ANDMEKAITSE INSPEKTSIOON

Lp TTO-de kasutatavate
kliendisuhtluskeskkondade seires
osalejad

Meie 28.01.2026 nr 2.1.-4/25/476-1676-8

TTO-de kasutatavate kliendisuhtluskeskkondade seire kokkuvõte ja soovitused

Andmekaitse Inspektsioon (AKI) algatas isikuandmete kaitse üldmääruse[1] (IKÜM) art 58 ja isikuandmete kaitse seaduse § 56 alusel omaalgatusliku seire, mille eesmärk oli kaardistada tervishoiuteenuse osutajate (TTO) poolt kasutatavate kliendisuhtluskeskkondades isikuandmete töötlemisega kaasnevad võimalikud kitsaskohad. Seire läbiviimise põhjuseks on asjaolu, et AKI on täheldanud erinevates valdkondades (sh tervishoius) andmetöötlejate poolt isikuandmete töötlemise käigus teenuste kasutamist ilma, et seda oleks reguleeritud kirjalike andmetöötluslepingutega. Terviseandmete puhul on tegemist eriliiki isikuandmetega[2], mille töötlemisel tuleb olla eriti hoolikas.

Seire küsimustiku saatis AKI 2025. aasta mais viiele TTO-de kasutatava kliendisuhtluskeskkonna haldajale - Certific OÜ, ePerearstikeskus OÜ, AS MEDISOFT, Minudoc OÜ ja VIVEO Health OÜ. AKI-le vastasid kõik küsimustiku saajad.

Küsimustik sisaldas 15 küsimust, mis hõlmasid keskkondade eesmärki, funktsionaalsusi, rolli- ja lepingukorraldust, säilitustähtaegasid, andmesubjekti taotluste lahendamist ja turvalisust.

Kliendisuhtluskeskkondade eesmärk ja funktsionaalsus

Kõigi valimisse sattunud keskkondade eesmärk on võimaldada klientidele vastuvõttude broneerimist TTO juures. Osa keskkondi võimaldab lisaks broneerimisele ka kliendi ja TTO vahelist suhtlemist – pöördumiste edastamine, tagasiside, failide vahetus, video- ja telefonivastuvõtt.

Täismahus funktsionaalsuse puhul töödeldakse keskkonna vahendusel regulaarselt suuremas ulatuses isikuandmeid (sh terviseandmeid) kui vaid broneeringut võimaldavates keskkondades ning seetõttu vajavad suurema funktsionaalsusega keskkonnad küpsemat rolli-, logi-, säilitus- ja lepingukorraldust. Andmekaitsealased riskid on funktsionaalsuse erinevusest tingituna platvormide vahel erinevad ning iga keskkonna haldaja kui ka vastavat keskkonda kasutav TTO peab neid riske hindama.

Nõue, et vastutav töötleja ja volitatud töötleja peavad isikuandmete töötlemisel riske hindama, tuleneb peamiselt IKÜM-st, eriti seoses isikuandmete turvalisuse tagamisega. Nimelt tuleks isikuandmeid töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahju eest. Selleks peaksid vastutavad töötlejad ja volitatud töötlejad võtma asjakohaseid tehnilisi ja korralduslikke meetmeid,

[1] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679.
[2] IKÜM art 9 lg 1.

et kaitsta isikuandmeid võimalike ohtude eest. Neid meetmeid tuleks hinnata, võttes arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning töötlemise laadi, ulatust, konteksti ja eesmärke, samuti töötlemisest üksikisikute õigustele tekkivaid erineva tõenäosuse ja suurusega ohte.[3]

Kuigi puhtalt broneerimise eesmärgil kasutatava keskkonna puhul võivad andmekaitse riskid olla mõnevõrra väiksemad, siis tuleb ka selliste keskkondade puhul silmas pidada, et töödeldakse IKÜM art 9 lg 1 mõistes eriliiki andmeid, st terviseandmeid. IKÜM pp 35 kohaselt kuuluvad tervisealaste isikuandmete hulka kõik andmesubjekti tervislikku seisundit käsitlevad andmed, mis annavad teavet andmesubjekti endise, praeguse või tulevase füüsilise või vaimse tervise kohta. See hõlmab teavet füüsilise isiku kohta, mis on kogutud füüsilisele isikule tervishoiuteenuste registreerimise või osutamise käigus. Euroopa Kohus on selgitanud, et terviseandmete definitsiooni tuleb mõista laialt.[4] Seega, kui broneerimissüsteemis on olemas andmed teenuse liigi kohta (nt kardioloog, psühholoog), saatekirja info, diagnoos, uuringud vms, siis need annavad teavet isiku tervisliku seisundi kohta ja on seega terviseandmed IKÜM mõistes. Töödeldavate terviseandmete hulka võib suurendada lisaks ka broneerimiskeskkonnas vabade tekstiväljade olemasolu, kuhu patsient võib sisestada mistahes infot. Riski, et tundlikke andmeid töödeldakse ilma piisavate kaitsemeetmeteta, võib suurendada omakorda asjaolu, kui keskkonda haldav andmetöötleja ise ei pea seejuures end terviseandmete töötlejaks nagu seirele antud vastustest ühe keskkonna puhul välja tuli.

