Tervise- või perearstikeskuste järelevalve 2015

2015. aastal viisime läbi 22 tervise- või perearstikeskuses (edaspidi TTO ehk tervishoiuteenuste osutajad) järelevalve eesmärgiga kontrollida, kas TTO-d järgivad oma tegevuses isikuandmete kaitse seaduses (edaspidi IKS) sätestatud põhimõtteid. Tervishoiuteenuse osutajatega ja tervishoiuteenustega puutuvad suuremal või vähemal määral kokku kõik Eesti elanikud.

Järelevalve eesmärk oli hinnata,
1. Kas andmete töötlemisel lähtutakse ja järgitakse isikuandmete kaitse seaduse § 6 põhimõteid ning täidetakse sealhulgas:
    1.1. seaduslikkuse põhimõtet – isikuandmeid kogutakse vaid ausal ja seaduslikul teel;
    1.2. eesmärgikohasuse põhimõtet – isikuandmeid kogutakse üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas;
    1.3. minimaalsuse põhimõtet – isikuandmeid kogutakse ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks.
2. Andmete töötlemise viisi (paber, elektrooniline andmetöötlus).
3. Juurdepääsu andmetele; infosüsteemi kasutamise korda sh kasutaja identifitseerimist, autentimis ja logimist.
4. Andmete säilitamist (varundamine).
5. Andmete edastamist e-tervise infosüsteemi või kolmandatele isikutele, sealhulgas teistele asutustele/ettevõttele.
6. Andmete (nii digi kui paber andmekandjate) hävitamist.
7. Riistvara sh serverite ja andmete ning tarkvara haldust.

Audit viidi läbi kahes etapis.
I etapiga esitati TTO-le küsimustikud 31 küsimusega, sh küsisime:

- infosüsteemi üldandmeid (kasutatava tarkvara nimetus, versiooni number ja tootja);
- infoturbe halduse küsimusi, sh küsimused koolituse, kirjalike infoturbe juhendite ja eeskirjade kohta;
- infosüsteemi kontrollisüsteemi (logidesüsteem) olemasolu, mis talletab sisenemisajad, tagades, et süsteemist ei ole võimalik andmeid ilma vastavate volitusteta kustutada, lisada ega muuta;
- andmete varundamist ning samuti edastamist (väljastamist) ehk kas ja kuidas on korraldatud infosüsteemi kaughooldus volitatud töötlejate poolt? Kas, kuidas ja kelle poolt toimub varukoopiate tegemine?

Samuti uurisime, kas TTO on liidestatud tervise infosüsteemiga (Digilugu) ja kas ning millisel kujul edastatakse andmeid kolmandatele isikutele (sh politsei, kohus, välisriik jne).

Järelevalve II etapi raames teostasime kohapealse TTO-de intervjueerimised, kus arvestati I etapi tulemusi (vastuseid).

Järelevalve tulemusel jõudsime järgmiste järeldusteni.

1. Isikuandmete töötlemine TTO-des vastab IKS-i § 6 põhimõtetele, st andmete töötlemine on eesmärgikohane, seaduslik ning järgitakse minimaalsuse printsiipi.
2. Kaugtööd TTO-d ei kasuta, samas volitatud töötlejale (tarkvara tootjale) on võimaldatud tarkvara kaughooldus.
3. Kõik TTO-d väljastavad andmed ainult kirjaliku või digitaalse taotluse esitamisel ning kõik toimingud registreeritakse vastavas päevikus.

4. Kõik TTO-d on liidestatud e-tervise infosüsteemiga (Digilugu). Andmeid edastatakse jooksvalt siis, kui andmed on valmis edastamiseks. Kõik TTO-d kasutavad digiloo andmeid ehk andmete liikumine on kahesuunaline, st TTO-st Digilukku ja vastupidi ehk TTO-d kasutavad Tervise infosüsteemi andmeid oma töös (infosüsteemis)
5. Paberdokumentide töötlemisel vastab isikuandmete töötlemise nõuetele nii hoiustamine kui hävitamine.
6. Andmete kasutamine ehk juurdepääs infosüsteemi andmetele on aktsepteeritud ainult konkreetse TTO töötalatele.
7. Andmete varundamine toimud automaatselt iga päev.
8. Andmeid edastatakse x-tee kaudu ja krüpteeritult.

AKI soovitused TTO-le:

1. Suuliste lepete probleem – neid on raske tõendada ning AKI soovitab lisaks suulistele lepetele vormistada need kirjalikult, sh korraldused, mis reguleerivad TTO-de põhimõttelisi küsimusi nagu infosüsteemi kasutamine, juurdepääs andmetele (kasutamine) ning samuti andmete väljastamise kord jne.
2. Samas juhtisime TTO-de tähelepanu asjaolule, et infoturve on pidev protsess, mis nõuab pidevat parendamist, tõhustamist (kaasajastamist) ning tööd. Tegelik olukord infoturbe osas ei pruugi vastata kehtivates dokumentides esitatud nõuetele. Kehtiva ja kaasajastatud infoturbereeglistiku puudumisel või juhul, kui töötajad ei ole nendega tutvunud, ei pruugi töötajad olla vajalikul määral teadlikud infotehnoloogiaga seotud riskidest ning oma osast turvaintsidentide ärahoidmisel.
3. Konfidentsiaalsuse nõudena peab olema väljatoodud nõue, et isik on kohustatud hoidma saladuses talle tööülesannete täitmisel teatavaks saanud isikuandmeid ka pärast töötlemisega seotud tööülesannete täitmist või töö- või teenistussuhte lõppemist.

Otsus: TTO-de poolt rakendatavad turvameetmed ei põhjusta isikuandmete kadu või isikuandmete omavolilist kasutamist ehk on tagatud isikuandmete kaitse seaduse § 25 lõike 2 turvanõuete täitmine. Olukord TTO-des andmete töötlemise küsimustes on rahuldav.

17.12.2015
Koostas: Boris Põldre