SISEMINISTEERIUM

Majandus- ja Kommunikatsiooniministeerium Teie: 10.05.2022 nr MKM/22-0568/-1K

Meie: 17.06.2022 nr 1-7/132-4

Siseministeeriumi vastuskiri "Eesti infoturbestandard" määruse eelnõule

Siseministeerium (edaspidi *SIM*) on tutvunud Majandus- ja Kommunikatsiooniministeeriumi (edaspidi *MKM*) 11.05.2022 kooskõlastamiseks esitatud ettevõtlus- ja infotehnoloogiaministri määruse "Eesti infoturbestandard" eelnõuga (edaspidi *määruse eelnõu*). Kooskõlastame määruse eelnõu järgmiste märkustega arvestamisel.

1. SIM on seisukohal, et Eesti infoturbestandardi (edaspidi *E-ITS*) versioonis tuleks võtta arvesse andmekogude turvatasemete määratlemist. Andmekogude osas jätkub turvaklassi määratlemisel senine ISKE-süsteem K-T-S (käideldavus, terviklikkus, konfidentsiaalsus), mis on reguleeritud edaspidi Vabariigi Valitsuse määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ tasandil. Samas standardis on see väga üldiselt välja toodud ja puudu on andmekogu turvataseme arvesse võtmise praktiline soovitus või juhis.

2. Leiame, et kahjustsenaariumide küsimustikud peavad arvesse võtma organisatsiooni iseärasusi, mistõttu peab olema võimaluse neid sobitada ja vajadusel täiendada. Määruse eelnõu sellist paindlikkust ette ei näe.

3. Määruse eelnõust ei selgu, kuivõrd on lubatud E-ITSi nõuete kohandamine. Näeme vajadust lisada määrusesse, et põhjendatud juhul on lubatud E-ITSi meetme kohandamine andmetöötlejale sobivaks. Näiteks tekib küsimus politsei andmetöötluse spetsiifikast, kus on põhjendamatu, et andmekaitsespetsialist peaks koos personaliosakonnaga otsustama testandmete kasutamise, kui neis võib ilmneda seos isikuga (rida 234, etalonmeetme kood OPS.1.1.6.M11).

4. SIMile tekitab küsimusi E-ITSi rakendumine infosüsteemi puhul, mis on auditeeritavad juba muudel viisidel, näiteks:
    a. infosüsteem toetab sisuteenust, millele rakendatakse eraldi meetmeid ja mida auditeeritakse (nt SIS rahvusvahelise operatiivinfo teenus);
    b. infosüsteemi peab olema Andmekaitse Inspektsiooni (edaspidi *AKI*) poolt auditeeritud, nõue tuleneb EL õigusaktist;
    c. teenust hinnatakse eraldiseisvalt EL poolt (Schengeni hindamine).

    Palume selgitada, kas ja kuivõrd on kirjeldatud protsesse võimalik ühildada ning kas see peab olema andmekogu vastutava töötleja ehk Politsei- ja Piirivalveameti (edaspidi *PPA*) ja järelevalveasutuse ehk AKI ning auditeerija kokkulepe.

5. Leiame, et täpsemini tuleb selgitada, kuivõrd on andmekaitsespetsialisti ülesanded ja kontroll ning E-ITSi meetmete rakendamine ja audit omavahel täiendavad, eristuvad või

Pikk 61 / 15065 Tallinn / 612 5008 / info@siseministeerium.ee / www.siseministeerium.ee
Registrikood 70000562

dubleerivad. Näiteks kas PPA-le tekib täiendavaid ülesandeid, kui asutused hakkavad teavitama asjakohastest intsidentidest (etalonmeetme kood DER.2.1.M4 meede c).

6. E-ITSis on kasutusel andmekaitsespetsialisti kõrval ka termin "andmekaitse juht". Määruse eelnõust ei selgu, mis on tema ülesanne, vastutus või mille poolest ta erineb andmekaitsespetsialistist. Lisaks tekib ka küsimus, et kas E-ITS nõuab andmekaitse juhi määramist või on see vaid võimalus. Palume selles osas eelnõud täiendada.

7. Määruse eelnõu seletuskirjas on selgitatud §-de 5 ja 6 osas, et teenuste kaardistus tuleb koostada Vabariigi Valitsuse 25.05.2017 määruse nr 88 „Teenuste korraldamise ja teabehalduse alused" (edaspidi *TKTA määrus*) alusel. Nõustume, et vajalik on asutuse teenuste süsteemne kirjeldamine, mis on aluseks ka infoturbe meetmete valikul. Kuid TKTA määrus paneb küll kohustuse kaardistada teenused ja sellega seotud protsessid, kuid ei paku ühtegi tööriista. Teeme ettepanekud täiendada kooskõlastusele saadetud määruse seletuskirja ja tuua välja millised on erinevad tööriistad, mis on sobilikud protsesside kaardistamiseks ja analüüsimiseks. Suurema asutuse või valitsemisala korral on erinevad tugiteenused omavahel seotud ning vajalik on vaadata nende omavahelisi sõltuvusi. Ka E-ITSI koolitusel selleks vajalikku tööriista ei pakutud. Rahandusministeerium arendab riigieelarve infosüsteemi, kus on ära toodud ka teenused nii tegevuspõhise eelarve (TERE) kui ka TKTA määruse vaates ning protsessid TERE teenuste elluviimiseks. Loodav infosüsteem ERIS on üks võimalus protsesside süsteemseks kirjeldamiseks. Palume koostöös MKMi digiriigi arengu osakonnaga täpsustada seletuskirja, et pakkuda tehnilisi lahendusi ja tuge määruse rakendamisel.

Infoturbe standardi rakendamiseks vajalikud kulud

Määruse eelnõu seletuskirjas ei ole välja toodud infoturbe standardi rakendamiseks vajalikke täiendavaid ressursse. SIM valitsemisala arvestuslik kulu on järgmine (detailid esitatud MKM-le riigieelarve strateegia materjalides 02.05.2022):

2023	**2024**	**2025**	**2026**
275 992	173 648	174 819	176 217

Juhime tähelepanu, et määruse mõjuga seotud kulud kasvavad just esimestel aastatel. Esiteks kasvavad kulud E-ITS ja selle uue lähenemise juurutamise tõttu ning teiseks auditeerimise, sh vaheauditi, põhiauditi jt läbiviimise vajaduse tõttu. Lisaks võib turul tekkida pakkumiste anomaalia (pakkumise ja nõudluse tasakaal ei ole rakendumise alguses paigas), kuna E-ITSi auditi läbiviijaid on turul vähe: kõigest 11 pakkujat/läbiviijat (Eesti Infosüsteemide Audiitorite ühingu veebilehel olev info). Seega võivad kulud auditi läbiviimise nõudluse suurenemise tõttu tõusta märkimisväärselt.

Palume eelnõu seletuskirja täiendada infoturbe standardi rakendamiseks vajalike ressursside planeerimisega.

Lugupidamisega

(allkirjastatud digitaalselt)

Kalle Laanet
kaitseminister siseministri ülesannetes

Veiko Ristissaar 6125249
veiko.ristissaar@siseministeerium.ee

Alli Murula 6125027
Alli.murula@siseministeerium.ee