Andmetöötlusleping ja andmetöötleja roll

Isikuandmete töötlemisel eristatakse andmetöötleja rolli sõltuvalt vastutusest. Vastutav töötleja kannab isikuandmete töötlemisel üldist vastutust ja on kohustatud tagama isikuandmete töötlemise põhimõtete järgimise. Vastutav töötleja määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid ning vastutab nii tema poolt kui tema nimel toimuva mis tahes isikuandmete töötlemise eest.[5]

Volitatud töötleja töötleb isikuandmeid vastutava töötleja nimel[6] ja tegutseb viimase juhiste alusel. Kui volitatud töötleja määrab ka ise isikuandmete töötlemise eesmärgid ja vahendid, loetakse volitatud töötleja selle töötlemistoimingu suhtes vastutavaks töötlejaks.

Vastutav töötleja peab volitatud töötleja valimisel olema hoolikas ja valima töötleja, kes esitab piisavad tagatised nii tehniliste turvameetmete kui ka korralduslike meetmete kohta isikuandmete kaitseks. Volitus andmete töötlemiseks peab olema vormistatud kirjalikult lepingu või Euroopa Liidu või liikmesriigi õiguse kohase siduva õigusakti alusel. Andmetöötlusleping reguleerib vastutava ja volitatud töötleja suhet ja piiritleb nende omavahelised rollid. Seetõttu peavad lepingus olema üksikasjalikult kirjeldatud töötlemise sisu ja kestus, töötlemise laad ja eesmärk, isikuandmete liik ja andmesubjektide kategooriad ning poolte kohustused ja õigused.[7] Seega, kui andmetöötleja kasutab isikuandmete töötlemisel vahendusteenust (nt kliendisuhtluskeskkonda), on vajalik poolt vahel sõlmida andmetöötlust reguleeriv leping, mis vastab IKÜM artiklis 28 toodud nõuetele.

Seires osalejatel on erinevate teenuste osutamise osas erinevad rollid. Kui TTO ja keskkonna vahel on lepinguline suhe, siis on seires osalejate puhul keskkond volitatud töötlejaks ja TTO vastutavaks töötlejaks ning õigused ja kohustused on kokku lepitud andmetöötluslepingus. Keskkond võib samas olla ka alltöötlejaks, mispuhul on TTO sõlminud lepingu teise volitatud töötlejaga. Seires osales ka platvorm, mis tegutseb iseseisva vastutava töötlejana.

[3] IKÜM art 5 lg 1 p f , art-d 25 ja 32.
[4] Euroopa Kohtu 04.10.2024 otsus kohtuasjas C-21/23 (Lindenapotheke), p 43 ja 81.
[5] IKÜM art 4 p 7.
[6] IKÜM art 4 p 8.
[7] Andmetöötluslepingu elemendid on loetletud IKÜM artiklis 28.

Euroopa Andmekaitsenõukogu on selgitanud oma suunises 07/2020, et vastutava töötleja ja volitatud töötleja mõisted on funktsionaalsed: nende eesmärk on jaotada vastutus töötlejate tegeliku rolli kohaselt. See tähendab, et töötleja õiguslik staatus kas vastutava või volitatud töötlejana tuleb põhimõtteliselt määrata selle alusel, milline on tema tegelik tegevus konkreetses olukorras, mitte ametliku määramise teel (näiteks lepinguga). See tähendab, et rollide jagamine peaks tavaliselt tulenema juhtumi faktiliste elementide või asjaolude analüüsist ja sellisena ei ole see läbiräägitav.[8]

Keskkond kui iseseisev vastutav töötleja

Kuigi seire raames ei esitatud konkreetseid küsimusi keskkondades konto loomise kohta, juhib AKI täiendavalt tähelepanu, et platvormile sisenemisel ja kasutuajakonto loomisel on keskkond ise vastavate andmete töötlemisel vastutavaks töötlejaks. Läbipaistvuse põhimõte eeldab, et isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud. Seetõttu tuleb inimest selgelt, arusaadavalt ja kokkuvõtlikult teavitada isikuandmete töötlemise eesmärkidest, õiguslikust alusest ja seejuures selgitada ka erisusi andmetöötleja rollide osas. Enne kasutajakonto loomist, peab see inimesele olema mõistlikult arusaadav ja selgelt esile toodud. Isikuandmeid võib töödelda nii, nagu inimesed mõistlikult oskavad eeldada ega tohi töödelda selliselt, et sel oleks inimestele (tema õigustele ja vabadustele) õigustamatult kahjulik mõju. AKI soovitab keskkondadel perioodiliselt üle vaadata ja vajadusel täiendada/muuta oma andmekaitsetingimusi, et need vastaksid IKÜM art 12–14 nõuetele. Andmekaitsetingimuste koostamisel ja ajakohastamisel tasub lähtuda mh suunistest määruse 2016/679 kohase läbipaistvuse kohta[9].

