



Kantavad seadmed ja privaatsus

Juhis organisatsioonidele¹ ja kodukasutajale seaduse² rakendamisel

Juhis kehtestatakse isikuandmete kaitse seaduse § 33 lõige 1 punkt 5 alusel

Kinnitatud 9.11.2015

¹ Avaliku sektori asutused, äriühingud, mittetulundusühingud, sihtasutused, avalik-õiguslik juriidilised isikud.

² [Isikuandmete kaitse seadus](#).

Sisukord

1. Mis on kantavad seadmed?.....	4
1.1. Inimeste füüsilise aktiivsuse ja tervisliku eluviisi edendamine.....	4
1.2. Meelelahutus ja elustiil.....	4
1.3. Tervishoid ja meditsiin.....	5
1.4. Julgeolek.....	5
3. Õiguslik käsitus.....	6
3.1. Isikuandmete kaitse.....	6
3.2. Nõusolek isikuandmete töötlemiseks.....	7
3.3. Delikaatsete isikuandmete registreerimine.....	7
4. Kokkuvõte.....	8

Sissejuhatus

Tänapäeva kiire tehnoloogia areng on digimaailma toonud uut tüüpi personaalsed seadmed ja lahendused. Seniste nutiseadmete (nt telefon, tahvelarvuti) üldlevinud avalik roll on asendumas miniatuursete ja kasutaja persooniga tihedalt suhestunud vahenditega, mille olemasolust võib olla teadlik ainult kasutaja ise. Muu avalikkuse eest võib seadme kasutamine jääda varjatuks. Sellised seadmed on näiteks kasutaja igapäevaelu jäädvustavad elustiili- ja kehalise aktiivsuse vahendid sh nutikellad või kaameraga varustatud nutiprillid.

Ülimalt tundlik valdkond on inimese terviseandmed. Olgu selleks siis meie kaal, pulss või vererõhk. Meditsiinisektor on koostöös tehnoloogiaettevõtetega jõudsalt arendamas mobiilset tervishoidu (m-tervis), kus personaalsetel seadmetel koostoimes nutitelefonide ja -rakendustega on kandev roll. Üks m-tervise eesmärk on parandada tervishoiu kvaliteeti. Tehnoloogia ja tervishoiu lähendamine võimaldab (1) paremat tervishoidu väiksemate kuludega, (2) patsientide õiguste suurendamist (st paremat kontrolli oma tervishoiuteenuse üle) ning (3) lihtsamat ja vahetumat juurdepääsu arstiabile ja teabele võrgus (nt võimaldades arstidel patsientide kaugjälgimist).

Kantavad seadmed koosmõjus *suurandmete*³ ja *asjade internetiga*⁴ on loonud üleilmse teabetaristu, kus üksikisiku põhiõiguste ja vabaduste, eelkõige eraelu puutumatus tagamiseks tuleb väga tähelepanelikult täita isikuandmete kaitse alaseid õigusnorme ning rakendada asjakohaseid infoturbe meetmeid.

Andmekaitse Inspeksioon on koostanud juhise, milles selgitame kantavate seadmete olemust, nende kasutamisel avalduvat mõju inimeste eraelule ja anname soovitusi kasutajate privaatsuse paremaks tagamiseks.

Juhis on selgitava abimaterjalina mõeldud seadmete riist- ja tarkvara arendavatele organisatsioonidele ning seadmete tänastele ja tulevastele kasutajatele.

Juhise valmimisele aitas kaasa Andmekaitse Inspeksiooni [nõukoda](#).

³ Inglise k. *Big Data*. Nii nimetatakse tänapäeval kogutavaid ja töödeldavaid andmemahтусid, mille iseloomustamiseks kasutakse kolme peamist väärtust: maht, andmeformaate paljusus ning andmete tekkimise ja töötamise kiirus.

⁴ Inglise k. *Internet of Things* (IoT). Kasutajate igapäevaste tarbeesemete (näiteks autod, elektroonika jms) seotus teineteisega läbi digitaalsete infokanalite.

1. Mis on kantavad seadmed?

Kantavate seadmete (inglise k. *Wearable Computing*) mõistega kirjeldatakse väikesemõõtmelisi mobiilseid seadmeid. Need on sisuliselt miniatuursed arvutid, mis on varustatud erinevate sensoritega.⁵ Sensorid suudavad reaajas koguda erinevaid kasutaja igapäevategevuste-või keskkonnaga seotud andmeid, mis on abiks näiteks trenni- või dieedipäeviku pidamisel. Kantavad seadmed võivad olla kinnitatud kasutaja kehale või riidele kas nähtavalt või varjatult. Paljudel juhtudel on seadme üheks omaduseks pilti ja videot jäädvustav kaamera. Kuigi ka nutitelefonid paigutuvad kantavate seadmete mõiste alla, on juhise eesmärk selgitada siiski kitsamal eesmärgil loodud vahendite kasutust. Nutitelefoni roll on pigem vahendada ja/või salvestada vahendite kogutud andmeid.

