TARTU ÜLIKOOL

ÕIGUSTEADUSKOND TALLINNAS

Eraõiguse osakond

Katri Remmelgas

TERVISEANDMETE EDASTAMINE NÕUSOLEKUTEENUSE KAUDU KOLMANDATELE ISIKUTELE JA SELLEGA KAASUVAD ANDMEKAITSEÕIGUSLIKUD KÜSIMUSED

Magistritöö

Juhendaja: *dr iur* Karin Sein

Tallinn 2021

SISUKORD

SISSEJUHATUS....4
1. TERVISEANDMED KUI ERILIIGILISED ANDMED JA NENDE TÖÖTLEMISE ÕIGUSLIKUD ALUSED....10
1.1. Terviseandmete mõiste....10
1.2. Terviseandmetega seotud innovatsioon ning õigusloome areng....12
1.3. Terviseandmete töötlemise õiguslik alus....14
2. RISKID SEOSES TERVISEANDMETE EDASTAMISEGA KOLMANDATELE OSAPOOLTELE....20
2.1. Terviseandmete edastamisega kaasnevad üldised riskid....20
2.2. Terviseandmete edastamine kolmandatele osapooltele majandushuvi eesmärgil…22
2.3. Terviseandmete töötlemine kolmanda osapoole poolt algsest erineval eesmärgil…26
2.4. Kolmandate osapoolte poolt terviseandmete anonüümimistehnika kasutamine.....32
2.5. Lapse terviseandmete töötlemine õigusliku aluseta....36
2.6. Andmetöötluse läbipaistmatus....36
2.7. Terviseandmete töötlemine õigusliku aluse ära langemisel....39
2.8. Terviseandmete edastamine madalama andmekaitse tasemega riiki....40
2.9. Terviseandmete edastamise ja sellele järgneva töötlemise kontekstis andmete usaldusväärsuse ja konfidentsiaalsuse tagamine....42
3. KEHTIVAD TERVISEANDMETE EDASTAMISEGA SEOTUD PIIRANGUD JA VÕIMALIKUD TÄIENDAVAD PIIRANGUD MAANDAMAKS 2. PEATÜKIS KÄSITLETUD NÕUSOLEKUTEENUSEGA KAASUVAID ANDMEKAITSEÕIGUSLIKKE RISKE....48
3.1. Andmekaitse üldmäärusest tulenevad piirangud....48
3.2. Olemasolevate piirangute piisavus terviseandmete edastamise ja edasise töötlemise kontekstis....51
3.3. Andmekaitse üldmääruse artikkel 9 (4) kohased täiendavad piirangud erasektorile EL liikmesriikide näitel....64
3.4. Võimalikud täiendavad tingimused ja/ või piirangud terviseandmete töötlemiseks Eestis andmekaitse üldmääruse artikli 9 (4) alusel....69
KOKKUVÕTE....75
SUMMARY....83
LÜHENDID....91

KASUTATUD ALLIKAD....92
Kasutatud kirjandus ja seaduseelnõud....92
Kasutatud normatiivaktid....96
Kasutatud kohtulahendid....98
Järelevalve otsused....98
Kasutatud muu materjal....99
Litsents....106

SISSEJUHATUS

Seoses tehnoloogia arenguga kasvab andmete, sh isikuandmete töötlemise maht iga aastaga. Eesti infoühiskonna arengukava 2020 kohaselt on plaan luua nii tehnoloogilised kui ka organisatoorsed ja õiguslikud tingimused selleks, et inimestel oleks suurem kontroll oma isikuandmete üle. St, et inimesed saaksid vabamalt otsustada millal ja kellega enda kohta käivad andmeid jagada.[1] Samas tuleb arvestada, pidevalt suurenevate andmemahtude ja nende ristkasutuse tõttu võib olla vajadus inimest oma informatsioonilise enesemääramisõiguse realiseerimisel piirata ja seda tehnoloogiliste arendustega kaasnevate isikuandmete töötlemisega seotud ohtude tõttu.[2]

Käesolev töö keskendub nõusolekuteenusega kaasnevate andmetöötlusriskide kaardistamisel ning analüüsimisel erasektori äriühingutele, kellel puudub seadusest tulenev alus pääseda ligi tervise infosüsteemis olevatele andmete ning kes pakuvad või soovivad pakkuda füüsilistele isikutele nende terviseandmetel põhinevaid teenuseid. Seejuures aga ei kvalifitseeruks nimetatud teenused tervishoiuteenuste korraldamise seaduse[3] (edaspidi TTKS) § 2 mõttes tervishoiuteenusteks.

Töö on aktuaalne, kuna käesoleval hetkel on Riigi Infosüsteemi Ameti (edaspidi RIA), Sotsiaalministeeriumi ning teiste koostööpartnerite poolt arendusjärgus nõusolekuteenus.[4] Selle kaudu saavad eraõiguslikud juriidilised isikud võimaluse liidestuda infosüsteemi andmevahetuskihi (edaspidi X-tee) kaudu erinevate riiklike andmebaasidega ning andmesubjektid saavad anda nõusoleku enda terviseandmete edastamiseks konkreetsetele kolmandatele osapooltele.[5] Tervise infosüsteemiga (edaspidi TIS) liitumisest on olnud huvitatud mitmed erinevad osapooled: nii kindlustusandjad kui ka muud lisaväärtusteenuseid

1 Eesti infoühiskonna arengukava 2020. Vabariigi Valitsus, uuendatud 2018, lk 2. Kättesaadav: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2020.pdf (28.04.2021).
2 Alexy, R. Põhiõigused Eesti põhiseaduses. - Juridica 2001, eriväljaanne, lk 5-96.
3 Tervishoiuteenuste korraldamise seadus. - RT I 2001, 50, 284...RT I, 17.05.2020, 13.
4 Riigi Infosüsteemi Ameti aastaraamat 2020, lk 26. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_48lk_est_veeb.pdf (28.04.2021).
5 vt täiendavalt Riigi Infosüsteemi Ameti aastaraamat 2020, lk 27 ja Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 22.

pakkuvad ettevõtjad.[6] Nõusolekuteenuse pilootprojektiga on plaanis pakkuda tervisega seotud andmetele ligipääsu just nendele ettevõtetele, kellel selleks muu seadusest tulenev alus puudub. Hetkel on nõusolekuteenuse pilootprojektis osalemas sellised ettevõtted nagu Dermtest, Cognuse, MediKeep, MinuDoc ja TempID, kes soovivad teenuste arendamisel kasutada terviseandmeid.[7] Autorile teadaolevalt täpselt sellist lahendust nagu nõusolekuteenus maailmas ei eksisteeri, küll aga on nõusolekuteenusele ja sellega seotud edaspidisele andmetöötlusele kasutatud sarnast lahendust USA-s.[8] Peamine erinevus seisneb selles, et Eesti lahenduse raames annab andmesubjekt kaks eraldiseisvat nõusolekut: üks nõusolekuteenuse raames andmete edastajale ehk riikliku andmekogu vastutavale töötlejale ja teine andmete edasiseks töötlemiseks otse kolmandale osapoolele.[9] USA-s annab aga andmesubjekt oma nõusoleku andmete küsimiseks ja edasiseks kasutamiseks otse mobiilirakendust arendavale eraõiguslikule kolmandale osapoolele.[10] Käesolevas töös on arvestatud ka USA lahendusega seotud probleeme, kuid arvestatud, et need ei ole üks-ühele võrreldavad. Esiteks seetõttu, et Eestis on terviseandmed kesksetes riiklikes registrites, kuid USA-s puudub samaväärne keskne andmebaas ning terviseandmed on suuresti fragmenteerunud erinevate tervisehoiuteenuse pakkujate juures.[11,12]

Teine põhjus on seotud sellega, et Euroopa Liidus on olemas otsekohalduv andmekaitse üldmäärus, mis kohaldub nii riiklikku tervishoiuteenust pakkuvatele vastutavatele töötlejatele kui ka kõigile eraõiguslikele isikutele, kes töötlevad isikuandmeid, sh terviseandmeid. USA-s kohaldub tervishoiuteenust osutatavatele töötlejatele andmete edastamise korral *Health Insurance Portability and Accountability Act* (edaspidi HIPAA),[13] kuid eraõiguslikele

6 Pärgmäe, R. jt. Õiguse ja eetika vaade Vabariigi valitsuse e-tervise strateegias aastani 2020. Õiguse ja eetika töörühma raport 2015, lk 24. Kättesaadav: https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Eesti_e_tervise_strateegia/oiguse_ja_eetika_tooruhma_raport.docx (28.04.2021).

7 Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 53.

8 Yednak, C. Providers and payers still grapple with privacy concerns under final interoperability rules. Price Waterhouse Coopers. 13.03.2020. Kättesaadav: https://www.pwc.com/us/en/industries/health-industries/library/privacy-concerns-interoperability-rules-3-13-20.html (28.04.2021).

9 Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 43.

10 Yednak, C. Providers and payers still grapple with privacy concerns under final interoperability rules. PWC.

11 Gliklich RE, Leavy MB, Dreyer NA, (eds). Tools and Technologies for Registry Interoperability, Registries for Evaluating Patient Outcomes: A User's Guide, 3rd Edition, Addendum 2. (Prepared by L&M Policy Research, LLC under Contract No. 290-2014-00004-C.) AHRQ Publication No. 19(20)-EHC017-EF. Rockville, MD: Agency for Healthcare Research and Quality. October 2019. Kättesaadav: https://www.ncbi.nlm.nih.gov/books/NBK551879/pdf/Bookshelf_NBK551879.pdf (28.04.2021).

12 Dash, S., Shakyawar, S.K., Sharma, M. et al. Big data in healthcare: management, analysis and future prospects. J Big Data 6, 54 (2019). Kättesaadav: https://doi.org/10.1186/s40537-019-0217-0 (28.04.2021).

13 Health Insurance Portability and Accountability Act of 1996. Public Law 104-191, 104th Congress.

kolmandatele osapooltele see üldjuhul ei kohaldu ning seetõttu kasutatakse riskide maandamiseks peamiselt teavitustööd.[14] Andmesubjektidel palutakse enne andmete edastamiseks nõusoleku andmist tutvuda kolmanda osapoole töötlemistingimuste ja eesmärkidega ning samuti infoga andmete edastamise kohta.

Varasemalt on seda teemat puudutatud Eesti e-tervise strateegias 2020[15] ning e-tervise strateegia 2020 kohta koostatud õiguse ja eetika töörühma raportis.[16] Neist esimeses on pakutud välja andmete avatud platvorm, mille kaudu on andmesubjektil võimalik oma andmeid jagada ka kommertsteenuse pakkujatega.[17] Õiguse ja eetika töörühma raportis leiti, et kommertsteenused, mis ei ole tervishoiuteenused võivad pakkuda inimestele olulist lisandväärtust (nt vaktsineerimiskalender või kaalu- ja toitumisharjumuste mobiilirakendus), aga terviseandmete edastamine TIS-ist saab selle tarbeks toimuda üksnes andmesubjekti nõusolekul. Nõusolekuteenuse tehnilist ülesehitust, andmekogudega seotud õiguslikke probleeme ning nõusolekuteenuse protsessiga seotud riske (nt väljastatavate andmekomplektide loomime ning vajaduse hindamine lähtuvalt kolmanda osapoole teenuse kirjeldusele, andmesubjekti poolt teadliku nõusoleku andmine andmete edastamisele, andmevahetuse turvalisus riigi ja erasektori vahel) on käsitletud nõusolekuteenuse analüüsi aruandes.[18]

Käesoleval tööl on kaks peamist uurimisküsimust: kas nõusolekuteenuse kaudu terviseandmete edastamisel riiklikest andmebaasidest kolmandatele osapooltele, on andmekaitse üldmääruses toodud kaitsemeetmed piisavad, et maandada kolmandate osapoolte poolt edasise andmetöötlusega kaasnevaid riske? Kas ja milliseid täiendavaid tingimusi oleks Eestil vajalik andmekaitse üldmääruse artikli 9 (4) alusel kolmandate osapoolte poolt terviseandmete töötlemiseks kehtestada?

Kättesaadav: https://www.congress.gov/bill/104th-congress/house-bill/3103/text (28.04.2021).

14 N. Hamm, New Federal Patient Health Data Sharing Rules: The Tradeoffs Between Access and Privacy Protections. Bipartisan Policy Center. 30.03.2020. Kättesaadav: https://bipartisanpolicy.org/blog/new-federal-patient-health-data-sharing-rules-the-tradeoffs-between-access-and-privacy-protections/ (28.04.2021).

15 E-tervise visioon 2025. E-tervise strateegiline arenguplaan 2020. Riigikantselei 2015, lk 22. Kättesaadav: https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Eesti_e_tervise_strateegia/e-tervise_strateegia_2020.pdf (28.04.2021).

16 Pärgmäe, R. jt. Õiguse ja eetika töörühma raport 2015, lk 24.

17 E-tervise visioon 2025, lk 22.

18 Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021.

Töö on jaotatud kolme peatükki, millest esimene osa käsitleb terviseandmete kui eriliigiliste isikuandmete mõistet. Samuti on käsitletud terviseandmete väärtuslikkust seoses uute innovaatiliste lahendustega. Kuna käesoleva töö raames on oluline just andmesubjekti nõusolek andmete edastamiseks ning edaspidiseks töötlemiseks, siis on õigusliku alusena käsitletud lähemalt nõusolekut (andmekaitse üldmääruse artikkel 9 (2) a)).

Töö teine osa käsitleb potentsiaalseid andmekaitseõiguslikke riske, mis kaasnevad nõusolekuteenuse kaudu terviseandmete edastamisega kolmandatele osapooltele, kuna tegemist saaks olema olulise innovatsiooniga terviseandmete teisesel kasutamisel ning autori hinnangul ei ole hetkel kõiki selle kasutuselevõtuga seotud andmekaitseõiguslikke asjaolusid kas üldse mitte arvestatud või piisavalt hinnatud. Arvestades, et nõusolekuteenus võib potentsiaalselt mõjutada kõiki üle 18. aastaseid Eesti elanikke ning ebapiisavate kaitsemeetmete rakendamisel tuua neil ka kahju, siis vajab antud temaatika eraldiseisvat õiguslikku analüüsi, sh peamiselt kolmandate poolt tekkivate andmekaitseõiguslike riskide osas. Ehkki teoreetilisi riske võib esineda rohkem, siis autor on pidanud kõige olulisemaks hinnata järgmisi käesolevas töös on kajastatud riske: terviseandmete töötlemine algsest erineval eesmärgil, lapse terviseandmete töötlemine, kolmandate osapoolte poolt läbipaistvuse põhimõtte täitmine ja andmete edastamine madalama andmekaitse tasemega riiki. Samuti andmete anonüümimise ja müügiga seotud problemaatikat, krediidiandjate ja kindlustusandjate võimalikku huvi terviseandmete järele ning terviseandmete usaldusväärsuse ja konfidentsiaalsuse tagamisega seotud andmekaitseõiguslikke riske. Käesolevas töös ei ole käsitletud nõusolekuteenuse kaudu väljastatavate andmete ulatuse kindlaksmääramisega seotud problemaatikat, kuna kolmandatele osapooltele ei võimaldata X-tee andmevahetusteenuse raames piiramatut ligipääsu riiklikkesse andmekogudesse, vaid väljastavate andmete hulk ning nende loogilist seost kolmanda osapoole poolt pakutava teenusega analüüsitakse vastava andmekogu vastutava töötleja poolt lähtuvalt minimaalsusprintsiibist enne konkreetsele ettevõttele X-tee andmevahetusteenuse võimaldamist.[19] Seetõttu on autori hinnangul andmete ulatusega seotud andmekaitseõiguslik risk piisavalt maandatud. Ehkki kolmas osapool võib esitada taotluse nö igaks juhuks ka teenuse(te) kohta, mida tegelikkuses ei suuda ega plaani pakkuda, siis käesoleva töö autori hinnangul on sellisel juhul tegemist nö jääkriskiga, mille täielik ennetamine on kas väga raske või võimatu. Seda põhjusel, et andmeteenusega liitumise taotlus on paratamatult seotud

19 Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 26, 58, 61.

taotleja usaldusväärsuse tunnetamisega. Seetõttu leiab autor, et käesolev töö ei pakuks edastatavate andmekomplektide kindlaksmääramise problemaatika analüüsi osas täiendavat väärtust. Samuti ei ole käesolevas töös käsitletud tööandja poolt terviseandmetele ligipääsu saamist, kuna nõusolekuteenus ei puuduta andmetöötlust olukordades, kus isikuandmete töötlemiseks, sh terviseandmete töötlemiseks on olemas mõni muu õiguslik alus. Töölepingulises suhtes on terviseandmete töötlemine lubatud andmekaitse üldmääruse artikli 9 (2) punkti b) alusel ning üldjuhul ei saa rääkida nõusolekust kui kehtivast õiguslikust alusest isikuandmete töötlemiseks. Kehtivast nõusolekust töösuhetes saaks rääkida üksnes olukorras, kus töötajal on reaalne võimalus valida kas nõusolek anda või mitte. Selliseks olukordadeks võib olla Andmekaitse Inspektsiooni (edaspidi AKI) hinnangul näiteks organiseeritud sotsiaalsed tegevused.[20]

Töö kolmas osa käsitleb olemasolevaid andmekaitse üldmäärusest tulenevaid piiranguid, nende vajadust ning samuti hinnangut nende piisavuse kohta. Piisavuse hindamiseks on lähtutud muuhulgas teises peatükis toodud andmekaitseõiguslikest riskidest. Viimaseks toob autor välja võimalikud terviseandmete töötlemisega seotud piirangud, mille rakendamine maandaks autori hinnangul terviseandmete edastamise järgselt terviseandmete töötlemisega seotud riske. Selleks on võrreldud Läti, Rootsi, Soome ja Ühendkuningriigi isikuandmete töötlemisega seotud õigusakte ning võimalikke terviseandmete töötlemisega seotud täiendavaid siseriiklikke piiranguid, mis kohalduksid väljaspool tervishoiuteenuse osutamist.

Töö peamisteks meetoditeks on õigusdogmaatiline analüüs ja võrdlev meetod. Õigusdogmaatiline meetod võimaldab teha kindlaks asjakohased õigusaktid ning nende tõlgendamise analüüsides selleks erinevaid kirjalikke materjale. Võrdlev meetod võimaldab tuvastada sarnasusi Eesti ja teiste EL liikmesriikide (Läti, Rootsi, Soome ja Ühendkuningriigid) vahel seoses terviseandmete töötlemisele esitatavatele nõuetele erasektori poolt ning kasutada seda teadmist võimalike siseriiklike piirangute ettepanekute tegemisele Eesti kontekstis. Nimetatud meetodite kasutamine võimaldab analüüsida ja leida vastused töös püstitatud uurimisküsimustele.

20 Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhetes. Abistav juhendmaterjal. Tallinn 26.05.2014, lk 43. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf (28.04.2021).

