Ravispaade (medical spa) auditi raport

Käesolev audit on osa kolme Balti riigi koostööprojektist, milles lepiti kokku möödunud aasta alguses Vilniuses toimunud Balti riikide andmekaitseasutuste kohtumisel. Eesti, Läti ja Leedu andmekaitsjad otsustasid auditeerida kõigis kolmes riigis tegutsevaid ravispaasid isikuandmete kaitseks kehtestatud infoturbe nõuete täitmise osas. Auditi läbiviimise aluseks oli ühiselt koostatud 42st küsimusest koosnev küsimustik.

Auditi eesmärk

Eestis viidi ravispaade audit läbi 2014. aasta maist kuni novembrini ning selle eesmärgiks oli kontrollida, kas ettevõtted järgivad oma tegevuses isikuandmete kaitse seaduses (edaspidi IKS) sätestatud põhimõtteid ehk kas isikuandmeid kogutakse seaduspäraselt ja seaduslike eesmärkide saavutamiseks, kas isikuandmeid töödeldakse kooskõlas isikuandmete kaitse seaduses (IKS) sätestatuga, samuti seda, kas isikuandmeid kogutakse ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks.

Auditi käigus jälgiti peamiselt viit aspekti: kuidas andmeid töödeldi (paberil ja/või elektrooniliselt); kuidas oli korraldatud juurdepääs andmetele ja kuidas toimus kasutaja identifitseerimine ja autentimine (sisse logimine); kuidas on tagatud andmete säilitamine (varundamine), millised on säilitamise tähtajad, sh logimisel; kas ja kuidas toimub andmete edastamine kolmandatele isikutele, sh teistele asutustele ning kuidas toimub andmete hävitamine (kustutamine) nii paber- kui ka digitaalsete andmekandjate puhul.

Auditi viisid läbi Andmekaitse Inspektsiooni (edaspidi AKI) andmeturbeekspert Boris Põldre (Eesti Infosüsteemide Audiitorite Ühingu liige) ning järelevalve vaneminspektorid Raavo Palu ja Kuldar Võsar. Auditi käigus tutvusid auditeerijad 12 Eestis asuva ravispaa infotehnoloogilisele keskkonnale juurdepääsu, keskkonda sisselogimise ning vastava dokumentatsiooniga (juhendid, eeskirjad ja tervisetõendid). Muuhulgas intervjueeriti ka võtmeisikuid, jälgiti tööprotsesse ning viidi läbi asjakohaseid kontrolliprotseduure.

Tulemused

Audit viidi läbi Kalev Spas, Viiking Spa Hotellis, Tervise Ravispaahotellis, Tervise Paradiisi spaa-hotellis & veekeskuses, Taastusravikeskuses Estonia, Tallinn Viimsi Spas, Fra Mare Thalasso Spas, Spa Hotellis Laine, Narva-Jõesuu Spas ja Sanatooriumis, Toila Spa Hotellis, Pühajärve Spas ja Puhkekeskuses ning Taastusravis & Hotellis Wasa.

Auditeerijate väitel järgisid kõik 12 ravispaad oma töös seaduslikkuse põhimõtet ning tulenevalt IKS § 30 lõikest 1 on määranud isikuandmete kaitse eest vastutav isiku ning peetakse andmetöötlemiste registrit või IKS § 27 lõikest 1 on registreerinud delikaatsete isikuandmete töötlemise Andmekaitse Inspektsioonis. Isikuandmeid koguti tervishoiuteenuse osutamisel üksnes eesmärgipäraselt ning ulatuses, mis seadusest tulenevalt on vajalik määratletud eesmärkide saavutamiseks. Samuti vastasid kõik 12 auditeeritud ravispaad isikuandmete kaitse seaduse § 6 sätestatud põhimõtetele ja täitsid § 25 lõikest 2 tulenevaid turvameetmeid, järgides infoturbe eesmärki ja strateegiat.

Kontrollimise käigus jälgiti ka infoturbe vastavust muudele õigusaktidega kehtestatud tehnilistele normidele ja nõuetele, mille järgimine on teenuse osutamise seisukohast oluline, nagu näiteks videovalvesüsteemi kasutamisele kehtestatud nõuded, samuti töötajatega, aga ka lepinguliste partneritega sõlmitud lepingutes sisalduva konfidentsiaalsuskohustuse nõude

täitmist. Kontrolli tulemusel saab kinnitada, et ravispaad järgisid olulises osas organisatsioonilisele turbele sätestatud tehnilisi norme ja nõudeid.

Kokkuvõte

Eesti ravispaad töötlesid (koguvad ja kasutavad) isikuandmeid vastavalt seadusele ning ainult määratletud eesmärkide saavutamiseks ega töödelnud neid muul eesmärgil. Andmeid töödeldi nii paberkandjal kui digitaalselt. Paberdokumente hoiti arsti kabinetis lukustatud kapis või seifis. Juurdepääsu võimaldamine infosüsteemis sisalduvatele andmetele oli kooskõlas kasutajale antud õigustega. Kaugjuurdepääs andmetele puudus.

Viirustõrje tarkvara kasutamise näol oli tagatud ka isikuandmete kaitse seaduse § 25 lõike 2 punkti 7 täitmine. Andmeid varundati regulaarselt. Kolmandatele isikutele, sealhulgas teistele asutustele isikuandmeid ei edastatud.

Videovalvesüsteemi andmeid väljastati vajadusel taotluse alusel, näiteks politseile ning väljastamine fikseeriti kohapeal.

Andmete hävitamiseks (kustutamiseks) kasutati rahvusvahelistele normidele vastavat dokumentide ja andmekandjate hävitusteenust, paberkandjatel sisalduvate andmete puhul ka nn lokaalset paberihunti.

Soovitused

Kuigi auditi käigus ei tuvastatud olulisi riske ja mittevastavusi IKS § 25 lõigete 2 ja 3 nõuetele, juhib Andmekaitse Inspektsioon tähelepanu asjaolule, et infoturve on pidev protsess, mis nõuab pidevat parendamist ja kaasajastamist, samuti töötajate järjepidevat kursis hoidmist tehtud muudatustega.

Õiguslik dokumentatsioon (juhised, eeskirjad, kasutamise korrad jne) tuleb hoida ajakohasena: regulaarselt läbi vaadata, täiendada ja vajadusel kehtivaid dokumente muuta. Samas tuleks vältida sarnase sisukirjeldusega dokumentide ja reeglistike olemasolu.