# Siseministeeriumi vastuskiri Ettevõtlus ja infotehnoloogiaministri 16. detsembri 2022. a määruse nr 101 „Eesti infoturbestandard“ muutmine

Anname tagasisidet „Ettevõtlus ja infotehnoloogiaministri 16. detsembri 2022. a määruse nr 101 Eesti infoturbestandard“ muutmisele Siseministeeriumi

Siseministeerium (edaspidi *SIM*) on tutvunud kooskõlastamiseks esitatud Ettevõtlus ja infotehnoloogiaministri 16. detsembri 2022. a määruse nr 101 „Eesti infoturbestandard“ muutmise eelnõuga (edaspidi määruse eelnõu). Alltoodud kirjas on Siseministeeriumi tähelepanekud esitatud mitmes osas ja kooskõlastame määruse eelnõu järgmiste märkustega arvestamisel

1. Märkused
   1. Määruse eelnõu lisa 1, punkt 10.2 on toodud nõuded infoturbe halduse süsteemile. Palun täpsustada millist eesmärki kannab regulaarne sõltumatu läbivaatus organisatsioonile, kui peab regulaarselt viima läbi ka E-ITS-i auditi? Kas sellisel juhul on sõltumatu läbivaatus veel täiendavalt vajalik ja mis eesmärki see täidab? Antud meede tähendab suurt täiendavat halduskoormust samas kui juba E-ITSi eel-, põhi-, järel ja vaheaudititega täidetakse vastavat eesmärki.
   2. Määruse eelnõu seletuskirjas (lk 3) on kirjas, et E-ITSi uuendamine toimub iga aasta sügisel – ettepanek uuendada standardit nt 3-5 aastase intervalliga, kuna iga-aastase uuendamisega kaasneb asutustele järjepidev ajaga võidu jooksmine. Teisisõnu, asutused ei pruugi jõuda veel uue versiooni meetodeid kasutusele võtta/nende rakendamiseks plaani teha, kui juba tuleb uus versioon. Eriti keeruline on see suurtes organisatsioonides, kus on palju protsesse, aga samuti ka väikestes organisatsioonides, kus sageli täidab üks inimene paljusid erinevaid rolle.
   3. Üldine tähelepanek – E-ITS ei ütle, kuidas käsitleda protsessile/teenusele määratud kaitsetarvet infosüsteemile määratava turvaklassi osas? – ehk kas need on 1:1 samad või peaks teatud juhul määrama kaitsetarbe infosüsteemile eraldi? Näiteks, kuidas määratleda infosüsteemi turvaklassi, kui see sisaldab kõiki neid tundlikke andmeid, mille tulemusel on ka protsessi kaitsetarve kõrge? Samas aga, kuidas määratleda infosüsteemi turvaklassi juhul, kui protsessi kaitsetarve on suur või väga suur, aga infosüsteemile nii kõrged nõuded ei pea kohalduma (nt infosüsteem ei pea olema 24h kättesaadav, ei tekita probleeme teistes infosüsteemides või ei sisalda selliseid isikuandmeid, mida protsessi käigus muul moel ja teises asukohas töödeldakse) – sellisel juhul võib see olla majanduslikult ebamõistlik rakendada infosüsteemile meetmeid suure või väga suure kaitsetarbe järgi.
   4. Hetkel on asutustesse pandud kohustus koormavam, kui võimalus seda tagada olukorras, kus organisatsioon (rakendab E-ITSi) ise ei taga IKT-teenuseid, vaid seda teeb eraldiseisva asutusena n-ö IT-maja (rakendab ISO-t). Taustakirjeldusena saab välja tuua, et dokumendi „E-ITS Nõuded infoturbe halduse süsteemile“ kohaselt on E-ITSi eesmärk tagada avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmav kaitse ning saavutada infoturbe ühtlane tase nende kõigis osades kogu elutsükli jooksul. (Lisa 1, lk 8). Samas dokumendis on viidatud, et E-ITSi rakendamisega standardturbe ulatuses saavutatakse vastavus rahvusvahelise standardiga ISO/IEC 27001. See vastavus võimaldab E-ITSi rakendajatel oma kaitsealale taotleda rahvusvahelist tunnustamist ISO/IEC 27001 sertifikaadiga. Siinjuures, ISO/IEC 27001 vastavussertifikaat ilma E-ITSi rakendusplaanita E-ITSi rakendatust ei kinnita. (Lisa 1, lk 8).   
      Standardturbe puhul rakendatakse lisaks esmajärjekorras rakendatud põhimeetmetele ka standardmeetmed ja veendutakse etalonturbe välise riskihaldusega etalonturbe meetmete piisavuses. Vajadusel rakendatakse olenevalt kaitsetarbest kõrgmeetmed ja etalonturbe välised lisameetmed. Väljajäetud põhimeetmeid ja standardmeetmeid põhjendatakse, lähtudes eelkõige riskide aktsepteerimise kriteeriumitest. (Lisa 1, lk 8).