Uurimisküsimustele vastuse leidmiseks on töös olulisemate allikatena kasutatud isikuandmete kaitse üldmäärust (edaspidi andmekaitse üldmäärus),[21] teiste Euroopa Liidu liikmesriikide andmekaitsealaseid õigusakte, kohtulahendeid ning järelevalve asutuste ettekirjutisi. Lisaks eelnimetatule on töös kasutatud allikatena isikuandmete kaitse seaduse eelnõu seletuskirja, artikli 26 alusel asutatud andmekaitse töörühma juhendmaterjale, Euroopa Andmekaitsenõukogu (edaspidi EDPB) ning Euroopa Andmekaitseinspektori (edaspidi EDPS) juhendeid ning arvamusi, samuti Andmekaitse Inspektsiooni (edaspidi AKI) juhendmaterjale ning muud eesti- ja võõrkeelset õiguskirjandust, sh on analüüsitud varasemaid magistritöid.

Enne andmekaitse üldmääruse jõustumist on analüüsitud näiteks tarbija nõusoleku kehtivust tüüptingimuste ja tarbija võimalust oma õigusi kohtulikult kaitsta[22] Nimetatud töös käsitletakse ka mobiilirakenduse poolt andmesubjektilt kogutud terviseandmete töötlemisega seotud õiguslikku problemaatikat. Kuuskmaa, L.M. kirjutas 2020. aastal oma magistritöös terviseandmete töötlemisesest personaalmeditsiini teenuste arendamiseks,[23] mille puhul toimub terviseandmete töötlemine tervishoiuteenuse raames. Käesoleva töö eesmärgiks ei ole analüüsida üksnes andmesubjektilt kogutavate terviseandmete töötlemist, vaid peamiselt riiklikes andmekogudes olevate terviseandmete kasutamist väljaspool tervishoiuteenuse pakkumist. Sellega kaasneda võivad andmekaitseõiguslikke riske ning õiguslikku hinnangut võimalike täiendavate preventatiivsete õiguslike meetmete järele, mida eelnimetatud magistritööde raames ei ole käsitletud.

Magistritööd iseloomustavad järgmised märksõnad: andmekaitse, terviseandmed, andmeedastus, andmetöötlusriskid.

21 Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, lk 1-88.

22 Nisu, N. Eesti tarbija kui andmesubjekti õiguste kaitse mobiilirakenduse poolt isikuandmete kasutamisel – Endomondo näitel. Magistritöö. Tartu Ülikool. Õigusteaduskond. Tallinn 2017. Kättesaadav: http://hdl.handle.net/10062/56497 (28.04.2021).

23 Kuuskmaa, L. M. Isikuandmete töötlemise õiguslik alus ning andmesubjekti õiguste kaitse tervise infosüsteemi kogutud terviseandmete kasutamisel kliiniliste otsuste tugisüsteemide arendamiseks ja rakendamiseks. Magistritöö. Tartu Ülikool. Õigusteaduskond. Tartu 2020. Kättesaadav: http://hdl.handle.net/10062/68545 (28.04.2021).

1. TERVISEANDMED KUI ERILIIGILISED ANDMED JA NENDE TÖÖTLEMISE ÕIGUSLIKUD ALUSED

1.1. Terviseandmete mõiste

Tervisega seotud isikuandmed on sellist liiki isikuandmed, mis annavad infot andmesubjekti endise, praeguse või tulevase füüsilise või vaimse tervise kohta.[24] Sellisteks andmeteks on näiteks number või tähis, mis on füüsilisele isikule määratud, et isik kordumatult tuvastada tervishoiuga seotud eesmärkidel: enamus Euroopa Liidu riikides isikukood või näiteks spetsiaalne tervishoiu number Portugalis[25] või Hispaanias;[26] teave kehaosa või kehast pärineva aine kohta, andmed haigusloo; kliinilise ravi või andmed andmesubjekti füsioloogilise ja biomeditsiinilise olukorra kohta. Samuti info haigestumisohu kohta: nt info füüsilise isiku kohta, et ta on Covid-19 kontaktne. Andmekaitse üldmääruse artikli 4 punkti 15 kohaselt loetakse terviseandmete alla ka andmesubjektile tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet andmesubjekti tervisliku seisundi kohta. Euroopa Kohtu praktika kohaselt tuleb tervislikku seisundit käsitlevaid andmeid tõlgendada laialt, mis võimaldaks hõlmata isiku tervist puudutava teabe kõiki aspekte.[27] Tervisealasteks isikuandmeteks tuleks lugeda seega kõiki neid andmeid, mille kaudu on võimalik saada midagi teada andmesubjekti tervisest sõltumata andmete allikast. Andmed võivad pärineda arstilt või mõnelt muult tervishoiutöötajalt, aga tänapäevases digitaliseeruvas maailmas koguvad ja analüüsivad meie andmeid ka üsna mitmed nutiseadmed, mis on meditsiiniseadmeks tunnistatud[28] või mida saab ühendada meditsiiniseadmete või anduritega. Samuti võivad mõned andmed muutuda terviseandmeteks olenevalt kontekstist ja koosmõjus teiste andmetega avalduvad konkreetse isiku terviseriskid.[29] Näiteks mobiilrakenduse poolt kogutud andmeid, mille põhjal

24 Andmekaitse üldmääruse selgituspunkt 35.

25 *Portaria n.º 981/95* (Portugali tervishoiu ministri määrus number 981/95). 01.08.1995. Kättesaadav: https://dre.pt/web/guest/pesquisa/-/search/477871/details/normal?q=N%C3%BAmero+de+utente+da+Sa%C3%BAde (28.04.2021).

26 *De cohesión y calidad del Sistema Nacional de Salud* (Hispaania seadus nr 16/2003 riikliku tervishoiusüsteemi ühtekuuluvuse ja kvaliteedi kohta), artikkel 57. Kättesaadav: https://www.boe.es/eli/es/l/2003/05/28/16/con (28.04.2021).

27 EKo C-101/01, *Bodil Lindqvist* v *Åklagarkammaren i Jönköping*, punkt 50.

28 Nt termomeetrid, nutikaalud või ka nutikell ScanWatch. Kättesaadav: https://support.withings.com/hc/en-us/articles/360015551577-ScanWatch-Regulatory-statement (28.04.2021).

29 Euroopa Andmekaitsenõukogu. Suunised 3/2020 terviseandmete töötlemise kohta teadusuuringute eesmärgil seoses COVID-19 puhanguga. 21.04.2020, lk 5. Kättesaadav:

teenusepakkuja saab viidata teatud terviseriskile: teatava ajavahemiku jooksul mõõdetud kõrge vererõhk, viidates suuremale südameinfarkti riskile[30] või Fitbit nutikellale sisseehitatud pulssoksümeeter, mis mõõdab magades vere hapnikusisaldust. Silmnähtavalt suurte variatsioonide korral selgitatakse kasutajale, et see võib vihjata uneajal esinevatele hingamishäiretele ning soovitatakse pöörduda arsti poole.[31]

Terviseandmeid ei ole peetud aga alati tundlikuks isikuandmete kategooriaks. Euroopaüleselt kodifitseeriti automatiseeritud isikuandmete töötlemise õigused ja põhimõtted esmakordselt 1981, mil Euroopa Nõukogu võttis vastu isikuandmete automaatsel töötlemisel isikute kaitse konventsiooni (edaspidi andmekaitse konventsioon).[32] Nimetatud konventsiooni artiklis 6 toodi terviseandmed esimest korda välja, kui täiendavat kaitset vajavad eriliigilised isikuandmed ning nimetatud sätte kohaselt ei võinud tervisliku seisundi kohta käivaid andmeid üldjuhul automatiseeritult töödelda. Erandina oli see lubatud, kui siseriikliku õigusega oli tagatud asjakohane kaitse.

Kui andmekaitse konventsioon ja selle alusel antud Euroopa Nõukogu Ministrite Komitee soovitused reguleerivad üldiselt[33] üksnes isikuandmete automatiseeritud töötlemist, siis isikuandmete töötlemist käsitleva direktiiviga 95/46 EÜ (edaspidi andmekaitse direktiiv)[34] sai hõlmatud igasugune isikuandmete töötlemine. Andmekaitse direktiiviga lisandus Euroopa üleselt ka nõusolek üheks õiguslikuks aluseks terviseandmete töötlemisel. Eestis kuni 14.01.2019 kehtinud isikuandmete kaitse seaduse[35] § 4 (2) punkti 3 kohaselt nimetati andmeid terviseisundi kohta delikaatseteks isikuandmeteks ning sama seaduse § 12 lõike 4 kohaselt võis delikaatseid isikuandmeid andmesubjekti nõusoleku alusel töödelda, kuid selleks tuli andmesubjektile selgitada, et tegemist on delikaatsete isikuandmetega ning nõusolek tuli võtta kirjalikku taasesitamist võimaldavas vormis. Andmekaitse direktiivis sätestatud põhimõte eriliigiliste andmete töötlemise kohta kanti suuresti üle ka andmekaitse üldmäärusse.

https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised (28.04.2021).

30 Euroopa Andmekaitsenõukogu. Suunised 3/2020 terviseandmete töötlemise kohta teadusuuringute eesmärgil seoses COVID-19 puhanguga, lk 5.

31 Fitbit help manuals. Kättesaadav: https://bit.ly/39JNIXn (28.04.2021).

32 Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. - RT II 2001, 1, 3.

33 ENMK toob välja, et soovituses nr R (97) 5 toodud põhimõtteid võib liikmesriik rakendada ka sellistele toob terviseandmetele, mis ei ole automaatselt töödeldavad, vt täpsemalt: Council of Europe Committee of Ministers. On the protection of Medical Data, Recommendation R (97) 5, 13.02.1997, lk 27. Kättesaadav: https://rm.coe.int/16804f0ed0 (28.04.2021).

34 Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281/31, 23.11.1995.

35 Isikuandmete kaitse seadus. - RT I 2007, 24, 127…RT I, 06.01.2016, 1.

1.2. Terviseandmetega seotud innovatsioon ning õigusloome areng

Terviseandmetega seotud innovatsiooni üheks aluseks on kvaliteetsete andmete olemasolu ning võimalus neid taaskasutada jagades andmeid riigi ja ettevõtjate vahel või ettevõtjatel omavahel. 25.11.2020 esitas Euroopa Komisjon ettepaneku koos seletuskirjaga üleeuroopalise andmehalduse määruse (edaspidi andmehalduse määruse ettepanek) väljatöötamiseks.[36] Nimetatud määruse eesmärk on parendada andmete kättesaadavust, suurendada usaldust andmevahendajate vastu ning muuhulgas võimaldada isikuandmete kasutamist nn isikuandmete jagamise vahendaja abil, kelle eesmärk on aidata üksikisikutel kasutada oma andmekaitse üldmäärusest tulenevaid õigusi.[37] Seoses tehnoloogia ja personaalmeditsiini arenguga on võetud kasutusele termin mobiilne tervishoid (*mHealth*).[38] Lisaks ravi- ja tervishoiuga seotud tegevusele on mobiilse tervishoiu all peetud silmas ka eluviisi ja heaolu puudutavaid mobiilirakendusi, mis annavad nõu vormis püsimise ja toiduvaliku kohta, edendavad terviseteadlikku käitumist parendades inimese tervist ja üleüldist elukvaliteeti. Samuti kuuluvad siia alla individuaalset nõustamist pakkuvad süsteemid, telemeditsiini teenuse pakkumine või lihtne ravimite meeldetuletuse edastamine mõne elektroonilise sidevahendi kaudu.[39] Globaalses digitaalse tervise 2020-2025 strateegias kasutab Maailma Tervishoiuorganisatsioon (edaspidi WHO) aga laiendatud mõistet - digitaalne tervis, mis tähendab digitaalse tehnoloogia arendamist ja kasutamist tervise parendamiseks.[40]

Eesti riik on aastaid kogunud füüsiliste isikute terviseandmeid, kuid seni ei ole neid erasektorile nõusolekuteenusega planeeritud viisil ja mahus jagatud. Eesti e-tervise visiooni 2025 kohaselt on riigil plaan luua andmete avatud platvorm, mis võimaldab inimestel oma terviseandmete kasutamist väljaspool nende tekkimise kohta, sh kolmandate osapoolte juures,

36 Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus Euroopa andmehalduse kohta (andmehaldust käsitlev õigusakt), 25.11.2020, seletuskirja punkt 1. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52020PC0767 (28.04.2021).

37 Samas, seletuskirja punkt 1.

38 WHO Global Observatory for eHealth. (2011). mHealth: new horizons for health through mobile technologies: second global survey on eHealth. World Health Organization, lk 6. Kättesaadav: https://apps.who.int/iris/bitstream/handle/10665/44607/9789241564250_eng.pdf?sequence=1&isAllowed=y (28.04.2021).

39 Euroopa Komisjon. Roheline Raamat mobiilse tervishoiu ehk m-tervise kohta. Eestikeelne väljaanne. Brüssel, 10.04.2014, lk 3. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52014DC0219 (28.04.2021).

40 Global strategy on digital health 2020-2025. World Health Organization, lk 5. Kättesaadav: https://cdn.who.int/media/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d_02adc66d-800b-4eb5-82d4-f0bc778a5a2c.pdf?sfvrsn=f112ede5_68 (28.04.2021).

kommertsteenuseks, piiriüleste teenuste pakkumiseks või muudel eesmärkidel.[41] Vastavalt andmekaitse üldmääruse artiklile 20 (3) ei kohaldata riiklikesse andmebaasidesse kogutud andmete töötlemise suhtes, mis on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks artiklis 20 sätestatud andmete ülekandmise põhimõtet (*data portability*). Sellest tulenevalt ei ole planeeritav andmete avatud platvorm midagi, mida riik on kohustatud arendama, vaid pigem riigi poolt pakutav nö mugavusteenus. Andmekaitsereformi üks eesmärke andmekaitse üldmääruse kehtestamisega oli suurendada füüsilise isiku kontrolli oma andmete üle ning võimalust digitaalset keskkonda rohkem usaldada.[42] Seda eesmärki aitab täita näiteks õigus tutvuda oma andmetega, paluda nende väljastamist ning samuti õigus andmete ülekandmisele ühelt vastutavalt töötlejalt, näiteks teenuseosutajalt, teisele. Kuigi riigi andmebaaside vastutavatele töötlejatele avalikes huvides oleva ülesande täitmiseks või avaliku võimu teostamisele see kohustus ei laiene, siis Eesti e-tervise strateegias kirjeldatud andmete avatud platvormi loomisega saavutatakse e-tervise teenuste osas kui mitte samaväärne, siis sisuliselt andmete ülekandmise õigusega võrreldav tulemus. Planeeritud platvorm järgib põhimõtet, et andmesubjekti terviseandmeid peab olema võimalik tema teadlikul nõusolekul tehniliselt kasutada kõikjal väljaspool nende tekkimise kohta ning inimesel on õigus jagada enda kohta käivaid andmeid igalt teenuseosutajalt[43] masinloetaval kujul.[44] Võrdluseks, andmete ülekantavuse põhimõtte kohta sätestab andmekaitse üldmääruse artikkel 20, et vastutav töötleja edastab isikuandmed otse teisele vastutavale töötlejale struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul, kui see on tehniliselt teostatav.

RIA poolt arendatav nõusolekuteenuse arendus nö riigipoolne mugavusteenus võimaldab füüsilistel isikutel hakata jagama nõusoleku alusel enda riiklikesse andmebaasidesse kogutud terviseandmeid erasektoriga ning ühtlasi järgib e-tervise strateegias toodud põhimõtet. Andmesubjekt saab hakata kasutama oma terviseandmeid ka väljaspool andmete tekkimise kohta ning jagatavaid andmeid edastatakse masinloetaval kujul. Praktilise poole pealt tähendab see, et erasektor pakub mobiilirakenduse või veebilehe kaudu füüsilisele isikule

41 E-tervise visioon 2025, lk 22.

42 Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu Määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus). Brüssel: 2012, lk 99. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52012PC0011&from=ET (28.04.2021).

43 Avatud andmete platvormi kaudu saab andmesubjektil olema võimalus jagada ka enda poolt kommertsteenuste kaudu kogutud terviseandmeid sekundaarseks kasutamiseks tervishoius. vt täpsemalt: E-tervise visioon 2025, lk 24.

44 E-tervise visioon 2025, lk 22.

mõnda teenust, mis vajab selleks konkreetse füüsilise isiku terviseandmeid ning andmesubjekt annab konkreetsele riigi andmekogu vastutavale töötlejale nõusoleku oma andmete edastamiseks kolmandale osapoolele. Autorile teadaolevalt ei ole sarnast võimalust Euroopas arendatud. Küll aga on olemas USA-s olemuselt sarnane lahendus, kus rakendusliidese ehk API (*application programming interface*) kaudu on eraõiguslikul kolmandal osapoolel võimalus patsiendi nõusolekul saada ligipääs terviseandmetele.[45] Patsient saab seejärel hallata endaga seotud terviseandmeid kolmanda osapoole poolt arendatud mobiilirakenduses.[46] Erinevus RIA poolt arendatava teenusega seisneb selles, et USA-s annab andmesubjekt oma nõusoleku mobiilirakenduse loojale mitte andmekogu vastutavale töötlejale nagu Eestis on plaanis.

1.3. Terviseandmete töötlemise õiguslik alus

Terviseandmete delikaatsusest tulenevalt näeb andmekaitse üldmäärus ette, et üldjuhul on eriliigiliste andmete, sealhulgas terviseandmete töötlemine keelatud. Töötlemine on lubatud ainult sellistel õiguslikel alustel, mis on andmekaitse üldmääruse artiklis 9 (2) loetletud: andmesubjekti nõusolek (v.a kui liidu või liikmesriigi õigusega on pole see lubatud),[47] töötlemine on vajalik tööõigusest ning sotsiaalkindlustuse ja sotsiaalkaitse valdkonna õigusest tulenevate kohustuste ja eriõigustega seotult, töötlemine on vajalik andmesubjekti või teise füüsilise isiku eluliste huvide kaitseks ning andmesubjekt ise on samal ajal füüsiliselt või õiguslikult võimetu nõusolekut andma, töötlemine on vajalik õigusnõude koostamiseks, töötlemine on vajalik rahvatervise valdkonna avalikes huvides või näiteks ka statistilisel eesmärgil jne. Samuti on üldmääruse kohaselt lubatud töödelda selliseid terviseandmeid, mille andmesubjekt on ilmselgelt avalikustanud. Terviseandmete töötlemisel on oluline märkida, et andmekaitse üldmääruse artiklis 6 (1) b) toodud õigus töödelda andmeid andmesubjekti osalusel sõlmitud lepingu täitmiseks ei kehti õigusliku alusena terviseandmete töötlemisel. Samuti ei võimalda andmekaitse üldmäärus artikli 9 kohaselt kasutada õigustatud huvi terviseandmete töötlemise õiguslikuks aluseks. See tähendab, et eraõiguslikul juriidilisel

45 Yednak, C. Providers and payers still grapple with privacy concerns under final interoperability rules. PWC.

46 N. Hamm, New Federal Patient Health Data Sharing Rules: The Tradeoffs Between Access and Privacy Protections.

47 Näiteks Austria sotsiaalkindlustuse numbrit võib kasutada üksnes sotsiaalkindlustuse eesmärkidel ning selle numbri kasutamine muudel eesmärkidel vajab täiendavad seaduslikku alust. Vt täiendavalt Feiler, L., Forgó, N., Weigl, M. The EU General Data Protection Regulation (GDPR): A Commentary. German Law Publishers 2018, kommentaar artiklile 9.

isikul, kes soovib füüsilisele isikule pakkuda teenust, mis vajab terviseandmeid, aga ei kvalifitseeru tervishoiuteenuseks on üldjuhul ainuke sobilik õiguslik alus andmesubjekti nõusolek. Seetõttu on käesoleva töö raames terviseandmete töötlemise õigusliku alusena käsitletud lähemalt üksnes nõusolekut.