Oluline on keskkonnal ka läbi mõelda, et andmeid iseseisva vastutava töötlejana töödeldes on järgitud seaduslikkuse põhimõtet. Seega peab keskkond suutma tagada, et isikuandmete töötlemiseks (nt konto loomisel) on olemas õiguslik alus. Olukorras, kus kliendi perearst on liitunud andmetöötleja keskkonnaga ning klient soovib kasutada platvormi oma perearstiga suhtlemiseks, saab kliendile platvormi kasutamise võimaldamisel isikuandmete töötlemise õiguslikuks aluseks olla lepingu täitmine (IKÜM art 6 lg 1 p b).

Olukorras, kus kliendi perearst ei ole liitunud andmetöötleja keskkonnaga ja inimene soovib ise luua omale platvormile kasutajakonto, saab AKI hinnangul isikuandmete töötlemise õiguslikuks aluseks olla andmesubjekti nõusolek. Nõusolekule (IKÜM art 6 lg 1 p a) tuginemine eeldab, et on täidetud vabatahtlikule nõusolekule tuginemise eeldused, mis on täpsustatud IKÜM art-s 7. IKÜM art 7 lg 1 kohaselt peab vastutaval töötlejal olema võimalik tõendada, et andmesubjekt on nõustunud oma isikuandmete töötlemisega ning lg 3 kohaselt peab olema andmesubjektil õigus oma nõusolek igal ajahetkel tagasi võtta sama lihtsalt, kui toimus selle andmine. Nõusolek peab olema antud selge kinnitusena, millega andmesubjekt annab vabatahtlikult, konkreetselt, teadlikult ja ühemõtteliselt nõusoleku teda puudutavate isikuandmete töötlemiseks konkreetsel eesmärgil (IKÜM pp 32).

Samuti ei tohi inimesele kasutajakonto loomise kohustuse seadmine olla eelduseks või ainsaks võimaluseks, kuidas ta saab välja selgitada, kas perearst on samuti platvormiga liitunud või mitte. Näiteks on võimalik avaldada platvormiga liitunud perearstide nimekiri andmetöötleja kodulehel või luua lahendus, mis võimaldab sisse logida ilma konto loomiseta. Mõistlik on võimaldada inimestel enne konto loomist välja selgitada, kas keskkonna kasutamine on talle vajalik. Seeläbi on platvormil vähem ka nn tühje kontosid ja ka infoturbeoht sellevõrra väiksem.

[8] Euroopa Andmekaitsenõukogu. Suunised 07/2020 vastutava töötleja ja volitatud töötleja mõistete kohta isikuandmete kaitse üldmääruses, ver 2.0. 07.07.2021, p 12, lk 9.
[9] Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse 2016/679 kohase läbipaistvuse kohta, WP 260 rev 01, vastu võetud 29.11.2017, muudetud 11.04.2018.

Andmete muul eesmärgil edasi töötlemine

AKI uuris seires osalejate käest, kas keskkonnad kasutavad andmeid (TTO poolt sisestatud isikuandmeid või TTO-ga suhtlemiseks andmesubjekti poolt sisestatud isikuandmeid) edasi muul eesmärgil iseseisva vastutava töötlejana (nt süsteemi testimiseks, otseturustuseks vm). Kõik seires osalejad vastasid küsimusele eitavalt.

AKI selgitab, et juhul, kui keskkond, kes tegutseb volitatud töötlejana, otsustab hakata andmeid kasutama enda poolt seatud uutel eesmärkidel, tuleb arvestada järgmiste oluliste õiguslike asjaoludega. Kui volitatud töötleja määrab iseseisvalt kindlaks isikuandmete töötlemise eesmärgid ja vahendid, loetakse teda selle töötlemise suhtes vastutavaks töötlejaks. See tähendab, et keskkond võtab endale täieliku vastutuse IKÜM nõuete täitmise eest, sealhulgas kohustuse tagada andmesubjektide õigused ja tõendada töötlemise seaduslikkust.

