes on võib olla juba kirjeldatud ka riskihalduse nõudeid, mistõttu ei ole mõistlik E-ITSiga neid nõudeid sätestada. Seega jäetakse edaspidi organisatsiooni enda otsustada, kuidas riske hinnata ja millist skaalat kasutada*“ on mitmeti mõistetav. Ei ole üheselt mõistetav kas see lõik käib ainult riskihindamise kohta või ka kaitsetarbe hindamise kohta? Kui ainult riskide kohta, siis kuidas siduda kaitsetarbe hindamine asutuse enda rakendatud riskikäsitlusega? Kuidas hinnata kaitsetarbe mõju riskikäsitluses? Lisanduvas juhendis võiks olla need lahti seletatud koos soovitusliku riskikäsitlusega.

   Määruse väljasttellimise ja nõuetega on küsimus, kuidas lähtuda E-ITSi meetmest „*OPS.2.1.M7.a Infoturbe meetmete rakendatust tõendab teenuseandja välise audiitori poolt väljastatud E-ITS auditi järeldusotsusega või akrediteeritud*“ kui E-ITS ei põhine enam ISO vastavusel. Kuidas sellest punktist lähtuda, et partneri asutuses olevast ISO-st piisab? Kuidas on tagatud tellija E-ITS-ist lähtuvate nõuete katmine, kui teenuseandja lähtub oma asutuses ISO rakendamisel enda asutuse vajadustest ja teenuslepetes ei reguleerita seetõttu piisavalt täpselt tellija nõudeid?

   Praktikas võib tekkida olukord, kus teenuseosutaja rakendab ISO standardit oma organisatsiooni vajadustest lähtudes, kuid teenuslepingutes ei ole tellija spetsiifilised E-ITSi nõuded piisava täpsusega sätestatud. Ettepanek on täpsustada kuidas peab tellija tagama E-ITS-i nõuete katvuse (all)hanke- ja lepingulistes suhetes.

Lugupidamisega

(allkirjastatud digitaalselt)

Igor Taro
siseminister