Kolmanda osapoole poolt terviseandmete kasutamise juures tuleb selgelt eristada kahte eraldiseisvat õigussuhet, millest üks esineb andmesubjekti ja riikliku andmekogu vastutava töötleja vahel ning teine kolmanda osapoole ning andmesubjekti vahel. Esimese raames annab andmesubjekt nõusoleku riikliku andmekogu vastutavale töötlejale eesmärgiga edastada terviseandmed kolmandale osapoolele. Teise õigussuhte raames annab andmesubjekt oma nõusoleku kolmandale osapoolele, kes töötleb neid andmeid eesmärgiga pakkuda andmesubjektile terviseandmetel põhinevat personaliseeritud teenust. Kuna terviseandmete töötlemisel pole võimalik kasutada õigusliku alusena andmekaitse üldmääruse artiklit 6 (1) b, siis kuidas saab pakkuda terviseandmetel põhinevat teenust nõusoleku alusel, mis mitte üksnes ei vaja lepingu täitmiseks või sõlmimiseks isikuandmeid, vaid mille kogu olemuslik sisu on ainult terviseandmete töötlemine. Viimase puhul muutuks leping ilma terviseandmeteta mõtetuks.[48] Kui aga nõusolek on osa lepingulisest kohustusest, siis see indikeerib, et tegemist ei ole vabatahtlikult antud nõusolekuga.[49] K. Pormeister toob välja, et alternatiivselt võiks käsitleda nõusolekut ka eraldiseisvana ehk paralleelselt lepinguga.[50] Sellisel juhul muutuks nõusolek lepingu sõlmimise eeltingimuseks. Andmekaitse üldmääruse artikli 7 (4) kohaselt ei saa lugeda nõusolekut vabatahtlikuks, kui nõusoleku terviseandmed ei ole vajalikud lepingu täitmiseks. Seega ei ole nõusolek oma olemuselt välistatud olemaks lepingu eeltingimus, kuid ainult juhul kui konkreetsed terviseandmed on tingimata vajalikud. Käesoleva töö autori hinnangul võiks läheneda kolmanda osapoole poolt terviseandmete töötlemisel, nõusoleku vajalikkuse ja seega ka kehtivuse hindamisel veel kahest aspektist. Esiteks teenused, mille põhiteenuseks on terviseandmete analüüs ehk ilma terviseandmete töötlemiseta ei eksisteeriks põhiteenust ja seega on nende töötlemine tingimata vajalik. Teiseks teenused, mille põhiteenus on midagi muud, kuid terviseandmete töötlemine abistab põhiteenuse täitmist. Samas aga ei muuda selle osutamist tingimata võimatuks. Nõusoleku teenuse raames võiks esimese alternatiivi näiteks tuua teenuse, mille põhiteenus on

48 Pormeister, K. Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of "23andMe". Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht, 6 (1), 17−23. 2017, lk 19.
49 Samas, lk 19.
50 Samas, lk 19.

fundamentaalselt konkreetse andmesubjekti terviseandmete analüüsil põhinev teenus. Teenuseks, mille puhul terviseandmed on pigem abistavad, aga ei muuda põhiteenuse osutamist võimatuks võiks autori hinnangul käsitleda näiteks vabatahtlikku hambaravi kindlustuslepingut. Kindlustusriski määramisel on kindlasti abiks kui teada konkreetse patsiendi haiguslugu, kuid see ei ole kuigi praktiline, sest hüvitatavad summad võrreldes näiteks eluaseme kindlustusega on kordades väiksemad ja autorile teadaolevalt ei ole see ka turupraktika.

Täiendavalt tekib küsimus, kas andmesubjekt saab anda nõusolekut riigile kuivõrd riik on avalik sektor ning üldjuhul ei ole saa lugeda nõusolekut kehtivaks olukorras, kus on selgelt ebavõrdne olukord. Andmekaitse üldmääruses on rõhutatud, et seda eriti juhul kui vastutav töötleja on avaliku sektori asutus, ning seega on ebatõenäoline, et nõusolek anti selle konkreetse olukorra kõigi asjaolude puhul vabatahtlikult.[51] AKI-i on samuti selgitanud, et avaliku võimu teostamise või avaliku ülesande täitmise käigus ei ole õigust küsida isikult lisaks ka nõusolekut, kuna see eksitab ning jätab mulje et andmesubjektil on vaba valik, kuigi tegelikkuses ei ole.[52] Küll aga ei tähenda see, et avaliku sektori jaoks on nõusolek õigusliku alusena täielikult välistatud, sest näiteks mugavusteenuste pakkumisel võiks nõusolek olla kohane õiguslik alus.[53] Andmesubjektil on ka praegu õigus paluda andmete väljastamist teistele isikutele. TTKS § 59^3 lg 7 täpsustatud, et lisaks muudele TTKS-s sätestatud isikutele väljastatakse isikuandmeid üksnes andmesubjekti enda nõusolekul. Nõusolekuteenusega tekiks andmesubjektile juurde veel üks võimalik andmete edastusviis.

Avalikus sektori võib vabatahtliku nõusolekuga olla tegu näiteks olukorras, kus vallavalitsus pakub välja võimaluse liituda isikutel meililistiga, et saada teavitusi mõne konkreetse projekti edenemise kohta. Sama info on esitatud ka omavalitsuse võrgulehel, aga konkreetselt selline meililisti kaudu saadav kirjavahetus saaks toimuda üksnes nõusoleku alusel ning isikul on igal ajal võimalus kirjade saamisest loobuda. Lisaks ei jää isik infost ilma, sest võib seda igal ajal võrgulehelt vaadata.[54] Sellisel juhul on andmesubjektil reaalne vaba valik, kas nõusolek anda või mitte. Osapoolte ebavõrdsuse tasakaalustamiseks peab olema võimalik näidata, et teenuse

51 Andmekaitse üldmääruse selgituspunkt 43.
52 Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend. 19.03.2019, lk 39. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (28.04.2021)
53 Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend, lk 39.
54 Näide pärineb: Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend, lk 39

kasutamine ei ole kohustuslik.[55] Samas, kui andmesubjektile ei järgne teenuse mittekasutamise tõttu otseseid kahjulikke õiguslikke tagajärgi, ei tähenda see automaatselt andmekaitse üldmääruse artikli 7 (4) mõttes vabatahtlikkuse nõude täitmist.[56] Näiteks koroonaga seotud mobiilirakenduste kasutamist on seostatud otseselt põhiõiguste piiramisega, kuna koroona mobiilirakenduse mittekasutamise tõttu võib olla vajadus pikendada sotsiaalelu ja vaba liikumise piiranguid.[57] Antud juhul on leitud, et kahjuliku tagajärjena tuleks antud juhul lugeda sotsiaalset survet, mis kehtestatakse avaliku sektori poolt tervele ühiskonnale, kuna sisuliselt on tegemist avaliku sektori meetmega pandeemia kontrolliks.[58] Lisaks, koroona mobiilirakenduse puhul puudub realistlik alternatiiv.[59] Nõusolekuteenuse näol pakub riik sisuliselt võimalust edastada andmeid nõusoleku teenuse kaudu kolmandatele isikutele, kuid riigil ei ole otsest kohustust andmesubjektidele sellist teenust pakkuda. Nõusolekuteenuse raames antava nõusoleku suhtes puudub andmesubjekti ja riikliku andmekogu vastutava töötleja vahel sundus, samuti ei plaani avalik sektor otseselt ega kaudselt nõusolekuteenuse mittekasutamise tõttu piirata inimeste põhiõiguseid ning kui andmesubjektile jääb ka alternatiiv oma terviseandmeid nt kindlustusandjale muul viisil edastada, siis on autori hinnangul vabatahtlikkuse nõue täidetud ning nõusolek nõusolekuteenuse raames lubatav õiguslik alus. Siinjuures ei tohiks autori hinnangul ajada segi võimalikku riski, et kolmas osapool võib seada nõusoleku andmise sisuliselt lepingu eeltingimuseks, mistõttu tekib küsimus nõusoleku vabatahtlikkuses kolmanda osapoole ja andmesubjekti vahel. Kuna tegemist on kahe eraldiseisva õigussuhtega ning see, et andmesubjekt võib tulevikus edastada andmed nõusolekuteenuse kaudu, selle asemel et küsida terviseinfot arstilt ning edastada dokumendid meili teel kindlustusandjale, ei muuda töö autori hinnangul nõusolekut konkreetsete andmete edastamisviisi suhtes kehtetuks või mittelubatavaks.

Nõusolek on oma olemuselt otsene tahteavaldus TsÜS mõttes (avalduse vormis või selgelt nõusolekut väljendava tegevuse vormis). Andmekaitse üldmääruse artikli 4 punkti 11 kohaselt peab kehtiv nõusolek olema vabatahtlik, konkreetne, teadlik ja ühemõtteline, mille kohaselt andmesubjekt nõustub enda kohta käivate isikuandmete töötlemisega. See tähendab, et andmesubjekti nõusolekus kolmandale osapoolele peab sisalduma sõnaselgelt tahe tuua kaasa

55 Bock, K., Kühne, C.R. jt, Data Protection Impact Assessment for the Corona App. 29.04.2020, lk 51. Kättesaadav: https://ssrn.com/abstract=3588172 (28.04.2021).
56 Samas, lk 51.
57 Samas, lk 52.
58 Samas, lk 52.
59 Samas, lk 52.

õiguslik tagajärg. Lisaks peab nõusolek selle kehtimiseks olema antud teovõimelise isiku poolt, st vähemalt 18 aastase poolt või alaealise ja piiratud teovõimega isiku puhul seadusliku esindaja poolt. Tuleb märkida, et vähemalt 16-aastane laps võib andmekaitse üldmääruse artikli 8 (1) kohaselt anda küll nõusoleku oma isikuandmete töötlemiseks, aga seda juhul kui tegemist on infoühiskonna teenuse pakkumisega otse lapsele ning nõusolek on antud artikli 6 (1) a) alusel. Viimati nimetatud artikkel aga ei hõlma eriliigilisi isikuandmeid, sh terviseandmeid, mistõttu alaealistel ei ole iseseisvalt võimalik anda kehtivat nõusolekut oma terviseandmete töötlemiseks.

Nõusoleku vabatahtlikkus tähendab, et andmesubjekt peab nõusoleku andmisel omama reaalset valikuvabadust ning puudub võimalus pettuseks, ähvarduseks ja sunniks. Samuti ei tohi nõusoleku küsimisega tekitada inimeses kartust, et kui ta võtab nõusoleku tagasi või keeldub nõusolekut andmast, siis kaasnevad talle sellega olulised negatiivsed tagajärjed.[60] Selgelt kahjulikuks tagajärjeks loetakse näiteks seda, kui nõusoleku tagasivõtmine toob andmesubjektile kaasa täiendavad kulud või osutatava teenuse piiramise, kui teenust saab ka ilma nõusolekuta pakkuda.[61] Nagu juba eelnevalt mainitud, siis nõusoleku vabatahtlikkuse hindamisel tuleb võtta arvesse ka konkreetse kolmanda osapoole poolt pakutava teenuse osutamise tingimusi ning hinnata nõusoleku vajalikkust sõlmitava lepingu täitmiseks (andmekaitse üldmääruse artikkel 7 (4)). Samuti ei peeta nõusolekut vabatahtlikult antuks, kui see on osa mitteläbiräägitavatest tingimustest[62] ja hõlmab lisaks muid eesmärke ning mille osas andmesubjekt ei saa valida mille kohta konkreetselt nõusolekut anda ja mille kohta mitte. Näiteks kui fotode töötlemist võimaldav mobiilirakendus sunnib teenuse kasutamiseks aktiveerima GPS-funktsiooni ning võtab täiendavalt nõusoleku käitumispõhise reklaami edastamiseks, siis kumbki neist ei ole vajalik fototöötlusteenuse osutamiseks ning sellisel juhul ei saa sellistel eesmärkidel antud nõusolekut lugeda vabatahtlikuks.[63] Andmesubjektil peab olema õigus otsustada nõusoleku andmist iga eesmärgi suhtes eraldi.[64] Seega teenusepakkuja poolt küsitavad nn kobarnõusolekud ei vasta andmekaitse üldmääruses toodud

60 European Union Agency for fundamental rights and Council of Europe. Handbook on European Data Protection Law, 2018 edition. Luxembourg: Publications Office of the European Union, 2018, lk 143. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (28.04.2021).

61 Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohase nõusoleku kohta. Vastu võetud 28.11.2017. Viimati muudetud ja muudatused vastu võetud 10. aprillil 2018, lk 11. Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_nousoleku_kohta_wp259_rev_0.1_et.pdf (28.04.2021).

62 Artikli 29 alusel asutatud andmekaitse töörühma suunised kohase nõusoleku kohta, lk 5.

63 Näide pärineb: Artikli 29 alusel asutatud andmekaitse töörühma suunised kohase nõusoleku kohta, lk 6.

64 Andmekaitse üldmääruse selgituspunkt 32.

nõuetele ja kolmas osapool vastutava töötlejana ei tohiks küsida andmeid nö igaks juhuks, vaid peab lähtuma minimaalsuse printsiibist – andmeid töödeldakse üksnes nii palju kui see on teenuse jaoks vältimatult vajalik.

Nõusolek peab olema konkreetne ning võimaldama andmesubjektil mõista selgelt tema terviseandmete kasutamise eesmärki. Selleks ei ole vaja tuua välja konkreetset kasutusjuhtumit, vaid piisab täpsest eesmärgi kirjeldamisest, mis kehtib ühe või mitme kasutusjuhtumi puhul.[65] Liigüldsõnaliseks eesmärgiks peetakse näiteks „kasutajakogemuse parendamist" või „turundust".[66] Selleks, et nõusolek oleks teadlik on vaja andmesubjektil teada enne nõusoleku andmist vähemalt seda milliseid terviseandmeid ja mis ulatuses väljastatakse, millisest andmebaasist väljastatakse. St, kes on vastutav töötleja, millisele juriidilisele isikule väljastatakse. Samuti on teadliku nõusoleku juures oluline, et andmesubjekt teab edasist töötlemise eesmärki ehk kuidas plaanitakse tema isikuandmeid kasutada.[67] Nõusolekuteenuse kontekstis on andmekogu vastutava töötleja poolt töötlemise eesmärgiks andmete edastamine, kuid selle ja kolmanda osapoole poolt pakutava teenuse puhul on tegemist omavahel seotud teenustega. Seega on oluline anda andmesubjektile võimalikult täielik informatsioon, et ta saaks teha informeeritud otsuse.

Tsiviilseadustiku üldosa seaduse (edaspidi TsÜS)[68] § 68 lõige 4 sätestab, et vaikimist või tegevusetust loetakse tahteavalduseks, kui see tuleneb seadusest, isikute kokkuleppest või nendevahelisest praktikast. Nõusolek on küll TsÜS mõttes tahteavaldus, kuid andmekaitse üldmääruse mõttes peab nõusolek olema lisaks ühemõtteline. Ühemõttelisuse tagamiseks peab nõusolek peab olema aktiivne tahteavaldus[69] ning erinevalt TsÜS § 68 (4) toodud võimalust lugeda vaikimist või tegevusetust teatud tingimustel tahteavalduseks, ei tohiks vaikimist, eeltäidetud lahtreid ega tegevusetust lugeda andmekaitse üldmääruse mõttes kehtivaks nõusolekuks.[70]

65 Feiler, L., Forgó, N., Weigl, M. The EU General Data Protection Regulation (GDPR): A Commentary. German Law Publishers 2018, kommentaar artiklile 4.
66 Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013, lk 52. Kättesaadav: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (28.04.2021).
67 Andmekaitse üldmääruse selgituspunkt 42.
68 Tsiviilseadustiku üldosa seadus. - RT I 2002, 35, 216...RT I, 23.05.2020, 2.
69 Artikli 29 alusel asutatud andmekaitse töörühma suunised kohase nõusoleku kohta, lk 16.
70 Andmekaitse üldmääruse selgituspunkt 32.

2. RISKID SEOSES TERVISEANDMETE EDASTAMISEGA KOLMANDATELE OSAPOOLTELE

2.1. Terviseandmete edastamisega kaasnevad üldised riskid

Nõusolekuteenuse turule toomine suurendab paratamatult terviseandmete töötlemise mahtu ning uute lisanduvate teenuste mõjul suureneb nõudlus terviseandmete järele. Seega võivad ka andmetöötlusega seotud rikkumised kasvada. Seda eelkõige kui olemasolevad preventatiivsed meetmed regulatiivsel tasandil ei ole piisavad, et riske maandada.

Kui seni said tervise- ja heaoluteenuseid pakkuvad mobiilirakendused tervisega seotud isikuandmeid (nt pulss, füüsiline aktiivsus, sammud, kehakaal, vere hapniku sisaldus) andmesubjektidelt endalt, siis nõusolekuteenuse kasutusele võtmisel võib kolmas osapool saada andmeid ka riiklikust andmekogust. Andmesubjekt annab riikliku andmekogu vastutavale töötlejale nõusoleku oma terviseandmete edastamiseks konkreetsele juriidilisele isikule ning andmekogu vastutav töötleja edastab andmed otse kolmandale osapoolele. Arvestades terviseandmete tundlikkust on vajalik analüüsida kas andmekaitse üldmääruses toodud sätted on piisavad või oleks vaja rakendada täiendavaid siseriiklikke preventatiivseid meetodeid. Igasugune andmete töötlemine, sh isikustatud andmete töötlemine hõlmab endas riske, kuid piisavate maandamismeetmete olemasolul ei pruugi need realiseeruda.