Kantavad seadmed võivad täita erinevaid eesmärke.

1.1. Inimeste füüsilise aktiivsuse ja tervisliku eluviisi edendamine

Sellised seadmed jälgivad näiteks kasutaja liikumisaktiivsust, mõõtes reaalajas läbitud vahemaad, selleks kulunud aega ja kasutaja pulssi. Kogutud andmete põhjal oskab seade välja arvutada kulunud kilokalorite hulga ja anda soovitusi, kas see on näiteks kehakaalu langetamiseks piisav. Tulenevalt treeningu eesmärgist oskavad seadmed soovitada kasutajale sobiliku treeninguplaani.

Levinud seda tüüpi seadmed on näiteks spordikellad, mis aitavad inimese enda sisestatud andmete (vanus, kaal, pikkus, sugu) ja seadme kogutud andmete (nt soorituse aeg, pulss) põhjal anda soovitusi kehalise aktiivsuse korrigeerimiseks. Seadme kogutud andmed on lisaks võimalik edastada vastavatesse programmidesse (rakendused), mis võimaldavad detailsemat andmete analüüsi ja tulemuste graafilist esitamist. Nii mõnigi kantava seadme rakendus võimaldab kogutud andmeid jagada näiteks treeneri, toitumisenõustaja või lähedaste ja sõpradega. Osad seadmed on mõeldud aga näiteks kasutaja unekvaliteedi mõõtmiseks.

Seadmed on võimalik kinnitada kas kasutaja käele, vöole, jalgratta käepidemele või paigutada suisa spordiriie sisemusse. Paljud seadmed võimaldavad kogutud andmed edastada reaalajas nutitelefoni andmesideühenduse abil näiteks seadme (kella) tootja või mõne muu teenusepakkuja serverisse (nn *pilv*). Pilves andmeid analüüsitakse ja antakse kasutajale soovitusi oma elustiili muutmiseks (näiteks rohkem kehalist aktiivsust või pikemat uneaega).

1.2. Meelelahutus ja elustiil

Need seadmed on näiteks kõikvõimalikud kaamerad, mis kinnituvad inimese kehale või riidele. Näiteks rattasõitja, lumelauduri kiivri, üleriie külge või on suisa prillidesse sisse ehitatud. Kasutaja igapäevaste argitegevuste jäädvustamiseks on loodud seadmed (inglise k. *lifeblogging tools*), mis näiteks kaela riputatult või riie nõõpauku peidetult teevad lühikese ajavahemiku tagant (30s) pildi kõigest ümbritsevast. Seade on võimeline pildile lisama asukohaandmed (kus pilt tehti) ning edastama pildid seadmega seotud

⁵ Sensor on tehniline seadis, mis reageerib mingile füüsilisele või keemilisele välistoimele ja muundab selle elektrisignaaliks, mida on hõlbus mõõta ja andmetötluseks rakendada.

rakenduse lehele, kus kogutud andmed muutuvad kättesaadavaks kas ainult kasutajale endale või tema nõusolekul laiemale avalikkusele.

Siia kategooriasse liigituvad ka nn virtuaalreaalsuse seadmed. Näiteks ekraaniga varustatud peakiiivid või prillid, mis pähe panduna kuvavad kasutajale tehisliku keskkonna (virtuaalreaalsus), milles toimuvates tegevustes kasutaja saab osaleda (näiteks sõitmine ameerika mägedel või olla osaline arvutimängus). Seade võib lisaks tehiskeskkonna kuvamisele samal ajal registreerida näiteks kasutaja reaktsioonikiirust või pulssi.