Kui edasise töötlemise eesmärk (nt testimine, arendus, otseturustus) ei ole identne algse kogumise eesmärgiga ja töötlemine ei põhine andmesubjekti nõusolekul või liidu või liikmesriigi õigusel, siis peab keskkond vastavalt IKÜM art 6 lg-le 4 hindama, kas uus eesmärk on kooskõlas algse eesmärgiga.

Silmas tuleb pidada, et igal töötlemistoimingul peab esinema IKÜM art 6 lg-s 1 toodud õiguslik alus ja eriliiki isikuandmete puhul lisaks ka art-st 9 tulenev erand[10] ning andmesubjekti tuleb teavitada uutest töötlemise eesmärkidest enne edasise töötlemise alustamist[11].

Terviseandmete töötlemine tehisintellekti vahendusel

Kui keskkond pakub või kavatseb pakkuma hakata oma platvormil ka tehisintellekti (AI) funktsionaalsust (nt pöördumise esitamisel täiendavate küsimuste genereerimine inimesele), siis tuleb tähele panna, et ka selliseks töötlemistoiminguks peab esinema õiguslik alus. Terviseandmete puhul on AI funktsionaalsust TTO-de poolt kasutatavas kliendisuhtluskeskkonnas võimalik kasutada nõusoleku alusel. IKÜM kohaselt peab nõusolek olema vabatahtlik, konkreetne, teadlik ja ühemõtteline.[12] Nagu eelnevalt märgitud, siis kehtiva nõusoleku andmise tingimused on toodud IKÜM art-s 7. Nõusolekut võttes ei tohi andmetöötleja sobimatult mõjutada keskkonna kasutaja valikuvabadust. Näiteks võib survestamisena käsitleda pärast keeldumist kohe korduvat nõusoleku küsimist (nt „Kas oled kindel, et ei nõustu?“ vms), kuna see muudab keeldumise protsessi tülikamaks kui nõustumise.

Läbipaistvuse põhimõttest tulenevalt tuleb inimest arusaadaval ja lihtsasti kättesaadaval kujul ning selges ja lihtsas keeles teavitada kõikidest selle töötlemisega seotud asjaoludest, nii et tal on võimalik hõlpsasti kindlaks määrata nõusoleku tagajärjed. Seeläbi on tagatud, et nõusolek antakse kõiki asjaolusid teades. Kui liides on kujundatud nii, et see suunab kasutajat tegema valikut, mida ta tegelikult ei soovi, ei pruugi antud nõusolek olla ühemõtteline tahteavaldus. Ka eksitava disaini kasutamine ei ole lubatud, st kui nõustumise nupp on värvi abil selgelt esile tõstetud ja keeldumise nupp vähem märgatav, võib see olla vastuolus nõudega esitada teave selgelt ja lihtsal viisil. Petliku veebidisaini äratundmise osas soovitab AKI tutvuda juhendmaterjaliga Andmeturbe soovitused e-poodidele, ptk 2.6.

Tehisintellekti funktsionaalsuse kasutamisel või kavandamisel tasub nii TTO-l kui ka keskkonna haldajal veenduda, kas ja millised kohustused võivad tuleneda tehisintellekti käsitlevast määrusest (AIA-määrus)[13].

[10] Isikuandmete töötlemise õiguslikud alused on ammendavalt loetletud IKÜM art-s 6. IKÜM art-s 9 on sätestatud erandid, mis peavad esinema eriliiki isikuandmete puhul lisaks IKÜM art-le 6.
[11] IKÜM art 13 lg 3 ja art 14 lg 4.
[12] IKÜM art 4 p 11.
[13] Euroopa Parlamendi ja Nõukogu määrus (EL) 2024/1689.

Säilitamine ja kustutamine

Igasuguste isikuandmete töötlemisel, sealhulgas nende säilitamisel ja kustutamisel, tuleb järgida isikuandmete kaitse üldpõhimõtteid. Eriliiki isikuandmed (sh terviseandmed) on tugevama kaitse all. Üheks andmekaitse põhimõtteks on säilitamise piirangu põhimõte[14], mis nõuab, et andmeid hoitakse kujul, mis võimaldab andmesubjekti tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse. Seega tuleb tagada, et andmete säilitamise aeg piirduks rangelt minimaalsega. Vastutav töötleja peaks kindlaks määrama tähtajad andmete kustutamiseks või perioodiliseks läbivaatamiseks lähtudes eesmärgi piirangu ja andmete minimaalsuse põhimõtetest. Teatud andmete puhul võib säilitamise tähtaeg tuleneda seadusest (nt tervishoiuteenuse osutamise andmeid säilitamine TTKS § 4^2 lg 4 alusel on 30 aastat).