Järgnevates alapeatükkides on toodud välja autori hinnangul suuremad andmekaitsealased riskid, mis terviseandmete kolmandatele osapooltele edastamisega kaasnevad. Käsitletud riskid ei ole uued ega kitsalt ainult Eesti riigi poolt arendatava nõusolekuteenuse ja selle pakkumisega seotud. Nagu eelnevalt viidatud, on USA-s kasutusel nõusolekuteenusega olemuselt sarnane lahendus. Seal nähakse peamiste probleemidena, et kolmandad osapooled võivad isikute terviseandmeid väärkasutada või ei rakenda andmete säilitamisele piisavaid meetmeid või müüakse andmesubjekti andmeid ilma nende nõusolekuta.[71] Kolmandatele osapooltele andmete edastamisel on USA-s suureks riskiks ka ühtse patsiendi identifikaatori

71 Yednak, C. Providers and payers still grapple with privacy concerns under final interoperability rules. PWC.

puudumine, mistõttu on erinevate tervishoiuasutuste vahel patsiendi info vahetamisel olnud probleemiks õige patsiendi andmete ühendamine.[72] Seetõttu on tervishoiuteenuse pakkujatel vaja olla eriti tähelepanelik, et mobiilirakenduse arendajatele ei saadeta vale patsiendi terviseandmeid. Eestis nõusolekuteenusega ei ole sellist probleemi ette näha, kuna iga patsient on unikaalselt tuvastatav läbi isikukoodi ning peamiselt kõik terviseandmed on säilitatud kesksetes riiklikes andmekogudes.

Käesolevas peatükis on toodud välja riskid, mis on juba praegu valmistanud probleeme isikuandmete töötlemisega, sh mitmel juhul ka terviseandmetega. Näiteks OWASP (*Open Web Application Security Project*) on toonud kõige olulisemate privaatsusriskidena välja järgmised: andmeleke, ebaadekvaatne turvaintsidentidele reageerimine, ebaturvaline andmevahetus, isikuandmete töötlemisega seotud dokumentatsioon ei ole läbipaistev ning andmesubjektile lihtsasti kättesaadav või arusaadav, andmeid kogutakse suuremal hulgal kui eesmärgi täitmiseks vajalik ning andmesubjekti isikuandmeid jagatakse kolmandate osapooltega ilma nende nõusolekuta.[73] Võimaldades terviseandmete edastamist erasektoris olevatele kolmandatele osapooltele tuleks neile riskidele pöörata täiendavalt tähelepanu, sest vastasel juhul võib suurel hulgal terviseandmete edastamine tuua kaasa hulga andmekaitsealaseid rikkumisi. Kui isikuandmed on kord juba avalikuks saanud, siis on rikkumisele eelnenud olukorda väga raske või ka võimatu taastada.[74]

Andmesubjekti isikuandmete õigusliku aluseta töötlemise riski juures tuleks autori hinnangul eristada ka ebaseadusliku töötlemise mõju andmesubjektile: kas töötlemine toimub üksnes kolmanda osapoole poolt ettevõttesiseselt või jagatakse andmeid omakorda edasi andmemaakleritele. Viimase puhul võib eeldada oluliselt suuremat kahjulikku mõju andmesubjektile kuivõrd võimalike töötlejate ring muutub näiteks andmete müümise korral sisuliselt määramatuks.

72 Yednak, C. Providers and payers still grapple with privacy concerns under final interoperability rules. PWC.

73 OWASP on mittetulundusühing, mis tegeleb rahvusvaheliselt erinevate tarkvara turvalisuse parandamise projektidega. Privaatsusriskide hindamisel on lähtutud selle esinemissagedusest ning mõjust. Täpsemalt OWASP Top 10 Privacy Risks 2014 ja 2021. Kättesaadav: https://docs.google.com/spreadsheets/d/1GstkaCzO7_ok1p4rr1drq0SuPLjg5MlkshG5oS58vAY/edit#gid=0 (28.04.2021).

74 Gutwirth, S., Leenes, R. De Hert, P. Data Protection on the Move - current developments in ICT and Privacy/Data Protection. Springer: 2016, lk 358.

2.2. Terviseandmete edastamine kolmandatele osapooltele majandushuvi eesmärgil

Käesolevas alapeatükis on kolmandate isikute all peetud silmas eraõiguslikke juriidilisi isikuid, kes võivad avaldada soovi tarbija terviseandmete saamiseks läbi nõusolekuteenuse selleks, et pakkuda tarbijale näiteks paremaid hindu, kuid sisuliselt tagatakse sellega ettevõtte enda majandushuvisid ja seadusest tulenevat kohustust. Sellisteks ettevõteteks on näiteks krediidiasutused ja krediidiandjad- ning krediidivahendajad (edaspidi ühiselt krediidiandja), kellel on seadusest tulenev kohustus hinnata enne tarbijakrediidi väljastamist tarbija krediidivõimelisust vastavalt võlaõigusseaduse (edaspidi VÕS)[75] §-le 403[4] ning samuti kindlustusandjad, kellel on kindlustuslepingute sõlmimisel kohustus hinnata kindlustusriske. Nii kindlustusriski hindamise kui ka krediidivõimelisuse hindamise eesmärk on eelkõige mõista riski olemust ja kaasneda võivat kahju. Seega üldistatult ettevõtetele piisavate käibevahendite tagamine ning krediidiandjate puhul ka tarbijate poolt ülelaenamise ning sellega seotud kahju vältimine.

Krediidiandjatele ja kindlustusandjatele andmesubjekti nõusoleku alusel terviseandmete jagamisega seotud oht seisneb peamiselt selles, et tarbijatega sõlmitavaid lepinguid hakatakse siduma andmesubjekti poolt antava nõusolekuga nii tugevalt, et sisuliselt pole võimalik nõusoleku andmisest keelduda ilma, et see tooks talle kaasa kahjulikud tagajärjed (nt kallim leping või ei sõlmita lepingut üldse). Seega sisuliselt muutub küsitavaks andmesubjekti poolt antava nõusoleku vabatahtlikkus.

Riski realiseerumise ja selle mõju ulatuse hindamisel tuleb kindlustusandjate puhul võtta arvesse ka seda, et praktikas küsivad ka praegu kindlustusandjad andmesubjektidelt vabatahtliku kindlustuse sõlmimise jaoks terviseandmeid nõusoleku alusel. Autori hinnangul mõjutab riski ka see kas kindlustusandjal on võimalik TIS-st saadavaid andmeid pärast kindlustuslepingu sõlmimist regulaarselt uuendada või on tegemist ühekordse andmepäringuga.

Kehtiva kindlustustegevuse seaduse (edaspidi KindlTS)[76] §-le 218 lg 2 punkti 1 kohaselt on kindlustusandjatel õigus töödelda terviseandmeid ilma andmesubjekti nõusolekuta, kui kindlustuslepingu sõlmimise kohustus tuleneb seadusest (nt kohustuslik liikluskindlustustus).

75 Võlaõigusseadus. - RT I 2001, 81, 487...RT I, 04.01.2021, 2.
76 Kindlustustegevuse seadus. RT I, 07.07.2015, 1...RT I, 04.12.2019, 8.

Seega selliste lepingute sõlmimise osas puudub kindlustusandjal vajadus nõusolekuteenuse kaudu terviseandmeid küsida, sest KindlTS § 219 alusel on õigus kindlustusandjal pöörduda riigi- või kohaliku omavalitsuse asutuse, tervishoiuteenuse osutaja, kindlustusandja või muu kolmanda isiku poole vajalike terviseandmete saamiseks. Samuti ei ole kindlustusandjal vajalik küsida nõusolekut terviseandmete töötlemiseks kõikvõimalike kindlustuslepingute puhul, kui kindlustuslepingu täitmise kohustuse ja selle ulatuse kindlaksmääramine ning tagasinõuete esitamine eeldab andmesubjekti terviseseisundi või puude kohta andmete töötlemist (KindlTS § 218 lg 2 p 2). Seda näiteks ka reisitõrkekindlustuse korral.[77] Terviseandmete töötlemine kindlustuslepingute sõlmimiseks ja kindlustusriski hindamiseks nõusoleku alusel tuleb kõne alla vabatahtlike kindlustuslepingute puhul (KindlTS § 218 lg 1). Näiteks võib kindlustusandjal tekkida huvi terviseandmete saamise vastu elukindlustuslepingu sõlmimisel, et tuvastada tarbija raskelt haigestumise tõenäosust. Samas tuleb arvestada, et KindlTS § 216 lg 2 kohaselt ei tohi kindlustusriski hindamisel võtta arvesse kindlustusvõtja rasedust ega emadust kindlustusmaksete ja – hüvitiste suuruse hindamisel. Seega nimetatud terviseinfo osas puudub risk, et kindlustusandja sooviks nende kohta andmesubjekti nõusolekut läbi nõusolekuteenuse. Küll aga võib kindlustusandja soovida muid terviseandmeid, mis on tervisega seotud kindlustusriski hindamise puhul olulised ja näiteks Compensa Life selgitab enda privaatsusteates, et „nõusoleku tagasi võtmine ning terviseandmete kasutamise keelamine võib tähendada, et me ei saa Teiega kindlustuslepingut sõlmida või muuta."[78] Omaette küsimus on see kuivõrd saab teatud kindlustuslepingu raames antavat nõusolekut terviseandmete töötlemise osas pidada üldse vabatahtlikult antavaks nõusolekuks olukorras kus andmed on vajalikud kindlustusriski kindlaksmääramiseks ning ilma vastavate andmeteta pole kindlustusandjal võimalik seda teha. Õiguse ja eetika töörühma raportis on selgitatud, et tervisekahjustuse või surma korral kindlustusandja on selge, et konkreetse juhtumi jaoks on vajalik saada terviseandmeid ning seadus annab talle ka õiguse neid andmeid töödelda sõltumata andmesubjekti nõusolekust.[79] Pigem on küsimus selles kas selle jaoks on vajalik ja õigustatud anda kindlustusandjale otsejuurdepääs andmekogule, sest seni sai kindlustusandja vajalikud andmed kas kindlustatu või arsti käest.[80] Kui andmesubjekt annab oma nõusoleku terviseandmete edastamiseks ning kindlustusandjad saavad selle alusel vastavat terviseinfot, siis töö autori hinnangul eksisteerib antud probleem juba ka täna ning see, et edaspidi võimaldatakse nõusoleku andmist nõusolekuteenuse kaudu ei tekita juurde

77 Pärgmäe, R. jt. Õiguse ja eetika töörühma raport 2015, lk 26.
78 Compensa Life Vienna Insurance Group SE. Privaatsusteade. Kättesaadav: https://www.compensalife.eu/EE/show.asp?docID=public.company.privacy (28.04.2021).
79 Pärgmäe, R. jt. Õiguse ja eetika töörühma raport 2015, lk 29.
80 Samas, 29.

täiesti uut ohtu. Samuti tuleb arvestada, et kindlustusandjale antav nõusolek sisaldab endas kindlustusriski tuvastamise eesmärki ning nõusolekuteenuse antava nõusoleku eesmärk on andmed edastada. Autori hinnangul tuleks seetõttu ka nende kehtivust eraldiseisvalt käsitleda. Kui andmesubjekt annab nõusoleku oma terviseandmete töötlemiseks kindlustusriski hindamiseks, siis selles osas on selgelt küsitav kas ka praegune regulatsioon vabatahtliku kindlustuslepingu puhul terviseandmete edastamiseks nõusoleku alusel on kohane. Seejuures arvestades ka. Näiteks Ühendkuningriigis leiti andmekaitseseaduse väljatöötamisel leiti, et kindlustuslepingute sõlmimiseks, mille jaoks on terviseandmete töötlemine vajalik, peaks tingimusliku nõusoleku vältimiseks olema lubatud terviseandmeid töödelda ka ilma andmesubjekti nõusolekuta.[81] Nõusolekuteenusega saaks andmesubjekt valida: kui andmed edastada, siis mis kanalit kaudu, st sisuliselt antaks nõusolek konkreetse edastamisviisi osas.

Krediidiandja võib kehtiva seaduse kohaselt töödelda ilma andmesubjekti nõusolekuta tavalisi isikuandmeid näiteks rahapesu ja terrorismi tõkestamise seadusest[82] (edaspidi RahaPTS) tulenevatel eesmärkidel ning krediidiasutuste seaduses[83] (edaspidi KAS) toodud juhtudel. Krediidiandja huviks võib aga olla ka krediidivõimelisuse hindamise käigus siduda laenuvõtja sissetulekuallika võimalikku vähenemist tarbija tervisest tulenevatest ohtudega. Selleks, et täpsemalt hinnata krediidiandjate võimalikku huvi tarbija terviseandmete saamiseks tuleks hinnata seda koos krediidivõimelisuse hindamise aluseks olevate nõuetega, mis on üks vastutustundlikku laenamise põhimõtetest, mida krediidiandjad kohustuvad rakendama. VÕS §-st 403[4] lg 2 tulenevalt peab krediidiandja hindama kõiki talle teadaolevad asjaolusid, mis võivad mõjutada tarbija võimet krediit tagasi maksta lepingus kokkulepitud tingimustel, sealhulgas tarbija varalist seisundit, regulaarset sissetulekut, teisi varalisi kohustusi, varasemate maksekohustuste täitmise ja tarbijakrediidilepingust tulenevate rahaliste kohustuste võimaliku suurenemise mõju, määrates vajalike hindamistoimingute ulatuse vastavalt tarbijakrediidilepingu tingimustele, tarbija kohta olemasolevatele andmetele ja võetava rahalise kohustuse suurusele. Lisaks peab krediidiandja lähtuma ka krediidiandjate ja -vahendajate seaduse (edaspidi KAVS) § 49 lõike 1 punktides 1–7, lõike 2 punktides 1–3, lõike 3 punktides 1–3 ja lõikes 7 sätestatust. KAVS § 49 lg 4 kohaselt peaks krediidivõimelisuse hindamise tulemusel olema krediidiandjal võimalik veenduda kas tarbija suudab endale võetavaid kohustusi täita kogu lepingu perioodi jooksul vastavalt kokkulepitule

81 Practical problems in processing medical information under the GDPR. 11.08.2017. Kättesaadav: https://kennedyslaw.com/thought-leadership/article/practical-problems-in-processing-medical-information-under-the-gdpr/ (28.04.2021).
82 Rahapesu ja terrorismi rahastamise tõkestamise seadus. - RT I, 17.11.2017, 2...RT I, 14.04.2021, 6.
83 Krediidiasutuste seadus. - RT I 1999, 23, 349...RT I, 04.01.2021, 33.

või mitte. Krediidivõimelisuse hindamise eesmärgiks on vältida klientide poolt ülelaenamist ning makseraskuste tekkimist, mis on oma olemuselt määratlematu risk. „Vastutustundliku laenamise põhimõtte rakendamisega ei saagi seetõttu igal üksikjuhul tarbija makseraskusi vältida, küll aga on selle põhimõtte järgimisel võimalik ära hoida ülelaenamisega seotud probleeme, mis on ilmsed juba krediidivõtmise ajal."[84] Seega, terviseinfo küsimine võimaldaks krediidiandjal vähemalt krediidivõtmise ajal hinnata kas lisaks kliendi vanusele võib olla ka tervisest tulenevaid spetsiifilisi asjaolusid miks tarbijal pole mingi hetk võetavat kohustust tõenäoliselt täita. Näiteks eluasemelaenu puhul kõrge ea tõttu. VÕS § 403[4] lg 2 kohaselt peab krediidiandja hindama kogumis kõiki talle teadaolevaid asjaolusid, mitte üksnes neid, mis on eraldi lg 2 välja toodud. Sama paragrahvi lg 3 kohaselt küsib krediidiandja vajaduse korral tarbijalt krediidivõimelisuse hindamiseks täiendavalt teavet ning tarbija peab esitama krediidiandjale õige ja täieliku teabe. Olgugi, et ainult tarbijal on täielik ülevaade enda kohustustest ja varalisest seisust, siis ei saa eeldada, et tarbija peaks teadma, millised konkreetsed andmeid on tema krediidivõimelisuse hindamise jaoks vajalikud.[85] Küll aga peab seda teadma krediidiandja ning seetõttu krediidiandja teavitab tarbijat millist liiki teavet ja milliseid tõendeid peab tarbija talle krediidivõimelisuse jaoks esitama.[86] Seega, kui krediidiandja küsib kas võib olla muid ettenähtavaid asjaolusid, mis tõenäoliselt võivad vähendada tarbija maksevõimet lähitulevikus ja kui tarbijal on diagnoositud viimases staadiumis olev pahaloomuline kasvaja, siis objektiivselt võttes on see teave, mis mõjutab tema maksevõimet ning seega kaasneks ka kohustus krediidiandjale seda infot jagama. Samuti võib objektiivselt võttes mõjutada maksevõimet emaduspuhkusele jäämine. Kui krediidiandja on konkreetset infot küsinud, aga tarbija jätab teadlikult info esitamata, siis ei ole ta enda kohustust täitnud. Võlaõigusseaduse kommenteeritud väljaandes on rõhutatud, et tarbija ei tohi krediidiandjale esitatavaid andmeid varjata või võltsida.[87] Siinjuures tuleb ka arvestada, et krediidivõimelisuse hindamist tuleb teostada enne lepingu sõlmimist VÕS §-st 403[4] lg 1, aga lisaks ka krediidisumma muutmisel või ülempiiri suurendamisel (VÕS § 403[4] lg 9) ning makseraskustesse sattumisel, et oleks võimalik leida sobilik meede lepingu restruktureerimiseks.[88] Kuigi käesoleva töö autori hinnangul ei ole laenusaajalt terviseandmete

84 Koll, K. Vastutustundliku laenamise põhimõte, lk 9. Kättesaadav: https://www.just.ee/sites/www.just.ee/files/kristiina_koll._vastutustundliku_laenamise_pohimote.pdf (28.04.2021).

85 Varul, P., Kull, I. Kõve, V., Käerdi. M. Sein, K. Võlaõigus II. Kommenteeritud väljaanne. Juura. Tallinn, 2019, lk 612.

86 Samas, lk 612.

87 Samas, lk 611.

88 Finantsinspektsiooni soovituslik juhend. Vastutustundliku laenamise nõuete kohta. Tallinn 13.06.2016. Kättesaadav: https://www.fi.ee/et/juhendid/banking-and-credit/vastutustundliku-laenamise-nouded (28.04.2021).

küsimine turu praktika, siis teoorias võib krediidiandjal olla huvi andmesubjekti terviseandmete vastu mitmel korral. Lisaks võib olla soov siduda laenulepingu sõlmimist mõne vabatahtliku kindlustuslepinguga, et maandada oma riske. Ent arvestades krediidivõimelisuse raames antavat infokohustust ei saa kindlalt väita, et tegemist oleks laenusaaja poolt vabatahtliku nõusolekuga terviseandmete töötlemiseks. Seetõttu tuleks pigem eitada võimalust anda nõusolekut terviseandmete töötlemiseks krediidivõimelisuse läbiviimiseks. Küll aga võiks käesoleva autori hinnangul olla andmesubjektil valik millist kanalit terviseandmete edastamiseks kasutada ehk andmesubjektil võib olla vaba valik otsustada, et ta soovib lasta edastada andmed elektrooniliselt läbi nõusolekuteenuse.