Samas Eesti Infoturbestandardi lehel on leitav täna kehtiv vastavustabel E-ITSi 2022 versiooni vastavustabel ISO/IEC 27001:2017 standardi nõuetele, mille enam kui 4000+ meetmest umbes pooled s.o 2000+ on üksnes osaliselt vastavuses, neist valdav enamus põhi- ja standardmeetmed. Seetõttu teeme ettepaneku ettepaneku palun selgitada õigusselguse huvides, kas ISO meetmed hakkavad lähiaastal vastama kõigile E-ITS meetmetele? Ja kui ei, siis millise erisusega käsitletakse organisatsioonile pandud vastutuskohustust (lisa 1, lk 10), kui vastavuse tagamine ei sõltu organisatsioonist endast? Või alternatiivselt, kuidas vastutus ja ülesanded vastavuserisuste mittekaotamisel jaotatakse?

* 1. Palume kaaluda antud määruse alusel muuta Riigi Kinnisvara AS (edaspidi RKAS) E-ITSi kohuslaseks. Peamine põhjus peitub selles, et RKAS haldab täna väga suurt osa riigi kinnisvarast, kus on kasutusel mitmesuguseid taristu ja infotehnoloogia komponente, mis mõjutavad klientide infoturvet ja halvemal juhul võivad kaasa tuua suure mõjuga intsidendi. Teiseks on RKAS-i puhul oluline roll turvalise tarneahela tagamisel ja see oleks oluline tarneahela riskide maandamismeetmena.

1. Meetmed:
   1. Miks nii CON.2.M2 Andmekaitsespetsialisti (andmekaitseametniku) määramine kui ka kõik CON.2 meetmed on sisustatud kitsalt IKÜM kaudu? Ka muus osas pole mainitud näiteks IKS või muu asjakohase regulatsiooni kohaldumist. Interpoli andmetöötlusreeglite alusel peab olema ka määratud andmekaitseametnik ja infoturbejuht ning rakendatud turvameetmed jne. Näiteks CON.2.M29 on sisse toodud avaliku sektori erisusena AvTS.
   2. Kui eITS on infoturvapoliitika ja – protsessi jne keskne, andmekaitse on konkreetsemalt pildil CON 2, siis kas või miks pole infoturvapoliitika ja – protsessi jne teemades andmekaitset/andmekaitsespetsialisti eraldi välja toodud, vaid see on konkreetsemalt vaid CON2?
   3. CON.2.M26 b. järgi viiakse andmekaitseaudit läbi vähemalt kord nelja aasta jooksul. Kas see on sama süsteem, mis nimetatud lisas 3 (eel-, põhi-, järel- ja vaheaudit)? Näiteks SIS ja VIS audit oli Andmekaitse Inspektsioonil (AKI) üles ehitatud ISO standardile, samuti on nende tulevased (2024. a alguse saavad) logide auditid ISO meetmete põhised. EL õigusaktidest tuleneb aga mitte vastutavale töötlejale, vaid järelevalveasutusele kohustus viia kas konkreetselt määratletud või umbkaudse intervalli järel auditeid. Kas praktikas see vaadatakse üle kas PPA ja AKI auditid oleks vaheldumisi? Asutusel on juba iga-aastaseid auditeid ja iga lisa audit on dubleerimine ja täiendav koormus. Palume täiendavalt luua välja selgitused ja arvestada teiste võimalike audititega.
2. Täiendavad tähelepanekud määruse eelnõule ja sõnastuse kohta:
   1. Palume täpsustada määruse lisa 1 punktis 4 sõnastust. Hetkel on segadus on sõnastuses, mille järgi E-ITS vastab ISO standardile. Sellest jääb mulje, otsekui oleks ISO standard midagi väga detailset ja spetsiifilist ning E-ITS proovib sellele vastata. Tegelikkus on ju vastupidine, ISO on palju üldisem. Kas me saame selle pinnalt öelda, et üks vastab teisele?
   2. Palun täpsustada määruses millal kasutada infoturva ja millal infoturve/infoturbe. Täiendavat selgitust oleks vaja, kuna probleemid tekivad nt muukeelsete dokumentide jms tõlkimisel eesti keelde. Tõlk võib tõesti aru saada, milline on semantiline vms vahe, ent tavainimese jaoks on see keeruline. Eriti kui läbivalt on tekstis kasutusel mõlemad.
   3. Lisa 1 punktis 7.1.3 tuuakse välja tarneahela hindamine väljas tellitavatele teenustele. Palume täpsustada või sõnastada antud punkt täpsemaks ja selgemaks eelkõige missugustele väljast tellitavatele teenustele peab selle tegema ja kuhu kirjeldama.