Kustutamise kohustus tekib, kui andmed ei ole enam eesmärkide täitmiseks vajalikud või kui need on ebaõiged ning sel juhul tuleb andmed ka reaalselt kustutada ja/või anonümiseerida. Kustutamisel on soovituslik kasutada automatiseeritud lahendusi ja kustutamistoimingud peaks logima, et hiljem saaks tegevuse toimimist kontrollida. Manuaalsel kustutamisel peab olema määratud vastutav isik ja samuti tegevus logitud või kustutamisaktiga kinnitatud.

Seirest ilmnes, et andmete säilitamise ja kustutamise põhimõtted on platvormiti erinevad. Oluline on tagada, et vaikimisi määratud aeg ei põhjustaks liigset andmete hoidmist või vastupidiselt ei takistaks eesmärgi täitmist (nt raviloos vajaliku info kadumist). Volitatud töötlejal ehk platvormil tuleb lähtuda tähtaja määramisel ka vastutava töötleja juhistest.

Andmete (nt konto andmed), mille osas keskkond on ise vastutav töötleja, tuleb samuti määrata säilitamistähtajad. AKI on täheldanud, et kui seadus otsest tähtaega ei anna, siis on osa andmetöötlejaid lähtunud tsiviilseadustiku üldosa seadusest ja määranud andmete aegumistähtajaks kolm aastat, tuues põhjenduseks, et ennast kaitstakse võimaliku kohtuvaidluse eest. Seetõttu juhib AKI andmetöötlejate tähelepanu asjaolule, et vastutaval töötlejal ei ole alati õigustatud huvi säilitada isikuandmeid kolm aastat üksnes hüpoteetilise kohtuvaidluse hirmus, kui puuduvad viited reaalsele ohule. Andmete säilitamine peab olema asjakohane, vajalik ja proportsionaalne. Isikuandmeid tohib säilitada vaid seni, kuni see on vajalik eesmärgi täitmiseks, milleks andmeid koguti. Kui algne eesmärk (nt teenuse osutamine) on täidetud, peab edasine säilitamine olema eraldi põhjendatud ja rangelt vajalik. Õigustatud huvi (nt enda kaitsmine kohtuvaidluses) on küll seaduslik alus andmete töötlemiseks, kuid see nõuab huvide kaalumist. Vastutav töötleja peab hindama, kas tema huvi andmeid säilitada kaalub üles andmesubjekti õiguse eraelu puutumatusele ja andmete kustutamisele. Kui andmeid säilitatakse massiliselt ja pikaajaliselt vaid seetõttu, et oht on „hüpoteetiline“, võib see osutuda ebaproportsionaalseks. Kui konkreetset vaidlust ei ole tekkimas, võib kõigi klientide andmete hoidmine maksimaalse aegumistähtaja lõpuni rikkuda andmete minimaalsuse põhimõtet.

Autentimine

Terviseandmed on isikuandmete eriliik, mis väärivad erilist kaitset ning sellest lähtudes peavad terviseandmeid sisaldavasse keskkonda sisselogimisel ja autentimisel (isikusamasuse tuvastamisel) kehtima ranged nõuded turvalisuse ja konfidentsiaalsuse osas.

Kõikidesse seires osalenud keskkondadesse saab siseneda ID-kaarti, Mobiil-ID või Smart-ID abil. Mõnes keskkonnas lubatakse sisselogimist lisaks ka Google’i kontoga, biomeetriaga või erandjuhtudel parooliga.

Terviseandmeid sisaldava keskkonna arendamisel tuleb kasutada autentimisviise, mis tagavad kõrge turvalisuse taseme ja vastavad Euroopa Liidu eIDAS regulatsioonile, kuna sellised lahendused vähendavad identiteedivarguse, andmelekete ja volitamata juurdepääsu riski. Seetõttu

[14] IKÜM artikkel 5 lg 1 p e.

tuleks seires osalenud keskkondade sisselogimiseks pakutavate vahenditena kasutada ainult ID-kaardi, Mobiil-ID ja Smart-ID lahendust, sest need põhinevad tugeval kaheastmelisel autentimisel ning alternatiivsetest sisselogimise viisidest tuleks loobuda.

Ainult parooli või kolmanda osapoole autentimisvahendid üksi ei paku samaväärset kaitset, sest eID kasutamine eeldab alati mitme vahendi (füüsiline ID kaart või mobiiltelefon) kasutamist, mis on samaväärne mitmikautentimise (MFA) põhimõttega. Seejuures, kui on vaja rakendada parooli, peab tõsiselt kaaluma täiendava autentimismehhanismi rakendamist ehk MFA-d.

Kolmanda osapoole sisselogimise võimaldamisega riskivad andmetöötlejad, et nt sotsiaalmeedia või e-maili konto ülevõtmisel saadakse ligi ka teistele platvormidele sh terviseandmetele. Tihti talletavad ka need kolmandad osapooled infot, kus on lubatud Facebook'i või Google kontoga autentimine.

