Lp majandus- ja tööstusminister hr Erkki Keldo
Majandus- ja Kommunikatsiooniministeerium
info@mkm.ee

28. oktoober 2024

Ettepanek küberturvalisuse seaduse alusel kehtestatud määruse "Võrgu- ja infosüsteemide küberturvalisuse nõuded" muutmiseks

Pöördume seoses ettepanekuga muuta küberturvalisuse seaduse („KüTS") §7 lõike 5 alusel kehtestatud määrust „Võrgu- ja infosüsteemide küberturvalisuse nõuded" (edaspidi *määrus*). Määruse §4 lg 1 kohaselt peab teenuse osutaja tagama Eesti infoturbestandardi („E-ITS") tingimuste täitmise auditi läbiviimise iga kolme aasta järel. Oleme arvamusel, et praegusel kujul kehtestatud auditeerimiskohustus on paljudele esmatasandi tervishoiuteenuste osutajatele ebaproportsionaalselt koormav. Kuigi määruse §4 lg 4 kohaselt on ette nähtud erandid, millistel juhtudel auditeerimiskohustus ei kehti, ei ole erandid piisavad ning ei täida eesmärki, mis on erandite määramisel seatud.

Praeguse regulatsiooni järgi kohaldub E-ITS auditeerimiskohustus ka väikeettevõtjatele, s.o. teenuseosutajatele, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aastakäive ei ületa 10 miljonit eurot, arvestades mikroettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L124, 20.05.2003, lk 36–41). Selliste väikeettevõtjatest teenuse osutajate hulgas on ka hinnanguliselt üle 200 perearstikeskuse. Paljud väga väikesed, üksnes 2-3 nimistuga perearstikeskused ületavad aga mikroettevõtja definitsiooni lävendit, sest neil on üle 10 töötaja. Sellegipoolest on aga tegu väga väikeste keskustega, kes tegutsevad piiratud ressurssidega. Selliste perearstikeskuste osas auditeerimiskohustuse sätestamine on ebaproportsionaalne ning ka ebavajalik, arvestades andmetöötluse eripära, majanduslikke põhjendusi, küberriskide olulist mõju ja proportsionaalsust.

Toome siinjuures oma seisukohtade detailsema põhjenduse.

1. **Tervishoiusektor tagab ajalooliselt ja valdkonna eripärast tulenevalt andmetöötluse turvalisuse keskmisest oluliselt kõrgemal tasemel**

Perearstikeskused töötlevad igapäevaselt hulgaliselt isikuandmeid ning eriliiki isikuandmeid. Kõikide tervishoiuteenuse osutamisse kaasatud isikute suhtes kehtib konfidentsiaalsuskohustus võlaõigusseaduse („VÕS") §768 järgi. VÕS regulatsiooni järgi peab tervishoiuteenuse osutaja

hoidma saladuses kõikvõimalikke andmeid patsiendi ja tema tervise kohta, kui seaduses või kokkuleppel patsiendiga ei ole ette nähtud teisiti. Sarnaselt advokaadi kutsesaladuse ja vaimuliku pihisaladuse kaitseb patsiendisaladus ehk arsti kutsesaladus usaldussuhet arsti ja patsiendi vahel. See on üldtunnustatud põhimõte, mille eesmärk on ühelt poolt tagada patsiendi privaatsus, aga teisalt ka tema usk meditsiinisüsteemi, mille puudumisel ei pruugi inimene ravile tulla ning võib seetõttu ohustada ennast ja teisi. Patsiendisaladuse mõiste on lai ning patsiendisaladuse kohta on Riigikohus selgitanud, et näiteks kriminaalmenetluses pole tervishoiutöötajal mitte üksnes õigus, vaid lausa kohustus keelduda patsiendi kohta ütluste andmisest ja dokumentide avaldamisest (RKKK 1-20-5071). Seega, tervishoiusektor on ajalooliselt ja juba valdkonna eripärast lähtuvalt majandusharu, kus väärtustatakse konfidentsiaalsust ja andmetöötluse turvalisust. Sellest tulenevalt on erinevad infoturbeprotsessid tervishoiusektoris tööprotsessides sisse kirjutatud juba ammu enne KüTSi jõustumist. Tervishoid on olemuselt valdkond, kus andmetega käiakse keskmiselt hoolsamalt ringi ning kus infoturbesse suhtutakse keskmisest tõsisemalt.