2.3. Terviseandmete töötlemine kolmanda osapoole poolt algsest erineval eesmärgil

Käesolevas alapeatükis on käsitletud terviseandmete töötlemiseesmärki, mis seondub kolmandale osapoolele antud nõusolekuga ehk sellega, mis antud terviseandmetel põhinevat teenust pakkuvale ettevõttele. Nagu eelnevalt kirjeldatud, siis nõusolekuteenuse puhul annab andmesubjekt kaks erineva sisuga nõusolekut ja need on seotud erinevate töötlemiseesmärkidega: üks andmete edastamiseks riiklikust andmekogust ja teine kolmandale osapoolele konkreetse teenuse pakkumiseks (nt vaktsineerimiskalender). Kuna kolmas osapool ei tegutse riikliku andmekogu volitatud töötlejana, vaid tegutseb iseseisvatel enda poolt kindlaksmääratud eesmärkidel, siis tuleb teda käsitleda vastutava töötlejana andmekaitse üldmääruse artikli 4 punkti 7 mõttes. Selleks vajab ta andmesubjektilt tema terviseandmete töötlemiseks eraldiseisvat nõusolekut. Teenuste arendamise või muude teenuseosutamisest eraldiseisvate töötlemistoimingute juures tuleb vastutaval töötlejal pidada silmas konkreetset nõusolekut, selles piiritletud eesmärgi kirjeldust ning hinnata kas töötlemiseesmärk võib aja jooksul muutuda. Andmekaitse üldmääruse kohaselt tuleb andmete töötlemisel algsest erineval eesmärgil veenduda, et kavandatav uus töötlemise eesmärk on kooskõlas algse eesmärgiga (artikkel 6 (4)). Kolmas osapool vastutava töötlejana peab suutma tuvastada niisiis iga töötlemise toimingu puhul, sh tehnilise uuenduse puhul kas tegemist on üksnes konkreetse töötlemistoimingu teostamiseks vajaliku tehnilise muudatusega ning andmete töötlemiseesmärk jääb samaks või toob tehniline uuendus kaasa ka töötlemise eesmärgi muutuse. Sellele vastuse leidmiseks tuleb kolmandal osapoolel vastutava töötlejana analüüsida järgmist: võrrelda esialgselt terviseandmete kogumise aluseks olnud eesmärki eesmärgiga, mida kavandatakse edasisel töötlemisel; võttes arvesse terviseandmete kogumise

konteksti, eelkõige andmesubjektide ja vastutava töötleja vahelist seost; arvestada, et terviseandmete näol on tegemist eriliigiliste andmetega; analüüsida planeeritava edasise töötlemise võimalikke tagajärgi andmesubjektide jaoks; ja tagada asjakohaste kaitsemeetmete olemasolu, milleks võivad olla näiteks krüpteerimine ja pseudonümiseerimine. Juhul kui terviseandmete edasine töötlemine oleks algse töötlemiseesmärgiga vastuolus, siis tuleks veenduda, et on olemas mõni muu andmekaitse üldmääruse artiklis 9 (2) toodud õiguslik alus. Kolmanda osapoole poolt, kelle töötlemiseesmärgid ei lange kokku artikli 9 (2) punktides b) - j) tooduga oleks ainsaks kohaseks õiguslikuks aluseks uue nõusoleku küsimine. Eksisteerib risk, et kolmas osapool, kes saab andmesubjekti terviseandmed enda valdusesse ei täida enda kohustust vastutava töötlejana piisava hoolsusega või eirab toodud nõudeid teadlikult näiteks majandusliku kasu eesmärgil.

Nõusolekuteenuse kaudu andmeid saavate kolmandate osapoolte poolt võib eristada kahte liiki andmekasutust: esmane ja teisene. Isiku terviseandmete esmane kasutus seisneb kolmanda osapoole poolt selles, et ettevõte võtab riiklikust andmekogust edastatud terviseandmed vastu ning seejärel osutab nende põhjal andmesubjektile teenust. Selleks võib olla näiteks mobiilirakenduse kaudu pakutav konkreetse isiku terviseandmetel põhinev ravimikapi teenus, mis saab hetkel andmed andmesubjekti sisestuse kaudu.[89] Nõusolekuteenusega on võimalik muuta protsess andmesubjekti jaoks lihtsamaks, sest andmesubjekt annab oma nõusoleku tervise infosüsteemi (edaspidi TIS) vastutavale töötlejale, kes edastab kogu nõusoleku kehtivuse aja jooksul konkreetse andmesubjektiga seotud eelnevalt kindlaks määratud terviseinfo[90] teenusepakkuja mobiilirakendusse.[91] Nii võib kolmas osapool ehk teenusepakkuja võimaldada näiteks teenust, mis analüüsib konkreetsele andmesubjektile väljakirjutatud või käsimüügist ostetavate ravimite, toidulisandite ning samuti vaktsiinide võimalikke kõrvalmõjusid ning omavahelisi konflikte.

89 vt MediKeep ravimikapi teenus. Kättesaadav: https://medikeep.eu/termsofuse/ (28.04.2021).

90 Enne kui andmesubjekt saab anda riiklikule andmekogule nõusoleku oma terviseandmete edastamiseks on vajalik seada üles andmevahetuse valmisolek konkreetse ettevõtte ja riikliku andmekogu vahel. Nõusolekuteenuse analüüsis toodud riskide maandamise ettepaneku kohaselt esitab ettevõte taotluse nõusolekuteenusega liitumiseks ning märgib ära talle teenuseosutamiseks vajalikud andmed või andmekomplektid ning selgitab nende seost enda edasise töötlemiseesmärgiga. Selle põhjal on võimalik taotluse menetlemise jooksul selgitada välja kas taotletavad andmed on loogilises seoses planeeritava teenusega. vt täiendavalt Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 31.

91 Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 64 (joonis nr 16).

Teisene kasutus kolmanda osapoole poolt seisneb aga algselt muul eesmärgil kogutud terviseandmete edasises töötlemises. Näiteks töötlemine, mis on suunatud pigem andmesubjekti kasule: teenusepakkuja lisab mobiilirakendusse täiendavaid teenuseid, kuid varasem nõusolek ei pruugi olla uute teenuste eesmärkidel töötlemiseks piisav. Ohtlikum on aga töötlemine, mis täidab üksnes teenusepakkuja huve. Näiteks kogutud terviseandmete, sh profileeritud kasutaja andmete müük kolmandatele isikutele. Seega nii andmete esmase kui ka teisese kasutamise juures on tähtis, et vastutav töötleja tagaks igal hetkel õigusliku aluse olemasolu.

Töötlemiseesmärk peab olema konkreetselt väljendatud ning ei tohiks jätta võimalust, et kolmas osapool vastutava töötlejana saab selle alusel töödelda andmeid ka viisil, milleks andmesubjekt ei ole nõusolekut andnud ning millest ei ole teda teavitatud. Andmekaitse üldmääruse selgituspunktis 50 on rõhutatud, et isikuandmete töötlemisel esialgsetest muudel eesmärkidel tuleb igal juhul tagada määruses sätestatud põhimõtete rakendamine ning eelkõige andmesubjekti teavitamine kõnealustest muudest eesmärkidest enne töötlemise alustamist.[92]

Kui vastutav töötleja väidab, et töötleb terviseandmeid andmesubjekti nõusoleku alusel, kuid eesmärgi kirjeldus on liiga lai ning üldine, siis ei ole võimalik teadliku nõusoleku olemasolu kindlalt väita. Isik peab nõusoleku andmisel saama selgelt aru õiguslikust tagajärjest, mis nõusoleku andmisega kaasneb. Liiga üldine ja lai eesmärgi kirjeldus on tihtipeale sätestatud nö igaks juhuks, kuid see ei ole andmekaitse üldmäärusega kooskõlas, sest andmesubjektilt võetakse ära võimalus saada täpselt aru, mille kohta ta nõusoleku annab. Kui andmesubjekt ei saa sellest aru ja sõnastuse kohaselt ei olnud isegi võimalik nõusoleku andmise hetkel töötlemiseesmärgist selliselt aru saada, siis ei saa lugeda sellist nõusolekut kehtivaks nõusolekuks ning seega töötleb kolmas osapool vastavaid andmeid ebaseaduslikult. Reeglina ei ole mobiilirakendustes olevad tingimused andmesubjekti poolt eraldi läbiräägitavad ning kui andmesubjekt soovib teenust kasutada, siis on tal põhimõtteliselt valik - nõustuda või loobuda teenuse kasutamisest. Seega ühest küljest nõusolekuteenus võimaldab andmesubjektil omada suuremat kontrolli endaga seotud terviseandmete kasutamisega, kuid teisalt pole andmesubjektil reeglina eriti suurt võimalust mõjutada kolmanda osapoole poolt tehtavaid

92 Andmekaitse üldmääruse selgituspunkt 50 ja artikkel 13 (3).

andmetöötlustoiminguid ega alati valida mille kohta nõusoleku annab. Arvestades aasta-aastalt kasvavat rikkumisteadete ning kaebuste, vaiete ning väärteoteadete statistilist mahtu,[93] samuti konkreetsete ettekirjutuste sisu elementaarsete nõuete eiramise kohta[94] võib eeldada rikkumiste jätkuvat kasvu ning sedagi, et tegelik rikkumiste arv on suurem kui AKI menetlusse jõuavad.

Praktikas leidub juhtumeid, kus vastutavad töötlejad küsivad nõusolekuid nö igaks juhuks,[95] mis sisaldab endas mitmeid eesmärke või siis on nõusolek nii üldine, et algsest töötlemiseesmärgist pole võimalik üheselt aru saada. See, kui täpselt peaks eesmärk kirjeldatud olema sõltub konkreetsest kontekstist ning milliseid isikuandmeid töödeldakse, kuid üldjuhul tuleks lugeda liialt üldsõnaliseks järgmisi eesmärgi kirjeldusi: kasutajakogemuse parendamine, turundus, IT-turvalisus või tulevaste uuringute eesmärgil.[96] Näiteks Google LLC-le määrati 2019. aastal Prantsusmaa andmekaitse inspektsiooni poolt 50 miljonit eurot trahvi, kuna ettevõtte poolt võetud nõusolekud andmete töötlemiseks ei olnud ühemõttelised ega konkreetsed.[97]

Teenuse osutamisega seotud eesmärkide varju võib peita ka näiteks otseturunduslikud eesmärgid või andmemüügi. Näiteks Austria postiasutus, Österreichische Post AG, müüs suurel hulgal oma klientide profileeritud isikuandmeid nii ettevõtetele kui ka poliitilistele erakondadele ning nimetatud andmekomplektid sisaldasid mh andmeid isikute poliitilise seotuse, eelistuste ja harjumuste kohta.[98] Austria andmekaitse inspektsioon määras ettevõttele selle eest 18 miljonit eurot trahvi.[99]

93 Andmekaitse Inspektsiooni veebileht. Statistika. Kättesaadav: https://www.aki.ee/et/teavitus-uudised/statistika (28.04.2021).
94 Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr. 2.1.-6/20/25, 20.07.2020. Kättesaadav: https://www.aki.ee/sites/default/files/ettekirjutused/2020/ettekirjutus-hoiatus_travibest.pdf (28.04.2021).
95 Andmekaitse Inspektsiooni aastaraamat. 2019. Kättesaadav: https://aastaraamat.aki.ee/aastaraamat-2019-jaa-hakkas-hooga-liikuma/avalikkus-ootas-tolgendamist-ja-selgitusi (28.04.2021).
96 Article 29 Data Protection Working Party opinion on purpose limitation, lk 52.
97 The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. 21.01.2019. Kättesaadav: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (28.04.2021).
98 GDPR Fines Database – List of Fines. International Network of Privacy Law Professionals. Kättesaadav: https://gdpr-fines.inplp.com/list/ (28.04.2021).
99 Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG (Austrian Postal Service). 23.10.2019. Kättesaadav: https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_et (28.04.2021).

Kuna terviseandmetel on personaalmeditsiini arengu juures väga oluline roll, siis on tõenäoline, et kolmandad osapooled otsustavad majandusliku kasu eesmärgil neid ka andmemaakleritele edasi müüa.[100] Andmemaaklerid omakorda müüvad infot ettevõtetele, kellel võiks sellest infost oma kauba või teenuse müümisel kasu olla. Siinjuures peab aga vastutav töötleja viima jälle läbi hindamise, et vältida vastuolu algse töötlemise eesmärgiga. Eraldi mainib väärimist asjaolu, et kui kolmas osapool vastutava töötlejana plaanib terviseandmed enne müümist anonüümida, siis ka anonüümimise protsessi võidakse lugeda edaspidiseks töötlemiseks, mis erineb algsest eesmärgist.[101] Andmekaitse töörühma arvamuses on selgitatud, et anonüümimistehnikate kasutamine on isikuandmete töötlemine ning neid kasutatakse andmete anonüümseks muutmise eesmärgil ning seega kujutab see endast „täiendavat töötlemist"[102] ja peab olema kooskõlas eesmärgipiirangu nõuetega.[103] Seda arvamust on ka kritiseeritud, kuna anonüümimist võiks tõlgendada kui vajalik andmeturbe meede ning kui anonüümimist peaks protsessina eraldiseisvalt õigustama, siis võib see takistada privaatsust tagavate tehnoloogiate kasutamist.[104]

Financial Times'i poolt läbiviidud uuringuga tuvastati saja tervisega seotud veebilehe (nt WebMD, Healthline, Bupa, Babycentre) puhul, et neist 79 % on lubanud kolmandatel osapooltel lisada küpsised, mis koguvad külastajatelt ilma nende nõusolekuta mitmesuguseid tervisega seotud andmeid nagu diagnoosid, sümptomid, väljakirjutatud retseptid, viljakus ning edastavad need kas mõnele vähemtuntud andmemaakleritele või tehnohiidudele nagu Google, Amazon, Facebook, Oracle.[105] Ühtlasi toodi välja, et isikuandmete töötlemise kordades, millega ajakirjanikud nõustusid, ei selgitatud nende terviseandmete jagamist kolmandate osapooltega või selle eesmärke ning ükski testitav veebileht ei küsinud nõusolekut

100 Your Data Is Shared and Sold…What's Being Done About It? Wharton School, University of Pennsylvania, 28.10.2019. Kättesaadav: https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ (28.04.2021).

101 Spindler, G., Schmechel, P. Personal Data and Encryption in the European General Data Protection Regulation. – Journal of Intellectual Property, Information Technology and E-Commerce Law, 163(7), 2016, punkt 2.2.2. Kättesaadav: https://www.jipitec.eu/issues/jipitec-7-2-2016/4440 (28.04.2021).

102 Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 05/2014 anonüümimistehnikate kohta. Vastu võetud 10. aprillil 2014, lk 7. Kättesaadav: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_et.pdf (28.04.2021).

103 Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation.

104 Spindler, G., Schmechel, P. Personal Data and Encryption in the European General Data Protection Regulation, punkt 2.2.2.5.

105 Kasutatud küpsiste hulgast tuvastati ka selliseid küpsiseid, mis jälitavad kasutajaid ning sisaldavad andmesubjekti unikaalselt tuvastatavat elementi. vt Murgia, M., Harlow, M. How top health websites are sharing sensitive data with advertisers. - Financial Times. 13.11.2019. Kättesaadav: https://www.ft.com/content/0fbf4d8e-022b-11ea-be59-e49b2a136b8d (28.04.2021).

konkreetselt eriliigiliste andmete töötlemiseks.[106]

Ühendkuningriigi andmekaitseasutus (edaspidi ICO) teavitas juunis 2019, et veebireklaamitööstus peaks vaatama üle enda andmetöötluse praktika, viima vajalikud muudatused sisse ning eelkõige pöörama tähelepanu korrektsele nõusolekule.[107] ICO toob reklaamitööstust käsitlevas raportis välja, et igasugune isikuandmete erikategooriate töötlemine toimub ebaseaduslikult, kui andmesubjektilt ei ole küsitud selgesõnalist nõusolekut selleks ning võib arvata, et reklaamitööstuses tegutsevad vastutavad töötlejad ei ole andmekaitsealaseid mõjusid korrektselt hinnatud, sh tundub turul puuduvat selge arusaam andmekaitsealase mõjuhinnangu nõuete osas.[108] Seega võib öelda, et terviseandmete töötlemine ilma õigusliku aluseta on muutumas järjest enam probleemiks.

Kokkuvõtvalt võib öelda, et kolmanda osapoole poolt algsest erineval eesmärgil andmete töötlemise osas seisneb risk peamiselt asjaolus, et vastutav töötleja ei oma andmete töötlemiseks uuel eesmärgil õiguslikku alust ja seda kas teadlikult eirates või hooletusest. Hoolimata sellest, et otseturundusega seotud nõusoleku küsimise kohta on tehtud küllaltki põhjalikku teavitustööd esineb endiselt sellega seotud rikkumisi. Näiteks tuvastati Küprosel, et üks arst jagas oma Instagrammi kontol ilma patsiendi nõusolekuta oma patsiendi isikuandmeid.[109] Samuti on Eesti Andmekaitse Inspektsioon (edaspidi AKI) saanud kaebusi andmete töötlemisest ilma isiku nõusolekuta. Näiteks saatis Reisibüroo Travibest OÜ andmesubjekti e-postile pidevalt soovimatut reklaami ning kaebaja ei olnud ise nimetatud büroole oma andmeid jaganud.[110] Samuti sai AKI kaebuse, kus tarbija tellis endale Thats It OÜ Facebooki lehelt kaupa, kuid pärast seda hakkas tarbija saama pidevalt otseturustusteateid nii SMS-i kui ka Facebooki sõnumirakenduse kaudu ning puudus igasugune võimalus nendest

106 Murgia, M., Harlow, M. How top health websites are sharing sensitive data with advertisers.
107 McDougall, S. Blog: ICO Adtech update report published following industry engagement. 20.06.2019. Kättesaadav: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/ (28.04.2021).
108 Information Commissioner Officer. Update report into adtech and real time bidding. 20.06.2019, lk 23. Kättesaadav: https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf (28.04.2021).
109 Doctor fined €14,000 for revealing personal data of patient on Instagram. 11.10.2019. Kättesaadav: https://in-cyprus.philenews.com/doctor-fined-e14000-for-revealing-personal-data-of-patient-on-instagram/ (28.04.2021).
110 Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr. 2.1.-6/20/25, 20.07.2020. Kättesaadav: https://www.aki.ee/sites/default/files/ettekirjutused/2020/ettekirjutus-hoiatus_travibest.pdf (28.04.2021).

loobuda, sh ei aidanud ettevõttele kirjutamine.[111]

2.4. Kolmandate osapoolte poolt terviseandmete anonüümimistehnika kasutamine

Tervisega seotud infot võidakse jagada, sealhulgas müüa ka anonüümsena. Anonüümseid andmeid, sh ka anonüümset terviseinfot ei loeta andmekaitse üldmääruse kohaselt isikuandmeteks juhul, kui mõistlikke pingutusi kasutusele võttes ei ole keskmisel isikul võimalik konkreetset isikut tuvastada.[112] Selles osas kui ulatuslikult tuleks tõlgendada mõistlikke pingutusi on mitmeid erinevaid õiguslikke arvamusi. Lihtsustatult võttes peab vastutav töötleja analüüsima iga krüpteeritud andmekogumit ning tegema kindlaks kas mõistlikult võttes võib dekrüpteerimine olla võimalik, sealjuures arvestama ka pidevalt arenevat tehnoloogiat.[113] Seega, juhul kui mõistlikke pingutusi kasutusele võttes on andmestik võimalik dekrüpteerida, siis kohalduvad terviseandmete töötlemisele andmekaitse üldmäärusest tulenevaid nõudeid.