Biomeetriaga sisselogimise viis vähendab oluliselt pettuseriske[15] ning on turvalisem kui parooli või kolmanda osapoole autentimisvahendid. Samas esinevad ka biomeetriaga autentimisvahendil teatud ohud (nt andmete leke, võltsimine), millega andmetöötlejal tuleks arvestada, et riske vähendada. Lisaks tuleb arvestada, et biomeetria näol on tegemist IKÜM mõistes eriliiki isikuandmetega, mille töötlemise aluseks sisselogimisel saab olla ainult andmesubjekti selgesõnaline nõusolek[16]. Kui andmesubjekt biomeetriat kasutada ei soovi, siis peab talle võimaldama ka alternatiivse autentimisvahendi nt eID näol.

Rollid ja õiguste haldus

Üks meetmetest, mis aitab tagada keskkonna vastavust mitmetele andmekaitse üldpõhimõtetele, on rollide ja õiguste haldus. Nimelt peab vastutav töötleja tagama, et andmete töötlemine toimuks viisil, mis tagab isikuandmete asjakohase turvalisuse. Juurdepääsu piiramise võimalus ehk õiguste haldus aitab tagada, et isikuandmetele on ligipääs üksnes õiguspärastel eesmärkidel. See tähendab, et rolli ja õiguste haldus võimaldab määrata, milline töötaja (nt arst/õde/administraator) on „volitatud“ ja milline on tema tööülesannetest tulenev eesmärk. Rolli ja õiguste halduse olemasolu on ka üks tõenditest, mis näitab, et vastutav töötleja on rakendanud asjakohaseid tehnilisi ja korralduslikke meetmeid tagamaks konfidentsiaalsust.

Seire vastustest ilmnes, et mitmes keskkonnas puudub võimalus TTO-l määrata kasutajatele erinevaid rolle ja õigusi. See võib põhjustada volitamata ligipääsu ning vähendada andmete minimaalsuse ja konfidentsiaalsuse põhimõtete järgimist.

Auditid ja turvatestimised

Veebikeskkondades, kus töödeldakse terviseandmeid, on turvaauditite ja -testimiste läbiviimine kriitilise tähtsusega mitmel põhjusel, mis tulenevad nii andmete tundlikkusest kui ka õiguslikest kohustustest tagada andmesubjektide põhiõiguste ja -vabaduste kaitse. Regulaarsete turvatestimiste ja -auditite tegemine aitab tuvastada haavatavusi ja nõrkusi enne, kui need võivad viia volitamata juurdepääsuni, andmete muutmiseni, valede seoste tekkimiseni või muude rikkumisteni. Seeläbi aitab regulaarne testimine keskkondadel vastu pidada mh küberrünnakutele ning minimeerida rünnakutest põhjustatud ohte.

Positiivne on, et kõik seires osalejad viivad läbi sisemisi turvateste. Mõned keskkonnad on kaasanud väliseid partnereid turvaauditite või -testide läbiviimiseks, kuid mitte kõik platvormid ei tee seda regulaarselt, piirdudes vaid sisekontrolliga.

[15] Eesti Infoturbestandard. Riskihaldusjuhend - E-ITS.
[16] IKÜM art 9 lg 2 p a kohaselt on eriliiki isikuandmete (nt biomeetria) töötlemine lubatud, kui andmesubjekt on andnud selgesõnalise nõusoleku nende isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil.

Osa seires osalenud keskkondadest on liitunud „Perearstiabi digiteenindusplatvormid (PADI)“ programmiga ning seetõttu läbinud Tervisekassa tellitud auditi.

Andmesubjekti õigus saada teavet (IKÜM art 15)

IKÜM art-st 15 tuleneb andmesubjektile õigus saada kinnitus, et tema isikuandmeid töödeldakse, tutvuda nende andmetega ja saada teavet andmete töötlemise kohta. Andmesubjekti taotluse lahendamise otsene kohustus lasub vastutaval töötlejal. Kuna volitatud töötleja hoiab sageli andmeid vastutava töötleja nimel, on temal oluline roll tagada, et vastutav töötleja saab täita oma kohustust andmesubjekti ees. Volitatud töötleja poolt vastutava töötleja abistamise kohustus andmesubjekti taotluste lahendamisel on ka üks andmetöötluslepingu kohustuslikest punktidest.[17]

Seire vastustest ilmnes, et keskkondadele tuleb platvormi kasutavate inimeste taotlusi oma isikuandmetega tutvumiseks harva või üldse mitte. Küll aga on keskkonnad enamuses teadvustanud oma rolli abistada vajadusel vastutavat töötlejat (st TTO-d) andmesubjekti taotluste lahendamisel.