2. **Majanduslikud ja ressursilised piirangud ja piiratud IT-võimekus**

Kuigi meditsiin on valdkond, kus andmed on hoitud keskmiselt turvalisemalt, siis samal ajal on väiksemate perearstikeskuste ja tervisekeskuste IT-võimekus keskmisest madalam. Väiksemad perearstikeskused ja teised meditsiinikeskused tegutsevad sageli piiratud ressurssidega. Keskmises perearstikeskuses ei ole enda IT-osakonda ega IT-tuge, vaid tavapäraselt ostetakse IT-teenused sisse. E-ITS nõuete regulaarne auditeerimine nõuab aga spetsiifilisi IT-valdkonna teadmisi. IT-partnerite hinnangul nõuab E-ITS auditeerimine keskmise perearstikeskuse puhul vähemalt 100 tundi vastava IT-spetsialisti tööd. Lisaks peavad auditi tegemisse olema kaasatud keskuse enda töötajad – arstid, õed ja ülejäänud personal. Seda rahastust pole arvestatud üldarstiabi rahastuse kulumudelisse. Kokkuvõtlikult tähendab eeltoodu, et IT-süsteemide regulaarsed auditid nõuavad olulisi finants- ja inimressursse, mis võiksid muidu olla suunatud patsientide teenindamiseks ja oluliste tervishoiuteenuste osutamiseks. Väiksemate perearsti- ja tervisekeskuste sundimine suunama ressursse regulaarsete IT-auditi tegemisele võib ohustada ka nende elujõulisust. Eriti ohtlik on see maa piirkondade jaoks, kus tervishoiu võimalused on niigi piiratud.

3. **Küberriskide olulisus**

Kõik perearstikeskused ei seisne sama suure küberturvalisuse riski ees, mis põhjendaks E-ITS auditeerimise vajadust iga 3 aasta järel. Väiksemad ja keskmised perearstikeskused töötlevad vähemtundlikke andmeid võrreldes suuremate haiglatega. Seega on perearstikeskused madalama riskitasemega võrreldes näiteks suurte Haiglavõrgu arengukava haiglatega, kus teostatakse operatsioone ning teisi suuremaid protseduure. Perearstikeskuste puhul on ka risk terviseandmete juurdepääsule küberintsidendi korral väiksem. Perearstikeskuse IT-süsteem dubleerib riigi poolt hallatavat Terviseportaali. Kõik tervishoiuteenuse osutajad saadavad andmed Tervise infosüsteemi kaudu Terviseportaali. Terviseportaali kaudu on patsiendi terviseandmed kättesaadavad ka siis, kui perearstikeskus peaks olema langenud küberintsidendi ohvriks ning perearstikeskuse süsteemid on näiteks ajutiselt lukustatud.

4. **Proportsionaalsus**

Ka praegu kehtiva küberturvalisuse seaduse seletuskirjas on auditeerimiskohustuse osas nenditud, et on võimalik, et auditeerimiskulud on majanduslikult koormavamad subjektidele, kelle IKT korraldus on oluliselt väiksema mahuga (nt suur osa perearstidest). Seletuskirjast tulenevalt oli seaduseelnõu eesmärk majandusliku mõju tasakaalustamiseks auditikohustust

kehtestava rakendusakti kavandis ettenähtud ka erand mikroettevõtjatele (nt suurele osa tegutsevatele perearstidele). Nagu eelpool punktides põhjendatud, siis praegune erand mikroettevõtjatele ei ole piisav. E-ITS auditeerimiskohustuse lävend on väga madal ning iga kolme aasta tagant kohalduv auditeerimiskohustus on ebaproportsionaalselt koormav ka perearstikeskustele, kes on keskmise suurusega ettevõtjad.

Lähtudes eelnevast teeme **ettepaneku**:

1) Muuta määruse „Võrgu-ja infosüsteemide küberturvalisuse nõuded“ §4 lg 4 p1 sõnastust ning sõnastada säte järgnevalt: 1) teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aasta bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades mikroettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L124, 20.05.2003, lk 36–41).
2) alternatiivselt, täiendada määruse §4 lg 4 uue punktiga 4 järgmises sõnastuses: 4) perearstikeskusest või tervisekeskusest teenuse osutajale, kellel on majandusaasta jooksul keskmiselt alla 50 töötaja ja kelle aasta bilansimaht või aastakäive ei ületa 10 miljonit eurot, arvestades mikroettevõtjate määratlusi Euroopa Komisjoni soovituses 2003/361/EÜ mikro-, väikeste ja keskmise suurusega ettevõtjate määratlemise kohta (ELT L124, 20.05.2003, lk36–41).

Lugupidamisega

Kersti Esnar

Tegevjuht
Eesti Esmatasandi Tervisekeskuste Liit
info@ettkl.ee