Õiguskirjanduses on toodud välja ka andmekaitseõigusega seotud kasvavat konflikti, mis autori hinnangul muutub eriti oluliseks just anonüümsete andmete kontekstis, sest tegemist võib olla ka andmetega, mille puhul on konkreetne isik halvasti rakendatud anonüümimistehnika tõttu tuvastatav ning sellest hoolimata müüakse andmed andmemaaklerile. Täpsemalt tekib siin, konflikt andmekaitseõiguse ja lepinguõiguse vahel seoses nõusoleku mõistega ja isikuandmete käsitlemist kui digitaalset kaupa. Kui andmekaitseõiguses käsitletakse nõusolekut väga rangelt ning õiguspäraselt kogutud andmete kasutamine ning edastamine on piiratud, siis lepinguõiguses võib pidada andmeid kaubaks - kui omandamine oli seaduslik, siis võiks õiguslikult ka kolmandatele isikutele müüa.[114] World Economic Forum (edaspidi WEF) on kirjeldanud isikuandmeid kui olulist majanduslikku ja sotsiaalset väärtust nii tarbijatele, eraettevõtetele kui ka avalikule sektorile.[115] WEF kritiseerib

111 Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr. 2.1.-6/20/20. 30.04.2020. Kättesaadav: https://www.aki.ee/sites/default/files/ettekirjutused/2020/ettekirjutus-hoiatus_thats_it_ou.pdf (28.04.2021).

112 Andmekaitse üldmääruse selgituspunkt 26.

113 Spindler, G., Schmechel, P. Personal Data and Encryption in the European General Data Protection Regulation, punkt 3.

114 Vicente, D. M., Casimiro, S. de V. Data Protection in the Internet. Springer 2020, lk 250.

115 Personal Data: The Emergence of a New Asset Class. An Initiative of the World Economic Forum. January 2011. In Collaboration with Bain & Company, Inc, lk, 32. Kättesaadav: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (28.04.2021).

muuhulgas, et õigusloome ei paku piisavat infrastruktuuri, et toetada hästitoimivat digitaalset majandust ja isikuandmete õiglast kasutamist, kuna eraettevõtted tekitavad isikuandmeid kasutades uut efektiivsust, stimuleerivad nõudlust ja teenivad nende pealt kasumit.[116] Seega peab ütlema, et samal ajal kui majanduse eest seisvad ettevõtted ja muud organisatsioonid peavad isikuandmeid kaubaks, siis õiguskirjanduses on see väga vaieldav. EDPB rõhutab, et isikuandmete kaitse on Euroopa Liidu Põhiõiguste Harta[117] artiklist 8 tulenev põhiõigus ning Euroopa Liidu Inimõiguste Kohus on korduvalt väljendanud oma seisukohta, et Euroopa Liidus ei saa isikuandmeid käsitleda kui eraldiseisvat varaklassi.[118] Isikuandmetele võib olla olemas potentsiaalne turg nagu ka inimorganitele, kuid see ei tähenda, et sellist teguviisi tuleks õiguslike vahenditega innustada.[119] Nõusolekuteenuse kontekstis on oluline, et vastutavad töötlejad ei hakkaks väärtuslikel terviseandmetel põhinevaid andmestikke müüma ning ka anonüümitud andmestike puhul peab olema selge veendumus, et andmed on ka päriselt anonüümsed ja et kolmandad osapooled ei tegeleks isikuandmete kaubandusega.

Seoses nõusolekuteenuse kasutusele võtuga on kolmandatel osapooltel võimalik tegeleda innovaatiliste teenuste arendamisega. On üsna tõenäoline, et mitmed teenusepakkujad kombineerivad konkreetse füüsilise isiku terviseandmete kogumist nii riiklikust andmekogust kui ka otse andmesubjektilt ning neid kahte kogumismeetodit kombineerides on teenusepakkujal võimalik luua unikaalseid andmekomplekte, mida varasemalt pole loodud. Sellised andmekomplektid võimaldavad uusi järelmeid, mis ei pruugi olla seotud üksnes üksikisiku tervise parendamisega, vaid võimaldab hinnata ja suunata ka tarbija ostukäitumist. Sellest lähtuvalt, usub autor, et loodavatel andmestikel on kaubanduslik väärtus ja võib olla suurem nõudlus ettevõtjate poolt. Kaubandusliku väärtuse tõttu võib teenusepakkuja otsustada enda valduses olevate andmestike müümist kolmandatele osapooltele. Anonüümimata terviseandmete edastamine või müümine ilma nõusolekuta pole lubatud siin võib olla tekkimas igapäevaselt andmesubjektidele mitte tajutav probleem, kus andmesubjektile teadaolevalt edastatakse teenusepakkuja poolt kolmandatele osapooltele üksnes anonüümitud andmeid, kuid tegelikkuses tekitatakse inimestele üksnes petlik turvatunne.

116 Personal Data: The Emergence of a New Asset Class. An Initiative of the World Economic Forum. January 2011. In Collaboration with Bain & Company, Inc, lk, 32. Kättesaadav: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (28.04.2021).

117 Euroopa Liidu Põhiõiguste Harta. - ELT C 326/02 2012, lk 391-407.

118 European Data Protection Supervisor. Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, lk 7. Kättesaadav: https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf (28.04.2021).

119 Samas, lk 7.

Teaduskirjanduses on juhitud tähelepanu, et anonüümsed andmed ei ole tegelikkuses nii anonüümsed kui andmesubjekt usub ning „tõeliselt anonüümse andmekogumi loomine, mis sisaldaks samas enamikku otstarbekohasest teabest, on väga keeruline."[120] Näiteks võib olla, et andmeid on töödeldud anonüümimismeetodiga, kuid õiguslikus mõttes pole tegemist siiski anonüümsete andmetega.[121] Dokument, mis ei sisalda konkreetselt isikute nimesid, aga sisaldab sündmusi või muide detaile, mille kaudu on isikud vähemalt kaudselt tuvastatavad ja vähemalt kolleegide poolt, siis tuleb piiripealsetel juhtudel eelistada isikuandmete nõuete sisustamisel alati tõlgendust, mis kaitseb tugevamini eraelu puutumatust.[122] Isikuandmete anonüümimise problemaatikat on põhjalikult uurinud ka professor L. Sweeney Harvardi ülikoolist analüüsides statistilisi anonüümitud terviseandmete komplekte, kus L. Sweeney suutis testide käigus tuvastada konkreetse füüsilise isiku ainuüksi kolme parameetri kasutamisel.[123] Seejuures demograafilise info juures mõjutas üksikisiku tuvastamise tõenäosust tugevalt see, kas andmekomplektis oli olemas isiku terviklik sünniaeg (päev, kuu ja aasta) või üksnes sünniaasta.[124]

Tegelik reidentifitseerimise risk ei sõltu üksnes kasutatavast anonüümimistehnikast, vaid ka sellest, mis infoga andmete vastuvõtja saadud infot kombineerib. Massandmete töötlemise ajastul ei saa lootma jääda sellele milliseid andmekomplekte on suudetud konkreetses juhtumianalüüsis tuvastada, reidentifitseerida ning teaduskirjanduses kajastada.[125] Seega, kui mõne anonüümitud andmekomplekti hulgast pole senimaani suudetud füüsilist isikut tuvastada, siis ei tohiks eeldada, et tegemist on turvalise andmekomplektiga ning, et see on täielikult anonüümne.

25.11.2020 Euroopa Komisjoni poolt esitatud andmehalduse määruse ettepaneku seletuskirja kohaselt planeeritakse laiendada mh isikustamata andmete (nt anonüümitud terviseandmete)

120 Artikli 29 alusel asutatud andmekaitse töörühma arvamus anonüümimistehnikate kohta, lk 3.
121 Bogdanov, D., Sillaste, T. Infotehnoloogilised võimalused põhiõiguste kaitsel. - Juridica 2020/6, lk 476.
122 Andmekaitse Inspektsioon. Vaideotsus avaliku teabe asjas nr 2.1-3/20/4685. 03.02.2021, lk 5. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).
123 Sweeney, L. Matching Known Patients to Health Records in Washington State Data. Harvard University. Data Privacy Lab. White Paper 1089-1. June 2013. Kättesaadav: https://dataprivacylab.org/projects/wa/1089-1.pdf (28.04.2021).
124 Gutwirth, S., Leenes, R. De Hert, P. Data Protection on the Move: Current developments in ICT and Privacy/ Data Protection. Springer 2016, lk 368.ja Sweeney, L. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. Kättesaadav: https://dataprivacylab.org/projects/identifiability/paper1.pdf (28.04.2021).
125 Samas, lk 363.

teisest kasutusvõimalust.[126] Andmehalduse määruse ettepaneku artiklis 5 (11) võetakse kasutusele väga tundlikuks tunnistatud isikustamata andmete mõiste ning sätestatakse, et selliste andmete edastamisel kolmandatesse riikidesse peavad olema rangemad tingimused. Ettepaneku põhjendusepunktis 19 selgitatakse, et see on vajalik andmete taaskasutamise vastu usalduse tekitamiseks ja väga tundlikeks isikustamata andmeteks võivad olla näiteks tervishoiu valdkonna teatavad andmestikud.[127]

Euroopa Andmekaitsenõukogu (edaspidi EDPB) ja Euroopa Andmekaitseinspektor (edaspidi EDPS) on juhtinud oma ühises arvamuses andmehalduse määruse ettepaneku osas tähelepanu, et isegi kui tegemist on anonüümsete andmetega ja konkreetse andmestiku kaudu ei ole võimalik füüsilist isikut tuvastada, siis täiendavate andmete kombineerimine võib tuua kaasa kaudse tuvastamise ning sellisel juhul jäävad need andmed tõenäoliselt isikuandmete määratluse reguleerimisalasse. Täiendavalt soovitavad EDPB ja EDPS tuua ka konkreetseid näiteid, milliseid andmeid tuleks lugeda väga tundlikeks isikustamata andmeteks.[128] See on oluline, sest mida rohkem informatsiooni on kättesaadaval ja mida rohkem seda taaskasutatakse sh järjest enam ka tehisintellekti poolt, seda raskem on pikaajaliselt tagada täielikku anonüümsust ning vastutavad töötlejad peavad arvestama teatava jääkriski võimalust.[129]

Teine suurem risk seondub sellega, et vastutav töötleja arvab ekslikult, et tegemist on anonüümitud andmetega, kuid tegelikkuses ei olnud privaatsustehnoloogiat korrektselt rakendatud ning üksikisik on andmestikust tuvastatav. Näiteks Harvardi Ülikooli teadlane L. Sweeney analüüsis oma artiklis ühte 2003. aastast pärit uuringut seoses ravimifirma turundusmaterjaliga, mille kohaselt 2,3% patsientidest olid üksikisikuna tuvastatavad ning 6,1% patsientidest oli võimalik tuvastada kaudselt, kus andmed viitasid kas ühele isikule või kahele samanimelisele isikule. Seda hoolimata sellest, et tegu oli anonüümitud retseptiravimite andmestikuga.[130]

126 Andmehalduse määruse ettepanek
127 Andmehalduse määruse ettepaneku põhjenduse punkt 19.
128 EDPB-EDPS joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act), lk 24. Kättesaadav: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-edps_joint_opinion_dga_en.pdf (28.04.2021).
129 Artikli 29 alusel asutatud andmekaitse töörühma arvamus anonüümimistehnikate kohta, lk 5.
130 Sweeney, L. Patient Identifiability in Pharmaceutical Marketing Data. Data Privacy Lab Working Paper 1015. Cambridge 2011, lk 1. Kättesaadav: https://dataprivacylab.org/projects/identifiability/pharma1.pdf (28.04.2021).

2.5. Lapse terviseandmete töötlemine õigusliku aluseta

Vähemalt 13-aastase lapse poolt antud nõusolek loetakse andmekaitse üldmääruse artikli 8 ja isikuandmete kaitse seaduse (edaspidi IKS)[131] § 8 lõike 1 kohaselt kehtivaks, kui kolmanda osapoole poolt pakutav teenus kvalifitseerub infoühiskonna teenuseks ning kohaldatakse andmekaitse üldmääruse artikli 6 (1) punkti 1). See aga tähendab, et lapse terviseandmete töötlemine infoühiskonna teenuse raames jääb andmekaitse üldmääruse artikli 8 kohaldamisalast välja, sest terviseandmete töötlemisele kohaldub artikkel 9. Seega alaealisel pole võimalik terviseandmeid vajavale infoühiskonna teenusele iseseisvalt kehtivat nõusolekut anda ja nõusolekuteenuse kaudu ei tohiks seda ka lubada, kui tehniliselt pole võimaldatud seadusjärgsel esindajal lapse eest nõusolekut anda. Muuhulgas peab ka kolmas osapool tagama, et alaealisel ei oleks võimalik konkreetset teenust mobiilirakenduses ilma seadusliku esindaja nõusolekuta kasutada. See on oluline juhuks kui konkreetset teenust saab kasutada ka selliselt, et andmesubjekt ise sisestab konkreetseid terviseandmeid. Praktikas on tavapärane, et mobiilirakenduses tuleb täita märkeruut, millega kinnitatakse oma vanus ning mis peaks tagama vastutavale töötlejale kehtiva nõusoleku. Autori hinnangul ei taga üksnes sellise märkeruudu kasutamine vastutavale töötlejale piisavat kindlust andmesubjekti vanuse väljaselgitamises ning seega kehtivat nõusolekut, sest seda on liiga lihtne võltsida.

2.6. Andmetöötluse läbipaistmatus

Andmetöötluse läbipaistmatust võib pidada terviseandmete kontekstis riskiks, mis kaasub nõusolekuteenuse pakkumisega ning selle laiema kasutusele võtmisega. Eelkõige siis, kui nõusolekuteenusega liituv ettevõte ei ole andmekaitsenõuetes piisavalt pädev ega ole arvestanud ka eraldi ressurssi sellega tegelemiseks. OWASP on üheks suuremaks privaatsusriskiks hinnanud läbipaistvuse põhimõttele mittevastavate isikuandmete töötlemise kordade kasutamise ja seda nii 2014 aastal kui ka 2021. aasta esialgsetes tulemustes.[132] Läbipaistvuse põhimõte eeldab, et vastutav töötleja selgitab andmesubjektidele lihtsal ja

131 Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.

132 OWASP Top 10 Privacy Risks 2014 ja 2021. Kättesaadav: https://docs.google.com/spreadsheets/d/1GstkaCzO7_ok1p4rr1drq0SuPLjg5MlkshG5oS58vAY/edit#gid=0; (28.04.2021). Loendi koostamise aluseks on kasutatud OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Kättesaadav: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (28.04.2021).

arusaadaval viisil oma andmetöötluse põhimõtteid, sh konkreetseid töötlemise eesmärke ja kellele andmeid omakorda edastada võidakse.[133]

Andmekaitse üldmääruse kohaselt peab nõusolek olema teadlik. Samas, kuivõrd saab nõusolekut pidada teadlikuks, kui isikuandmete töötlemise korrad on praktikas väga pikad ja keerulised, mistõttu enamus andmesubjekte jätavad need lugemata. Mcdonald, M. A. ja Cranor, F. L. uurisid aastal 2008 kui palju võtaks keskmisel internetti kasutaval ameeriklasel aega, et lugeda sõna-sõnalt läbi iga uue veebilehe privaatsuspoliitika, mida nad ühe aasta jooksul külastavad ning jõudsid järeldusele, et selleks kuluks ligikaudu 54 miljardit tundi.[134] Seega võib öelda, et andmesubjektid jätavad privaatsuspoliitika lugemata, kui see on liiga ajakulukas. Autorile teadaolevalt ei ole samasugust uuringut Euroopas tehtud, kuid on vähetõenäoline, et tulemus oleks teistsugune. Selline tulemus on selgelt vastuolus andmekaitse üldmääruses tooduga, mille kohaselt tuleb kogu andmesubjektidele antav teave esitada kokkuvõtlikult.[135] Ka andmekaitse üldmääruses on selgitatud, et ettenähtud teabe tõhusamaks edastamiseks tuleks kasutada ka muid meetodeid, näiteks visualiseerimist.[136]

Andmekaitse üldmääruses on läbipaistvuse põhimõte ja sellega seotud kord reguleeritud artiklites 12-15 ning terviseandmete edastamise kontekstis on neist olulisemad järgmised kohustused:

- teave vastutava töötleja kohta
- teave terviseandmete vastuvõtjate või vastuvõtjate kategooriate kohta
- teave isikuandmete töötlemise eesmärgi ja õigusliku aluse kohta
- kui andmekaitseametnik on määratud, siis tema kontaktandmed
- kui isikuandmed on kogutud andmesubjektilt, siis teave selle kohta kas vastutav töötleja kavatseb edastada terviseandmeid kolmandale riigile ning teave kaitse piisavust käsitleva komisjoni otsuse olemasolu või puudumise kohta või artiklis 46 või 47 või artikli 49 lõike 1 teises lõigus osutatud edastamise korral viide asjakohastele või sobivatele kaitsemeetmetele ja nende koopia saamise viisile või kohale, kus need on tehtud kättesaadavaks;
- kui isikuandmed ei ole saadud andmesubjektilt, siis teave selle kohta, et vastutav töötleja kavatseb edastada isikuandmed kolmandas riigis asuvale vastuvõtjale, ning teave kaitse piisavust käsitleva komisjoni otsuse olemasolu või puudumise kohta või rakendatud

133 Andmekaitse üldmääruse selgituspunkt 39.
134 Mcdonald, M. A, Cranor, F. L. The Cost of Reading Privacy Policies. - I/S: A Journal of Law and Policy for the information society. Vol. 4:3 2008, lk 536.
135 Andmekaitse üldmääruse selgituspunkt 58.
136 Andmekaitse üldmääruse selgituspunkt 58.

asjakohastele kaitsemeetmetele.