Vastuste seas ilmnes ka, et keskkonnad võivad ise inimese andmetega tutvumise taotluse lahendada ja vastata ilma, et protsessi oleks kaasatud TTO kui vastutav töötleja. AKI selgitab, et kui keskkond saab otse andmesubjekti taotluse, olles vastavate andmete töötlemisel ainult volitatud töötleja rollis, siis tegutseb keskkond vastutava töötleja esindajana ning peaks seejuures tegutsema vastutava töötleja juhiste alusel. Järelikult peaks vastutava töötleja ja volitatud töötleja vahelises lepingus olema täpsustatud, kes ja kuidas taotlustele vastamise ülesande tegelikult täidab (st kas volitatud töötleja abistab andmete kogumisel või teeb seda täielikult vastutava töötleja nimel).

Andmesubjekti taotluste lahendamisel tasub silmas pidada, et kui vastus sisaldab eriliiki isikuandmeid (nt terviseandmeid), tuleb vastuse edastamisel rakendada asjakohaseid turvameetmeid, et vältida volitamata juurdepääsu. Praktikas tähendab see enamasti krüpteerimist (nt krüpteeritud e-kiri, turvaline failiedastus või turvaline e-teenuste keskkond).

Andmekaitsespetsialist

IKÜM-st tuleneb teatud organisatsioonidele kohustus määrata andmekaitsespetsialist. Selline kohustus on ka ettevõtetel, mille põhitegevuseks on ulatuslik eriliiki isikuandmete (nt terviseandmete) töötlemine.[18] Andmekaitsespetsialist aitab tagada õiguspärase ja turvalise isikuandmete töötlemise. AKI on oma kodulehel käsitlenud lähemalt, millised on andmekaitsespetsialisti ülesanded ja kompetentsid ja kes saab andmekaitsespetsialisti rolli täita.

Oluline on andmekaitsespetsialisti määramisel silmas pidada, et ettevõtte juhatuse liige ei saa samal ajal täita andmekaitsespetsialisti ülesandeid. Sellisel juhul tekib huvide konflikt ning täielik sõltumatus ei ole tagatud.[19] IKÜM-i pp-s 97 on märgitud, et andmekaitseametnikel peaks olema võimalik täita oma kohustusi ja ülesandeid sõltumatul viisil. Seega kui andmekaitseametnik täidab andmekaitsespetsialisti ülesannetele lisaks ka muid ülesandeid ja kohustusi, tohib ta seda teha tingimusel, et sellised ülesanded ja kohustused ei põhjusta huvide konflikti. Kuna juhatuse liikme puhul on tegemist ettevõtte esindajaga, kes määrab isikuandmete töötlemise eesmärgid ja vahendid, tekitab see huvide konflikti.

Seires osalejate seas on andmekaitsespetsialistina määratud isikute seas ka juhatuse liige, mis ei ole aga IKÜM-ga kooskõlas.

[17] IKÜM art 28 p e.
[18] IKÜM art 37 lg 1 p c.
[19] IKÜM art 38 lg 6.

Kokkuvõte ja soovitused

Eesti perearsti- ja tervishoiuvaldkonna kliendisuhtlusplatvormid on isikuandmete töötlemisel valdavalt volitatud töötleja rollis. Keskkonnad rakendavad ID-kaarti, Mobiil-ID või Smart-ID abil sisenemist mõningate erisustega. Ainult broneerimiseks kasutatavad keskkonnad erinevad kliendisuhtlusplatvormidest riskiprofiili poolest. Samas tuleb arvesse võtta, et broneerimissüsteemi vabad tekstiväljad ja broneeringu metaandmete iseloom viitab selgelt terviseandmete töötlemisele.

Kõik platvormid viivad läbi sisemisi turvakontrolle nõrkuste tuvastamiseks, kuid lisaks ka järjepidev kolmanda osapoole hinnang on soovitatav kõigile keskkondadele, kes ei ole välist auditeerimist veel läbi viinud.

Riskide maandamiseks tuleb selgelt määratleda andmetöötlusrollid, tugevdada tehnilisi ja organisatsioonilisi kontrollmeetmeid ning tagada regulaarne sõltumatu auditeerimine. See aitab hoida andmekaitse ja turvalisuse taset ning vähendada võimalikust rikkumisest tulenevaid riske.

Soovitused:

1. Täpsustada õiguslikud rollid ja tagada IKÜM art 28 nõuetele vastavate andmetöötluslepingute sõlmimine – õiguslik roll peab olema dokumenteeritud ja arusaadav kõigile osapooltele. Silmas tuleb pidada, et volitatud töötleja peab lähtuma vastutava töötleja juhistest. AKI soovitab seetõttu vaadata üle juba sõlmitud andmetöötluslepingud või nende koostamisel tagada, et kokkulepped vastaksid IKÜM art 28 nõuetele ning omavahelised rollid oleksid selgelt piiritletud.