1.3. Tervishoid ja meditsiin

Need seadmed on mõeldud kasutamiseks eelkõige tihedas koostöös tervishoiuteenuse osutajatega⁶ (näiteks perearstid, eriarstid) ja aitavad kaasa telemeditsiini ehk m-tervise arengule. Seadmed on võimelised mõõtma kasutaja terviseandmeid nagu vererõhk või registreerima võimalikke südamerütmi häireid. Allaneelamiseks mõeldud väikesed kapslid suudava maomahla analüüsides kasutajale meelde tuletada, et võtmata on näiteks nõutud ravim. Erinevad tehnoloogiaettevõtted teevad esimesi katsetusi silmaläätsede osas, mis suudavad mõõta kasutaja veresuhkru taset. Kõik selliselt kogutud terviseandmed suudab seade edastada inimese raviarstile, kes saab andmete põhjal teha vajadusel kiireid meditsiinilaseid otsuseid (näiteks sekkuda võimaliku infarktikahtluse korral või avastada varakult arenev suhkruhaigus).

1.4. Eriotstarbelised seadmed

Nende eesmärgiks on toetada näiteks korrakaitse- ja järelevalveasutusi nende tegevuses. Seadmed võivad olla kas miniatuursed kaamerad jälgimistegevuseks või sisaldada teisi eriotstarbelisi sensoreid (näiteks öövaatlusseadmed, soojuskiirgust avastavad seadmed või ümbritseva keskkonnna radioaktiivset- või keemiareostust registreerivad seadmed). Üldjuhul sellised seadmed laiatarbekaubana kättesaadavad ei ole.

2. Kantavate seadmete mõju privaatsusele

Kantavate seadmete ajastu on loonud uue olukorra privaatsüsteemade käsitlemisel. Kasutaja andmete kogumine ja edastamine võib mõningatel juhtudel toimuda märkamatuks, kasutaja teadmata. Reaalajas toimuv andmete salvestamine ja/või edastamine kasutaja nime, soo, vanuse, asukoha, hetkemeeleolu, füüsilise vormi või tervisliku seisundi kohta on seostatav konkreetse kasutajaga. Isegi kui edastatavad andmed on põgusad ja ei võimaldada kasutajat otseselt tuvastada, võib siiski olla võimalik kasutaja hilisem profileerimine.

Harvad pole juhud, kui kasutajal on eelnevalt keeruline tutvuda seadme toote- ja kasutustingimustega, kuna seadmel endal puudub ekraan, kuhu seda infot kuvada. Seadme võrgulehelt ei pruugi see aga olla lihtsasti leitav. Samuti on mõned kasutajad liigagi usinad kohe uut toodet proovima, mispuhul annavad kasutajad kergekäeliselt oma „jah” sõna kõigele, mida võrgulehel isikuandmete või nende töötlemise osas

⁶ Tervishoiuteenuse osutamist reguleerib [tervishoiuteenuste korraldamise seadus \(TKKS\)](#).

teenusepakkuja küsib. Selline kergekäeliselt antud nõusolek võib aga pahatihti tähendada kasutaja eraelulise informatsiooni tingimusteta loovutamist kellelegi kolmandale, kellel on sisuliselt vabad käed teha andmetega mida tahes.

Seadmete väiksus ja võimalus neid kanda varjatult (näiteks riiete all) võib kujutada ohtu ka teistele seadme mõjuvälja jäävatele inimestele. Näiteks miniatuurse kaameraga seade salvestab ja edastabki just teisi samas keskkonnas (avalik või mitteavalik ruum) olevaid inimesi. Kusjuures teadmatusest puudub neil võimalus ka kaamera vaatevälja vältida.

Kui seade töötleb kasutaja terviseandmeid siis on ülimalt oluline töödeldavate andmete kvaliteet ja usaldusvärsus. Kuidas näiteks kindlustada, et erinevad laiatarbe terviseandmeid mõõtvad seadmed tagavad samu parameetreid (näiteks vererõhk) mõõtes usaldusväärsed mõõtetulemused. Sõltub ju tulemusest arsti otsus ravimeetodi või ravimi valiku osas.

Võrku (interneti) ühendatud seadmed ilma nõuetekohase autentimis –ja/või infoturbe lahenduseta on küberrünnete korral kergesti haavatavad. Rünnak meditsiiniseadmetele ei pruugi ohustada mitte ainult kasutaja terviseandmeid, vaid suisa kasutaja tervist. Näiteks küberrünne interneti ühendatud insuliinipumbale, mille käigus manipuleeritakse ravimi doosi, võib patsiendile lõppeda surmavalt.

3. Õiguslik käsitlus

Euroopa Liidu andmekaitsealase regulatsiooni aluseks on [andmekaitse direktiiv](#).⁷ Eestis sätestab direktiivi põhimõtete rakendamist [isikuandmete kaitse seadus](#) (IKS).