Nõusolekuteenuse esialgse lahenduse kohaselt kuvatakse andmesubjektile eesmärgideklaratsioon, mis sisaldab edastatavate terviseandmete kirjeldust, infot selle kohta, kellele andmed edastatakse ning samuti kolmanda osapoole poolt edastatud eesmärgi kirjeldust, milleks teenusepakkuja talle edastatavaid terviseandmeid plaanib kasutada.[137] Siinjuures tuleb tähele panna, et andmesubjekt annab kaks nõusolekut – ühe riigi andmekogu vastutavale töötlejale ning teise kolmandale osapoolele, kes talle terviseandmete pinnalt vastavat teenust pakub. Kui andmesubjekt annab nõusolekuteenuse kaudu oma nõusoleku ja seal on võimalik anda nõusolek andmete edastamiseks selliselt, et erinevatele andmekomplektidele nõusoleku andmisel eristatakse ka kolmanda osapoole kasutamiseesmärke, siis ühest küljest võimaldab see andmesubjektil teha informeerituma otsuse. Teisest küljest võib nõusoleku andmine läbi riikliku teenuse tekitada andmesubjektis liigse turvatunde, mistõttu ei panda tähele kui kolmandale osapoolele antud nõusolek on oluliselt erinevatel eesmärkidel. Näiteks liiga üldsõnaline või ka vastuolus eesmärkidega, mida kirjeldati andmesubjektile eesmärgideklaratsioonis. Samuti ei pruugi olla tagatud nõusoleku andmine iga eesmärgi suhtes eraldi nagu andmekaitse üldmäärus ette näeb.[138]

Teatud määral annab riski maandada see kui inimestel soovitatakse enne nõusolekuteenuse kaudu terviseandmete edastamist nõusoleku andmist tutvuma ka vastava kolmanda osapoole andmetöötlus põhimõtetega, kuid autori hinnangul ei maanda see riski täielikult, kuna andmesubjekt ja vastutav töötleja on ebavõrdses olukorras. Ebavõrdsus seisneb selles, et andmesubjektil puudub reeglina võimalus konkreetse mobiilirakenduse teenusetingimuste osas läbi rääkida. Ehkki andmekaitse üldmääruse kohaselt ei loetaks liiga üldist või nn kobarnõusolekuna võetud nõusolekut kehtivaks, siis vastutav töötleja ei pruugi enda poolt aktiivselt midagi muuta enne, kui on toimunud rikkumine ning andmesubjekt on esitanud selle kohta kaebuse järelevalveasutusele.

Läbipaistvuse põhimõtte järgimine on oluline ka näiteks veebireklaamide puhul, mida kolmandad osapooled kasutavad, sest tehnoloogia keerukuse tõttu on andmesubjektil raske teada saada ja mõista, kes andmeid kogub, mis eesmärgil ja kellele võidakse andmeid omakorda edastada. Tihtipeale sätestavad pankade või muude kontsernide üldtingimused

137 Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 62.
138 Andmekaitse üldmääruse selgituspunkt 32.

võimaluse edastada andmesubjekti isikuandmed samasse kontserni kuuluvatele ettevõtetele. Lisaks lubavad paljud tingimused edastada andmeid ka koostööpartneritele. Kui kontserni kuuluvate ettevõtjate koosseisu kindlakstegemine on andmesubjektil teoreetilisel veel võimalik, siis koostööpartneritega muutub isikute ring sisuliselt määramatuks ning sellisel juhul ei ole autori hinnangul andmekaitse üldmääruses toodud läbipaistvuse nõue isikuandmete vastuvõtjate osas täidetud (artiklid 13 (1) e) ja 14 (1) e)).

Problemaatiline on ka olukord, kus andmesubjektile jäetakse vajalik teave üldse esitamata. Näiteks Ühendkuningriikides tegi National Health Service (edaspidi NHS) koostööd Googlega tehisintellekti arendamisega ning NHS-st liikusid välja ka nende isikute andmed, kes ei olnud andnud nõusolekut oma andmete jagamiseks väljaspool tervishoiuteenuse osutamist.[139] Sellest tulenevalt on oht, et kui isegi tervishoiuteenuse pakkujad ei töötle andmeid seaduslikult ja läbipaistvalt, siis mille alusel peaks andmesubjekt usaldama suvalist kolmandat osapoolt.

2.7. Terviseandmete töötlemine õigusliku aluse ära langemisel

Andmekaitse üldmääruse kohaselt peab vastutav töötleja kustutama kõik isiku andmed pärast seda kui õiguslik alus andmete töötlemiseks on ära langenud (artikkel 17 (1) b)). Nõusolekuteenuse kasutuselevõtuga võib tekkida olukord, kus pole kolmandale osapoolele selge kas andmesubjekti tegelik tahe oli nõusolek edasiseks töötlemiseks tagasi võtta või mitte. Näiteks juhul, kui andmesubjekt on nõusolekuteenuse kaudu võtnud enda nõusoleku tagasi, et edaspidi andmekogust tema terviseandmeid enam kolmandale osapoolele ei saadetaks, kuid ei tee sama teenusepakkuja juures, sest õiguslikult on andmesubjekt andnud kaks nõusolekut. Ühe riikliku andmekogu vastutavale töötlejale terviseandmete edastamiseks ning teise konkreetsele kolmandale osapoolele terviseandmete töötlemiseks konkreetse terviseandmeid vajava teenuse osutamiseks. Juhul kui andmesubjekt jätkab kolmanda osapoole teenuse kasutamist ja see on võimalik ilma pidevalt uuenevate andmeteta, siis on selge, et kehtiv nõusolek edasiseks andmetöötluseks on olemas. Probleemne olukord tekib siis, kui andmesubjekt on nõusolekuteenuse kaudu antud nõusoleku andmete edastamiseks tagasi võtnud ja sisuliselt lõpetab ka teenusepakkuja teenuse kasutamise. Näiteks isik kustutab

139 Hodson, H. Revealed: Google AI has access to huge haul of NHS patient data. - NewScientist. 26.01.2016. Kättesaadav: https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-haul-of-nhs-patient-data/ (28.04.2021).

mobiilirakenduse, kuid ei taju, et üksnes rakenduse kustutamisega ei kustutata enamasti sellega seotud kasutajakontot. Selle vältimiseks tuleks kolmandal osapoolel teenusetingimustega sätestada, et kui inimene pole pika aja jooksul teenust kasutanud, siis töötlemine lõpetatakse.[140] Vastasel juhul jääb kolmandal osapoolel õigus inimese isikuandmeid, sh terviseandmeid edasi töödelda, sest ta ei ole oma nõusolekut konkreetselt tagasi võtnud.

Siiski tekib sellises olukorras küsimus, kas andmesubjekti tegelik tahe rakenduse kustutamisel võis sisaldada ka soovi nõusolek terviseandmete töötlemiseks tagasi võtta? Andmekaitse üldmääruse artikli 7 (3) kohaselt lõppeb nõusolek selle tagasivõtmisega. Andmekaitse üldmäärus aga ei sätesta mis on nõusoleku kehtivuse pikkuseks muudel juhtudel. Arvestades töötlemise eesmärgi piirangut saab eeldada, et sõltuvalt kontekstist võib nõusolek ka aja jooksul kehtetuks muutuda.[141] Selle hindamiseks on vajalik kaaluda nõusoleku esialgset ulatust ning andmesubjekti ootuseid. Kui kolmanda osapoole töötlemise eesmärgid muutuvad ning täienevad, siis ei pruugi varasemalt antud nõusolek enam kehtiv olla. Kolmas osapool vastutava töötlejana ei tohiks eeldada nõusoleku olemasolu sellest, et andmesubjekt ei ole kasutanud oma õigust esitada vastuväidet või esitanud AKI-le kaebust.

Käsitletud riski realiseerumise tõenäosust suurendab autori hinnangul ka andmesubjektide informeerituse tase oma õigustest ja kohustustest seoses andmetöötlusega. St andmesubjektid võivad jätta teenusepakkujale antud nõusoleku tagasivõtmata üksnes teadmatuse tõttu ning sellega seotud riski tuleks hinnata pigem suureks.

2.8. Terviseandmete edastamine madalama andmekaitse tasemega riiki

Terviseandmete edastamisel kolmandatesse riikidesse võib juhtuda, et vastutav töötleja ei kontrolli milline on sealne andmekaitse tase ning edastab andmeid riiki, milles ei tagata euroopa inimestele samaväärset andmekaitse taset kui andmekaitse üldmäärusega on ette

140 Pärgmäe, R. jt. Õiguse ja eetika töörühma raport 2015, lk 29.

141 Information Commissioner's Office. Consultation: GDPR consent guidance. - ICO, 02 March 2017-31 March 2017, lk 25. Kättesaadav: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf (28.04.2021).

nähtud. Kolmas osapool peab vastutava töötlejana hindama kas ja milliseid isikuandmeid, sh tervisega seotud andmeid kolmandatesse riikidesse edastatakse. Üldjuhul tähendab see seda, et kolmandatesse riikidesse võib terviseandmeid edastada juhul kui, on rakendatud nõuetekohaseid lisakaitsemeetmeid (andmekaitse üldmääruse artiklid 46-49) ja selleks on olemas kohane õiguslik alus (andmekaitse üldmääruse artikkel 9). Erandkorras võib järgida samu reegleid, mis kehtivad Euroopa Liidu siseselt, kuid seda üksnes juhul kui andmete edastamine toimub riikidesse, mille kohta Euroopa Komisjon on andnud andmekaitsetaseme piisavuse otsuse.[142] Käesoleva töö kirjutamise hetkel on Euroopa Komisjon tunnistanud Andorra, Argentiina, Kanada, Fääri saarte, Guernsey saare, Iisraeli, Mani saare, Jaapani, Jersey erihalduskonna, Uus-Meremaa, Šveitsi ja Uruguay Idavabariigi andmekaitsetaseme piisavalt tugevaks ning seega saab öelda, et seal on euroopa inimestele tagatud andmekaitse üldmääruse kohaselt samaväärne tase.[143] Lõuna-Korea ning Ühendkuningriigi osas on hetkel veel menetlus käimas. Ülejäänud riikide osas, mis jäävad Euroopa Liidust väljapoole tuleb vastutaval töötlejal endal rakendada piisavaid turvameetmeid ning tagada andmekaitse üldmääruses toodud eesmärke. See aga ei pruugi olla alati võimalik. Näiteks USA puhul on leitud, et USA ei taga andmekaitse üldmäärusega samaväärset kaitsetaset. Seda on põhjalikult analüüsitud kahes Euroopa Kohtu lahendis: *Schrems I*[144] ja *Schrems II.*[145] Kohtuasja aluseks oli Austria kodaniku M. Schremsi kaebus, et Facebook edastab tema isikuandmeid kas täielikult või osaliselt Facebook Inc. serveritesse, mis asuvad USA territooriumil ning palus sellise andmetöötluse lõpetada, sest USA kehtiv õigus ja valitsev praktika ei taga isikuandmeid sealsete avaliku võimu asutuste juurdepääsu eest. Peamiseks probleemiks leiti olevat see, et USA ametiasutustel on ligipääs Euroopast USA-sse liikuvale andmevahetusele ning Euroopa ettevõtetel puudub sisuliselt võimalus seda takistada. Seetõttu tunnistas Euroopa Liidu kohus 2020. a juulis Euroopa Komisjoni otsuse isikuandmete kaitse piisavuse kohta Euroopa Liidu ja USA andmekaitseraamistiku *Privacy Shield* osas kehtetuks.[146] Edaspidiseks on EDPB andnud juhised, et see kas isikuandmeid võib standardsete andmekaitse tüüptingimuste (*Standard Contractual Clauses*) alusel kolmandatesse riikidesse edastada sõltub andmekaitsealasest mõjuhinnangust.[147] Kui selle tulemusel selgub, et

142 Euroopa Komisjoni andmekaitse taseme piisavuse otsused. Kättesaadav: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_et (28.04.2021).
143 Samas.
144 EKo C-362/14, *Maximillian Schrems versus Data Protection Commissioner,* ECLI:EU:C:2015:650
145 EKo C-311/18, *Data Protection Commissioner* versus *Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559
146 EKo C-311/18.
147 Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. 24.07.2020, lk 3. https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_et.pdf

täiendavate meetmete kasutusele võtmisel ei ole võimalik andmekaitse üldmäärusest toodud kaitsemeetmeid suudeta tagada, andmesubjekti võimalus saada kohtulikku kaitset asjaomases riigis või töötlemiseesmärgi piirang, siis tuleb andmetöötlus lõpetada.[148]

Käesolevas peatükis toodud riskiga kaasneb ka andmesubjekti enda vastutustundetu käitumine. Nimelt on AKI ühes oma varasemas juhises toonud välja, et andmesubjektid on tihtipeale liiga usinad uut toodet proovima ning annavad kergekäeliselt oma „jah" sõna kõigele, mida teenusepakkuja isikuandmete või nende töötlemise osas küsib.[149] Selle tagajärjeks võib olla see, et andmesubjekt ei teagi oma andmete edastamisest kolmandatele osapooltele, kes asuvad madalama andmekaitsetasemega riigis.

2.9. Terviseandmete edastamise ja sellele järgneva töötlemise kontekstis andmete usaldusväärsuse ja konfidentsiaalsuse tagamine

Terviseandmete edastamise ja säilitamisega seotud risk seisneb peamiselt selles, et ebapiisava turvalisuse tõttu võivad saada terviseandmetele ligi isikud, kellel puudub selleks õiguslik alus ning kelle eesmärk on saada illegaalselt omandatud andmetest majanduslikku kasu, tekitades sellega andmesubjektile varalist või mittevaralist kahju. Andmekaitse üldmääruse artikli 25 kohaselt peab vastutav töötleja rakendama lõimitud andmekaitset ja tema vastutab andmetöötluse piisavate tehniliste või korralduslikke meetmete rakendamise eest. Ehk kolmas osapool peab tagama terviseandmete töötlemisel asjakohase turvalisuse, sh kaitsma neid loata või ebaseadusliku töötlemise ning juhusliku kaotamise, hävitamise või kahjustumise eest (artikkel 5 (1) f)). Tehniliste ja korralduslike meetmete valikul tuleks vastutaval töötlejal võtta arvesse teaduse ja tehnoloogia viimast arengut ning selle rakendamise kulusid (andmekaitse üldmääruse artikkel 32 (1)). Arvesse tuleb võtta ka spetsiifiliselt terviseandmete töötlemisest tulenevaid ohte,[150] kuna terviseandmeid võidakse kasutada mitmesuguste süütegude toimepanemiseks. Kõige kahjulikumaks neist võib pidada stsenaariume, kus kasutatakse ebaseaduslikult raske haiguse või surmaga lõppeva haiguse üksikasju või pannakse toime

(28.04.2021)

148 Samas, lk 3.

149 Andmekaitse Inspektsioon. Kantavad seadmed ja privaatsus. Juhis organisatsioonidele ja kodukasutajale seaduse rakendamisel. 09.11.2015, lk 5. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/juhis-kantavad_seadmed_ja_privaatsus.pdf (28.04.2021).

150 Andmekaitse üldmääruse selgituspunkt 83.

pikaajaline identiteedivargus.[151]

Info raske haiguse või surmaga lõppeva haiguse kohta, samuti vaimse tervise kohta on väga tundlik ning seda infot võidakse kasutada väljapressimiseks. Näiteks Soome psühhoteraapiakeskuse Vastaamo andmebaasist on kahel korral lekkinud suurel hulgal soomlaste terviseandmeid: 2020. aastal saadi ligipääs 40 000 patsiendi isikuandmetele ning 2021 jaanuaris saadi kätte ligi 32 000 soomlase vaimse tervise informatsioon. Infot kasutati hiljem isikutelt raha väljapressimiseks.[152]

Identiteedivarguse toimepanemiseks kasutatakse erinevaid vahendeid, alates dokumendi võltsimisest kuni kirurgilise sekkumiseni, kuid toimingute eesmärk jääb samaks - isik presenteerib end teadlikult teise isikuna.[153] Õiguskirjanduses on leitud, et identiteedivargusega tekitatud kahju on eelkõige seotud isiku põhiõiguste ja vabaduste rikkumisega.[154] Töö autori hinnangul tuleks terviseandmetega seotud identiteedivarguse potentsiaali ning sellega seotud tagajärgi lugeda suuremaks ohuks kui muude isikuandmete puhul, kuna terviseandmeid ei saa muuta ja seetõttu võib identiteedivargusel olla väga pikaajalised tagajärjed.

Kuni 2009. aastani ei olnud Eesti karistusseadustikus (edaspidi KarS) eraldiseisvat identiteedivarguse koosseisu ning see oli probleem, sest kelmuse koosseis (KarS § 209) hõlmab küll teisele isikule tegelikest asjaoludest väärkujutluse tekitamise, kuid koosseis näeb ette ka varalise kasu saamise, mida identiteedivarguse puhul ei pruugi alati esineda. Alates 2009 lisati KarS-i § 157^2, millega kriminaliseeriti teise isiku identiteedi ebaseaduslik kasutamine (nn identiteedivargus). Täpsemalt karistatakse selle sättega teise isiku identiteeti puudutavate andmete nõusolekuta edastamise, juurdepääsu võimaldamise või nende kasutamise eest eesmärgiga luua teise isikuna esinemise teel temast teadlikult ebaõige ettekujutus, kui sellega on tekitatud kahju teise isiku seadusega kaitstud õigustele või huvidele või sooviga varjata kuritegu. Teoorias eristatakse kolme kategooriat juhtumeid kui isik esineb teise isikuna: 1) kasutatakse teise andmesubjekti andmeid, 2) kasutatakse surnud isiku

151 Steger, A. What happens to stolen Healthcare Data? HealthTech magazine. 30.10.2019. Kättesaadav: https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (28.04.2021).
152 Soomlaste vaimse tervise andmed lekkisid taas internetti. 27.01.2021. Kättesaadav: https://eestinen.fi/2021/01/soomlaste-vaimse-tervise-andmed-lekkisid-taas-netti/ (28.04.2021).
153 Nõmper, A., Tikk, E. Informatsioon ja õigus, Juura 2007, lk 184.
154 Nimmo, M., Identiteedivarguse piiritlemine solvamisest ja laimamisest Eesti õigussüsteemis. - Juridica 10/2017, lk 717.

andmeid või 3) kasutatakse väljamõeldud ehk fiktiivse isiku andmeid.[155] KarS-i kohaselt on reguleeritud neist kaks esimest. Andmekaitse mõttes omab suuremat olulisust esimene olukord ehk kannatanu, kelle identiteeti on nõusolekuta kasutatud. Andmekaitse üldmäärust surnud isiku andmetele ei kohaldata, kuid siseriiklikult on Eesti reguleerinud ka surnud isikute andmete kasutamine (IKS § 9).