2. Teadvustada, et teatud töötlemistoimingute osas (nt platvormile sisenemine ja kasutuajakonto loomine) on keskkond ise vastutava töötleja rollis ning tagada, et igasuguseks isikuandmete töötlemiseks on olemas õiguslik alus.

3. Regulaarselt hinnata ja vajadusel kaasajastada andmekaitsetingimusi, et need vastaksid IKÜM art 12–14 nõuetele ja tegelikule andmetöötlusele. Inimest tuleb selgelt, arusaadavalt ja kokkuvõtlikult teavitada isikuandmete töötlemise eesmärkidest, õiguslikust alusest ja seejuures selgitada ka erisusi andmetöötleja rollide osas. Andmekaitsetingimuste koostamisel on abiks AKI isikuandmete töötleja üldjuhend ja andmekaitse töörühma suunised määruse 2016/679 kohase läbipaistvuse kohta.

4. Kui keskkond kavatseb TTO poolt või TTO-ga suhtlemiseks andmesubjekti poolt sisestatud isikuandmeid kasutada ise uuel eesmärgil (nt testimine, arendus, otseturustus), peab ta esmalt tuvastama, kas uus eesmärk on algsega kooskõlas ning töötlemiseks on üldse olemas õiguslik alus. Kui töötlemiseks seaduslikku alust ei ole, siis andmeid uuel eesmärgil töödelda ei tohi. Samuti tuleb uuest eesmärgist andmesubjekti teavitada enne töötlemist.

5. Tehisintellekti integreerimise kavandamisel ja kasutamisel tagada, et töötlemiseks oleks olemas sobiv õiguslik alus (terviseandmete puhul üksnes kehtiv ja vabatahtlik nõusolek). Inimest tuleb selgelt ja arusaadavalt teavitada AI-töötluse olemusest ja tagajärgedest ning vältida petlikku või suunavat disaini. Nõusolekut ei või küsida eksitaval või survestaval viisil. Lisaks tuleb hinnata, kas AI-funktsioonist tulenevad lisaks IKÜM-le kohustused ka AIA-määruse alusel.

6. Broneerimiskeskkondadel tuleb teadvustada, et teatud andmete puhul toimub terviseandmete töötlemine. Vajadusel piirata või tehniliselt kontrollida vabasid tekstivälju, et vältida liigsete terviseandmete sisestamist, kui see pole broneeringu tegemiseks ilmtingimata vajalik. Vajadusel lisada selged hoiatused.

7. Tugevdada autentimist - lubada sisselogimist ainult turvaliste mitmeastmeliste autentimisvahenditega (ID-kaart, Smart-ID, Mobiil-ID). Kolmanda osapoole abil sisenemist või parooli kasutamise võimaldamist terviseandmete keskkonda tuleks vältida või rakendada seejuures täiendavaid turvameetmeid (nt kinnitused, limiidid, logimine).

8. Arendada rollihaldust – võimaldada TTO-l määrata kasutajatele erinevate rollide (administraator, arst, õde, registraator jms) ja õiguste andmine, et seeläbi tagada andmete ligipääsude osas vajaduspõhisus ja minimaalsus.

9. Andmete säilitamise ja kustutamise põhimõtete rakendamisel lähtuda vastutava töötleja juhistest ja tähtaegade hindamisel arvestada nii minimaalsuse põhimõttega kui eesmärgipärasusega, et tagada vajaliku info säilimine.

10. Kustutamisel on soovituslik kasutada automatiseeritud lahendusi ja kustutamistoimingud logimist. Manuaalsel kustutamisel määrata vastutav isik ja samuti tegevus logida või kustutamisaktiga kinnitada.

11. Korraldada regulaarseid sõltumatuid auditeid või turvakontrolle, et tuvastada ja lahendada võimalikke turvanõrkuseid. Pakkuda nii andmekaitse kui ka infoturbe teadlikkuse tõstmist nii oma töötajatele kui ka lepingupartneritele.

12. Andmetöötluslepingus leppida kokku, kuidas toimub andmesubjekti taotluse (nt andmetega tutvumiseks) lahendamine ja abistada seejuures vastutavat töötlejat. Andmesubjektile vastuse edastamisel kasutada asjakohaseid turvameetmeid.

13. Tagada, et määratud andmekaitsespetsialisti puhul puudub huvide konflikt ja sõltumatus.

Lugupidamisega

(allkirjastatud digitaalselt)

Kirsika Lääts
jurist
peadirektori volitusel