3.1. Isikuandmete kaitse

Nagu varasemalt selgitasime, võivad kantavad seadmed koguda ja edastada erinevaid kasutajaga seotud andmeid, näiteks vanus, sugu, kehakaal või terviseandmed. Kõikide nende andmete alusel võib kasutaja olla otseselt või kaudselt tuvastatav. Sellisel juhul on [seaduse](#) kohaselt tegemist [isikuandmetega](#)⁸ ja nendega tehtavad toimingud on [isikuandmete töötlemine](#).⁹

Poolt, kes kasutaja isikuandmeid töötleb, nimetab seadus [isikuandmete töötlejaks](#). Selleks võib olla füüsiline või juriidiline isik, välismaa äriühingu filiaal või riigi- või kohaliku omavalitsuse asutus, kes töötleb või kelle ülesandel töödeldakse isikuandmeid (IKS § 7 lõige 1).

Isikuandmete töötleja peab enne andmetöötlust kindlaks määrama (1) isikuandmete töötlemise eesmärgid, (2) töödeldavate isikuandmete koosseisu, (3) isikuandmete töötlemise korra ja viisi ning (4) isikuandmete kolmandatele isikutele edastamise lubamise (IKS § 7 lõige 2).

Isikuandmete kaitseks on isikuandmete töötleja kohustatud täitma isikuandmete

⁷ [Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta](#).

⁸ Isikuandmete kaitse seadus (IKS) § 4. Andmed terviseseisundi kohta on delikaatsed isikuandmed (IKS §4 lõige 2).

⁹ IKS § 5.

töötlemise nõudeid sh rakendama organisatsioonilisi, füüsilisi ja infotehnilisi turvameetmeid. Tagatud peab olema andmete terviklus¹⁰, käideldavus¹¹ ning konfidentsiaalsus¹² (IKS § 24,25).

Pane tähele:

Juhul kui isikuandmeid ei salvestu ainult seadmesse, vaid neid saab edastada kas reaalajas või hiljem kasutaja soovil mõnele teenusepakkujale (näiteks andmete analüüsi teenus) peab teenusepakkuja enne andmetöötluse algust võimaldama kasutajal tutvuda teenuse kasutustingimuste ja selle osaks oleva isikuandmete töötlemise põhimõtetega.¹³ Kasutajalt tuleb enne andmetöötluse algust küsida tema nõusolek.

3.2. Nõusolek isikuandmete töötlemiseks

Isikuandmete töötlemise aluseks saab olla kas:

- 1) seadus;
- 2) kasutaja nõusolek või;
- 3) kasutajaga sõlmitud leping.

Üldjuhul toimub kantavates seadmete ja nendega seotud teenustes isikuandmete töötlemine kasutaja nõusolekul.

Nõusolek kui ühepoolne tahteavaldus peab rajanema kasutaja vabal tahtel, selles peavad olema selgelt määratletud andmed, mille töötlemiseks luba antakse, andmete töötlemise eesmärk ning isikud, kellele andmete edastamine on lubatud, samuti andmete kolmandatele isikutele edastamise tingimused ning kasutaja õigused tema isikuandmete edasise töötlemise osas. Vaikimist või tegevusetust nõusolekuks ei loeta.

Nõusolek peab olema kirjalikku taasesitamist võimaldavas vormis. Kui nõusolek antakse koos teise tahteavaldusega, peab isiku nõusolek olema selgelt eristatav. Nõusolekule kehtivad tingimused on sätestatud IKS §-s 12.

Pane tähele:

Kasutajal peab nõusoleku andmise ajal olema selge, kellele ja milleks ta nõusoleku annab. Kantavate seadmete tootja-või andmete analüüsi võrgulehel täidab seda nõuet näiteks võimalus märkida „linnukesega“ vastav lahter. Või mõni muu infotehniline lahendus, mis võimaldab kasutajal selgelt ja üheselt aru saada nõusoleku andmisest ning mida on võimalik teenusepakkujal hiljem tõendada.

Kui kantava seadme puhul on tegemist tervishoiuteenuse osutamise käigus kasutatava meditsiiniseadmega siis kasutaja eraldi nõusolekut isikuandmete töötlemiseks ei ole vaja.

¹⁰ Andmete põhinemine algallikal ning veendumus, et need pole hiljem muutunud või neid pole volitusteta muudetud.

¹¹ Andmete õigeaegne ja hõlbus kättesaadavus selleks volitatud isikutele.

¹² Andmete kättesaadavus ainult selleks volitatud isikutele.

¹³ IKS § 6.

