



Kadri Luga
Rapla Perearstikeskus OÜ
Rapla.perearst@gmail.com

30.04.2024 nr 8-1/23-0291/24735

VÄLJAVÕTE

Järelevamemenetluse lõpetamine

Austatud Kadri Luga

Riigi Infosüsteemi Amet (edaspidi RIA) alustas 18.09.2023 saadetud järelepärimisega nr 8-1/23-0291/231394 Rapla Perearstikeskus OÜ (edaspidi RPK) suhtes riikliku järelevamemenetluse, mille eesmärk oli kontrollida RPK poolt küberturvalisuse seaduse (edaspidi KÜTS) §-des 7 ja 8 sätestatud nõuete täitmist.

Järelevamemenetluse läbiviimisel kontrolliti nõuetekohast täitmist järgmiste tegevuste osas:

1. alaliste organisatsiooniliste, füüsiliste ja infotehniliste turvameetmete rakendamine küberintsidentide ennetamiseks, lahendamiseks ja leevendamiseks (asjakohaste infoturbealaste tegevuste korraldamine, sh infoturvet korraldavate organisatsiooniliste dokumentide (strateegia, korrad, poliitika, arvutivõrgu arhitektuuriline üleskirjutus, juhised jm) olemasolu ja nende rakendamine);
2. võrgu- ja infosüsteemi riskide haldamine;
3. küberintsidentide käsitlemine ja teavitamine.

Järelevamemenetluse jooksul küsiti välja asjassepuutuvaid dokumente, analüüsiti neid ning viidi kohapealse kontrolli käigus läbi intervjuud ning täpsustati tehnilisi aspekte RPK vastava valdkonna eest vastutavate esindajatega. Kohapealne kontroll toimus 06.10.2023, millele järgnes edasine suhtlus. Kontrollakt allkirjastati mõlemapoolselt 18.04.2024.

Lähtuvalt eeltoodust ja vastavalt haldusmenetluse seaduse § 43 lõike 1 punktile 1 **lõpetab RIA RPK suhtes algatatud järelevamemenetluse**, kuivõrd järelevametoimingute tulemusena jõuti järeldusele, et RPK on loonud infoturbe halduse süsteemi (ISMS), tegeleb asjakohaste infotehnoloogiliste turvameetmete rakendamisega ulatuses, mis loob eeldused küberintsidentide ennetamiseks ja lahendamiseks ning infoturbeteadlikuks teenuseosutamiseks. RIA hinnangul on KÜTS-ist tuleneva kohustuse täitmine kontrollitu ulatuses piisav. Soovitame jätkata senist praktikat turvameetmete alalise rakendamise osas.

KÜTS § 7 sätestatud nõuete paremaks täitmiseks ning võrgu- ja infosüsteemi turvariskide vähendamiseks soovitame hoida infoturvet reguleerivad juhised ja kinnitatud töökorralduslikud reeglid ajakohasena ja vastavuses Eesti Infoturbestandardiga (E-ITS), arvestades seejuures muutuvat infoturbe olukorda laiemalt ning kontrollida reeglite täitmist oma töötajatelt ning partneritelt.