Sellisel juhul toimub isikuandmete, sh delikaatsete isikuandmete (andmed tervises seisundi kohta, IKS § 4 lõige 21 punkt 3) töötlemine tervishoiuteenuse osutamise lepingu täitmiseks (võlaõigusseaduse 41. peatükk).

3.3. Delikaatsete isikuandmete registreerimine

Kantavate seadmete registreeritavate või mõõdetavate andmete hulgas võivad olla ka kasutaja tervislikku seisundit kirjeldavad andmed ehk delikaatsed isikuandmed. Juhul kui need andmed ei salvestu ainult seadmesse, vaid edastatakse ka teenust osutavale või andmetöötlusega tegelevale organisatsioonile (isikuandmete töötleja), on viimane kohustatud registreerima delikaatsete isikuandmete töötlemise Andmekaitse Inspektsioonis (IKS §27).

Pane tähele:

Registreerimiskohustus laieneb kõigile delikaatsete isikuandmete töötlejatele, sõltumata sellest kas tegemist on raviasutuse, tootearendus- või tarkvaraettevõttega.

Isikuandmete töötleja ei ole kohustatud registreerima delikaatsete isikuandmete töötlemist, kui ta on määranud isikuandmete kaitse eest vastutava isiku. Isikuandmete kaitse eest vastutava isiku määramisest ja tema volituste lõppemisest tuleb viivitamata teavitada Andmekaitse Inspektsiooni. Isikuandmete kaitse eest vastutava isiku määramisel tuleb inspektsioonile teatada tema nimi ja kontaktandmed (IKS § 30 lõige 1). Isikuandmete kaitse eest vastutava isiku rolli kirjeldab IKS § 30 lõige 2-5.

Pane tähele:

Kui kantav seade kvalifitseerub [seaduse](#) kohaselt meditsiiniseadmeks¹⁴, tuleb seadme turule laskmisest või kasutuselevõttust teavitada Terviseametit.¹⁵

4. Kokkuvõte

Tänapäeval koguvad ja töötlevad kantavad seadmed väga erinevaid kasutaja eraelulisi andmeid. Seadme kasutuselevõtul tekkiv põnevus ja hasart võib aga uinutada tähelepanu selles osas, mis puudutab kogutavate andmete koosseisu ja võimalikku edastamist kolmandatele isikutele. Kasutajal võib kaduda kontroll oma andmete üle. Ta ei pruugi teada, kes ja mida tema andmetega teeb.

Kuigi isikuandmete töötlemise õigusraamistik sätestab väga selgelt nõuded isikuandmete töötlejale, on kasutaja tihtilugu siin nõrgemas positsioonis, kuna andmetöötlusprotsessi läbipaistmatuse tõttu ei ole võimalik nõuete täitmises veenduda.

¹⁴ Meditsiiniseadme seadus (MSS) § 3

¹⁵ MSS § 26.

Soovitused:

- isikuandmete töötlemine kantavates seadmetes peab olema nii seadme kasutajale kui ka teistele, kelle andmeid töödeldakse masimaalselt läbipaistev;
- seadme kasutamisega seotud isikuandmete kogumine, edastamine ja avalikustamine peab olema seadme kasutajale arusaadavalt esitatud ning peab toimuma kasutaja selgesõnalise nõusoleku alusel; nõusolek peab olema võimalik iga ajal tagasi võtta;
- kasutajal peab olema võimalik soovi korral peatada seadmes isikuandmete kogumine;
- seadmel ei tohiks olla kohustuslikku vaikeseadet automaatseks ühendumiseks ja andmete edastamiseks seadme tootja või teiste teenusepakkujate andmetöötlusplatvormidesse sh [pilveteenused](#); kasutaja peab saama muuta seadme seadeid enda tugevama privaatsuse tagamiseks;
- austada tuleb seadme kasutaja õigust saada juurdepääs tema kohta kogutud isikuandmetele, andmeid muuta/parandada või kustutada. Kasutajat tuleb informeerida, kui kaua tema andmeid säilitatakse.
- kasutajal peab olema võimalus ise määrata töödeldavate andmete detailsus; nn dünaamilised seaded peavad andma kasutajale valiku, milliste tegevuste korral mis täpsusega isikuandmete kogumist lubada;
- soovi korral peaks kasutajal olema võimalus kogutud andmed salvestada endale sobivasse salvestusvahendisse (nutitelefon, mälupulk, mälukaart);
- seadme kasutamisega peaks olema tagatud andmete teisaldatavus (inglise k. *portability*) st kasutaja võimalus andmeid ühest teenusest teise mugavalt üle kanda (kopeerida).