Eestis registreeriti aastatel 2009–2017 teise isiku identiteedi ebaseadusliku kasutamisega seonduvate juhtumite tõttu kokku 808 kuriteoteadet. Kui 2009. aastal registreeriti 0 kuriteoteadet ja 2010. aastal 55 kuriteoteadet, siis 2017. aastal oli see number juba 131.[156] 2020. aasta esimese 5 kuu jooksul registreeriti teise isiku identiteedi ebaseadusliku kasutamisega seonduvaid juhtumeid kokku 92, millest üle poole (49 tk) registreeriti eriolukorra perioodi jooksul.[157] See näitab, et identiteedivargusega seotud kuritegude registreerimiste arv on jätkuvalt kasvavas trendis. Sama trendi võib märgata ka mujal maailmas.[158,159] Samas peab arvestama, et ühtset statistikat on siin võimatu teha, kuna rahvusvahelises praktikas puudub ühtne arusaam identiteedivarguse olemusest ning mõistest. Kasutusel on nii identiteedikuritegu (*identity crime*), identiteedipettus (*identity fraud*) kui ka identiteedivargus (*identity theft*).[160]

Õiguskirjandusest ja raportitest võib lugeda mitmeid identiteedivarguse juhtumeid. USA-s on need eelkõige seotud sotsiaalkindlustusnumbriga (*social security number - SSN*), et taotleda ohvri nimel laenu või sooritada mõni muu kuritegu, mis jääb seotuks ohvri SSN-iga ning ohvri karistusregistri väljavõttega.[161] M. Gercke toob oma küberkuritegude aruteludokumendis välja veel, et identiteedivarguste toimepanijad on väga huvitatud

155 Karistusseadustiku eelnõu seletuskiri, SE 530, 11.06.2009, lk 5. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/2b386832-b657-ab0c-fb52-de02708302bc/Karistusseadustiku%20muutmise%20seadus (28.04.2021).

156 Kuritegevus Eestis 2017. Kriminaalpoliitika uuringud. Justiitsministeerium. Tallinn 2017, lk 144. Kättesaadav: https://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevuseestis_2017_veebi01.pdf (28.04.2021).

157 Registreeritud kuriteod jaanuar-mai 2016-2020. Baromeeter. Justiitsministeeriumi kriminaalpoliitika osakonna võrgukodu. Kättesaadav: https://www.kriminaalpoliitika.ee/et/statistika-ja-uuringud/kuritegevuse-baromeeter (28.04.2021).

158 Karistusseadustiku eelnõu seletuskiri, lk 4.

159 FTC. Medical Identity theft. January 2011. https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (28.04.2021).

160 Karistusseadustiku eelnõu seletuskiri, lk 10.

161 Gercke, M. Internet-related identity theft. A discussion paper. Project on Cybercrime. Council of Europe. 22.11.2007, lk 7. Kättesaadav: https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/internet-related-identity-theft%E2%80%93a-discussion-paper.pdf (28.04.2021).

erinevatest allikatest saadaoleva info ühildamisest.[162] Ka Martin, Y.-S. ja del Alamo, J. M rõhutavad oma artiklis, et teenusepakkujad, kes koondavad erinevat andmesubjektide kohta käivat infot, sh mainet kahjustavat infot on problemaatilised.[163] Seega praegune globaalne trend e-äris, mis võimaldab eri sotsiaalmeedia kontosid omavahel ühildada ning tervise- ning elustiili mobiilirakendusi omavahel ühildada aitab andmete agregeerimisele kaasa, lihtsustades küberkuritegude toimepanemist.

Seoses 2020. aastal alanud Covid-19 kriisiga on arendatud või arendusjärgus mitmed mobiilirakendused, et hoida viirust kontrolli all või võimaldada vabamat liikumist neil, kes on viiruse läbi põdenud, vaktsiini teinud või saanud negatiivse testi. Kõige selle taustal on ülemaailmselt teavitatud mitmetest küberrünnakutest andmebaasidesse, mis sisaldavad andmesubjektide terviseandmeid. Sealhulgas saadi Terviseameti andmebaasist kätte üle 9 000 inimese eriliigilisi isikuandmed, mis sisaldasid infot koroonahaigete ning nende lähikondsete kohta.[164] Samuti juba eelnevalt mainitud Vastaamo andmebaasi andmeleke, kust saadi kahel aastal, sh 2021. aasta jaanuaris ligi 32 000 patsiendi vaimse tervisega seotud infot. RIA küberturvalisuse aastaraamatus 2021 tuuakse välja, et 2020. aastal toimus küberruumis rekordarv küberintsidente, mille kaudu üritati mh saada isikuandmeid.[165] See näitab selgelt, et terviseandmete edastamisse kolmandatele osapooltele ei saa suhtuda kergekäeliselt, sest isegi riigiasutused, kus on kehtestatud kõrgendatud turbenõuded ei ole neis olukordades alati kaitstud ning sarnaseid rünnakuid võib oodata ka edaspidi.

Kui andmesubjekt annab nõusolekuteenuse kaudu riikliku andmekogu vastutavale töötlejale oma nõusoleku, et viimane edastaks tema terviseandmed kolmandale osapoolele, siis liiguvad terviseandmed turvaliselt riiklikult arendatud X-tee kaudu.[166] Riiklikele asutustele, sh andmekogudele ja ühiskonna toimimise seiskohast oluliste võrgu- ja infosüsteemide pidamisele (näiteks pangad või tervishoiuteenuseid pakkuvad erakliinikud) on

162 Samas, lk 7.
163 Gutwirth, S., Leenes, R. De Hert, P. Data Protection on the Move: Current developments in ICT and Privacy/ Data Protection. Springer 2016, lk 253.
164 Riigi vastu toimusid küberründed, kätte saadi 9158 koroonapatsiendi andmed. 01.12.2020. Kättesaadav: https://www.err.ee/1192309/riigi-vastu-toimusid-kuberrunded-katte-saadi-9158-koroonapatsiendi-andmed (28.04.2021).
165 Küberturvalisuse aastaraamat 2021. Riigi Infosüsteemi Amet, lk 8. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2021.pdf (28.04.2021).
166 Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021, lk 61.

küberturvalisuse seadusega (edaspidi KüTS)[167] nähtud ette võrgu- ja infosüsteemide nõuded, vastutus ja järelevalve. Näiteks tervise infosüsteemi põhimääruse[168] §2[2] kohaselt on tervise infosüsteemile määratud spetsiifiline turbeaste. Erasektorile selliseid nõudeid pole ette kirjutatud, v.a KüTS-is toodud erandid. Suurettevõtted, kellel on piisavalt rahalist ressurssi, saavad võtta endale ISO (*International Organization for Standardization*) kohustused. Nõusolekuteenuse esimesed potentsiaalsed teenusepakkujad on pigem (idu)ettevõtted, kellel sellist võimalust ei pruugi olla ja mille tõttu on küberturvalisusega seotud oht pigem suur.

Infosüsteemide andmevahetuskihi määruse (edaspidi X-tee määrus)[169] §12 (1) punktis 1 on sätestatud, et andmeteenuse kasutamiseks sõlmitakse X-tee liikmete vahel andmeteenuse kokkulepe. Selles lepitakse muu hulgas kokku andmeteenuse kasutamiseks vajalikud infoturbemeetmed ning andmeteenuse kasutaja alamsüsteemilt nõutavad organisatsioonilised, füüsilised ja infotehnilised turvameetmed, arvestades töödeldavate andmete koosseisu ning õigusaktidega ettenähtud nõudeid. See tähendab, et terviseandmete vastuvõtmiseks X-tee kaudu peab kolmas osapool rakendama andmeteenuse kokkuleppes toodud turvanõudeid, kuid selle lepinguga ei ole sätestatud tingimusi andmetöötlusele, mis toimub pärast terviseandmete edastust. Seega edasise töötlemise osas jääb terviseandmete turvalisuse tase suuresti vastutava töötleja enda määrata. Siiski, võttes arvesse andmekaitse üldmääruse artiklitest 5 (1) f), 25 ja 32 tulenevaid nõudeid, milleks on muu hulgas isikuandmete pseudonümiseerimine ja krüpteerimine.

AKI aastaraamatu kohaselt suurenes 2019. aastal andmekaitse rikkumistest teatajate arv võrreldes 2018. aastaga, sh kasvas rikkumisteadete kuupõhine koguarv 16% võrra. Arvestades AKI-le esitatavaid märgukirju eeldab AKI, et kõik intsidendid ei ole nendeni jõudnud ning suure tõenäosusega on tegelikkuses isikuandmete intsidente rohkem.[170] Samuti rõhutatakse, et üldine teadmine andmekaitsest ei ole kahjuks jõudnud veel tasemele, kus võiks igas olukorras end teenusesaajatena turvaliselt tunda.[171]

167 Küberturvalisuse seadus. - RT I, 22.05.2018, 1.
168 Tervise infosüsteemi põhimäärus. - RT I, 06.12.2016, 11...RT I, 26.02.2021, 31.
169 Infosüsteemide andmevahetuskiht, määrus. RT I, 06.08.2019, 17 … RT I, 06.08.2019, 6.
170 Andmekaitse Inspektsiooni aastaraamat. 2019. Kättesaadav: https://aastaraamat.aki.ee/aastaraamat-2019-aastast-peadirektori-pilgu-labi/millised-olid-rikkumised-ja-nende-pohjused (28.04.2021).
171 Samas.

Samas ei ole andmete turvalisuse tagamata jätmine ainuke põhjus, sest identiteedivargust soodustab ka andmesubjektide endi vähene teadlikkus ning hooletu suhtumine oma isikuandmetesse.[172] Näiteks on andmesubjektid valmis jagama enda terviseandmeid tundmatutele kolmandatele osapooltele tumeveebis, et osta negatiivse tulemusega koroonatesti sertifikaat või vaktsineerimistõend.[173] Kui andmesubjekt laeb alla kolmanda osapoole mobiilirakenduse, kus on tema terviseandmed, siis on ka tema kohustus hoolitseda oma isikustatud turvaelementide eest. Ehkki ka siin ei sõltu alati kõik andmesubjekti hoolsusest. 2020 tuvastati Eestis ligi 20 turvanõrkusega veebilehte, mis ei kontrollinud ID-kaardiga autentimisel kaardi sertifikaadi kehtivust, sealhulgas kas sertifikaat on SK ID Solutionsi poolt allkirjastatud. Praktikas tähendanuks see seda, et teenuse kasutaja saanuks logida neisse teenustesse sisse ükskõik kelle nime või isikukoodiga. Ühel juhul oli tegemist ka kiirlaenu pakkuva ettevõttega, mis tähendab, et kolmas isik võinuks andmesubjekti nimel võtta laenu.[174]

Seega, on äärmiselt oluline, et kõik kolmandad osapooled, kes saavad nõusolekuteenuse kaudu terviseandmeid, rakendavad andmelekke või muu küberintsidendi vältimiseks asjakohaseid ning piisavaid turvameetmeid. Kui kolmas osapool, kellele on riigi andmebaasist edastatud andmesubjekti nõusolekul konkreetne andmekomplekt terviseandmeid, ei ole investeerinud turvavõimekusse, siis tekitatakse sellega juurde üks nö nõrk lüli terviseandmete turvalisuse tagamises.

172 Nõmper, A., Tikk, E. Informatsioon ja õigus, Juura 2007, lk 184.
173 Tumeveebis tehakse äri võltsitud vaktsineerimistõenditega. Postimees. 26.03.2021. Kättesaadav: https://tervis.postimees.ee/7211071/tumeveebis-tehakse-ari-voltsitud-vaktsineerimistoenditega (28.04.2021).
174 Küberturvalisuse aastaraamat 2021. Riigi Infosüsteemi Amet, lk 11. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2021.pdf (28.04.2021).

3. KEHTIVAD TERVISEANDMETE EDASTAMISEGA SEOTUD PIIRANGUD JA VÕIMALIKUD TÄIENDAVAD PIIRANGUD MAANDAMAKS 2. PEATÜKIS KÄSITLETUD NÕUSOLEKUTEENUSEGA KAASUVAID ANDMEKAITSEÕIGUSLIKKE RISKE

3.1. Andmekaitse üldmäärusest tulenevad piirangud

Isikuandmete kaitse on muutumas ajas järjest tähtsamaks, sest tänapäeval on suur enamus andmeid digitaliseeritud, mis tähendab, et andmeid töödeldakse automatiseeritult ning võimalused eraelu ründamiseks võrreldes esimeste andmekaitsega seotud õigusaktide vastuvõtmisest on kasvanud tohutult.[175] Eriliigilised isikuandmed, sealhulgas terviseandmete töötlemine vajab tugevamat kaitset, kuna nende töötlemisel võib olla andmesubjektidele märkimisväärne kahjulik mõju diskrimineerimise oht.[176] Käesoleva töö 2. peatükis on toodud välja valik näiteid olukordadest, mis juba praegu on eraõiguslike juriidiliste isikute poolt andmetöötluses probleemseks osutunud või ohud, mis võivad realiseeruda konkreetselt nõusolekuteenuse kaudu andmete edastamise tagajärjel. Põhjuseid võib olla erinevaid: kolmas osapool ei taga terviseandmetele samaväärset turvalisuse taset kui on riiklikes andmekogudes terviseandmetele konkreetses andmekogus ette nähtud või kolmas osapool töötleb andmeid algsest erineval eesmärgil ilma õigusliku aluseta jne.

Eelnevast tulenevalt on selge, et vajadus terviseandmete kaitseks on suur ning seetõttu on andmekaitse üldmääruses sätestatud terviseandmete töötlemisele hulk piiranguid. Andmekaitse üldmääruse artiklis 9 (1) sätestatud normi eesmärgiks on piirata täielikult igasugust eriliigiliste andmete töötlemist ning lõike 2 kohaselt nähakse ette erandjuhud, millal on töötlemine lubatud. Kui 1981-1995 aastatel loeti andmekaitse konventsiooni kohaselt isikuandmete töötlemiseks üksnes nende automatiseeritud töötlemist, siis alates andmekaitse direktiivi ja ka kehtiva andmekaitse üldmääruse artikli 4 punkti 2 kohaselt loetakse

175 Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. - Juridica 2002 nr VII, lk 435.
176 Andmekaitse üldmääruse selgituspunkt 53.

isikuandmete töötlemiseks nii automatiseeritud kui ka automatiseerimata toimingut või toimingute kogumit. Selliseks toiminguks võib olla andmete kogumine, korrastamine, säilitamine, lugemine, kasutamine, edastamine, kustutamine jne. Seega loeb andmekaitse üldmäärus iga isikuandmetega tehtavat toimingut töötlemiseks ning üldjuhul on eriliigiliste, sh terviseandmete töötlemine keelatud (artikkel 9 (1)). Igal liikmesriigil on võimalik andmekaitse üldmääruse artikli 9 (4) kohaselt säilitada või kehtestada terviseandmete töötlemiseks täiendavad tingimused ja piirangud. Lisaks üldisele andmekaitse üldmääruse artiklist 9 tulenevale terviseandmete töötlemispiirangule sh õiguslikule alusele kohalduvad spetsiifilised piirangud järgmistes olukordades: 1) terviseandmete ulatuslik töötlemine vajab andmekaitse mõjuhinnangut, 2) andmesubjektile tuleb anda kogu andmekaitse üldmääruses toodud info, 3) andmete töötlemist võib viia läbi üksnes selliselt, et oleks tagatud nende usaldusväärsus – ja konfidentsiaalsus, 4) terviseandmete töötlemisel nõusoleku alusel tuleb võtta nõusolek iga eesmärgi suhtes eraldi ning rakendada eesmärgipärasuse testi[177] ja 5) andmete edastamisel kolmandatesse riikidesse tuleb üldjuhul täita täiendavaid nõudmisi.

Andmekaitse üldmääruse artiklist 35 (1) tulenevalt peab kolmas osapool vastutava töötlejana viima läbi andmekaitsealase mõjuhinnangu kui isikuandmete töötlemise laadi, ulatust konteksti ja eesmärke arvesse võttes tekib tõenäoliselt andmesubjektide õigustele ja vabadustele suur oht. Lisaks täpsustab sama artikli lõige 3, et mõjuhinnang on kohustuslik kui kui toimub eriliigiliste andmete töötlemine ja see on ulatuslik. Mõjuhinnangu sisu on sisuliselt riskihinnang, mille kohaselt peaks kolmas osapool tuvastama ja arvestama võimalikke ohtudega, mis puudutavad andmesubjekti huve, sh käesoleva töö 2. peatükis kirjeldatud riskidega (artikkel 35 (7)). Enne töötlemise alustamist tuleb hinnata vähemalt:

1) kavandatud isikuandmete, sh terviseandmete töötlemise toimingute ja töötlemise eesmärkide, süstemaatiline kirjeldus;

2) isikuandmete, sh terviseandmete töötlemise toimingute vajalikkuse ja proportsionaalsuse hindamine eesmärkide suhtes;

3) töötlemistoimingute ja eesmärkidega seonduvalt anda hinnang andmesubjektide õigusi ja vabadusi puudutavatele ohtudele, ning

4) kirjeldada ohtude käsitlemiseks kavandatud meetmed, sealhulgas tagatised, turvameetmed ja mehhanismid isikuandmete kaitse tagamiseks ning andmekaitse üldmääruse

177 Käsitletud lähemalt töö esimeses peatükis, vt punkt 1.3.

järgimise tõendamiseks, võttes arvesse andmesubjektide ja teiste asjaomaste isikute õigusi ja õigustatud huve.

Piiranguks tuleks lugeda ka seda, et enne kui kolmas osapool võib hakata andmesubjekti terviseandmeid töötlema peab ta teavitama inimest nii sellest, kes on tema andmete suhtes vastutav töötleja, mis eesmärgil andmeid töödeldakse, info, et nõusoleku saab alati tagasi võtta kui ka see kas andmeid edastatakse kolmandatesse riikidesse. Täpsemalt on nimetatud kohustused sätestatud andmekaitse üldmääruse artiklites 12-15 ja nendega seotud riske kajastatud käesoleva töö alapeatükis 2.6. Sätete eesmärk on tagada andmetöötluse läbipaistvus ning suurendada andmesubjekti kontrolli omaandmete üle.

Euroopa Majanduspiirkonnas peab kolmas osapool vastutava töötlejana jälgima, et terviseandmete edastamisel oma volitatud töötlejatele või muudele isikutele, kui selleks on õiguslik alus, ta rakendab andmekaitse üldmääruses toodud isikuandmete töötlemise üldpõhimõtteid, millest üks on usaldusväärsus ning konfidentsiaalsus (artikkel 5 (1) f). Selle põhimõtte eesmärk on tagada sisuliselt edastatavate andmete turvalisus, kaitsta loata või ebaseadusliku töötlemise eest, samuti juhusliku hävimise või kahjustumise eest. Sisuliselt peaks antud põhimõtte efektiivne rakendamine maandama riske nagu läbipaistmatuse suurenemine (p 2.6), õigusliku aluse ära langemine (p 2.7) ning identiteedivarguse, andmelekke või muude küberintsidentide esinemine (p 2.9). Täpsemalt on sisustatud seda põhimõtet andmekaitse üldmääruse artiklites 25 ja 32. Artikkel 25 näeb ette lõimitud ja vaikimisi andmekaitse (*privacy by design and by default*) rakendamist mis peaks tagama usaldusväärsuse ja konfidentsiaalsuse põhimõtte efektiivse rakendamise. Lõimitud andmekaitse meetmetega tagatakse eelkõige see, et vastutav töötleja ei tohi teha isikuandmeid vaikimisi ilma asjaomase isiku sekkumiseta määramata füüsiliste isikute ringile kättesaadavaks. See on ka üks riskidest, mis võib nõusolekuteenuse kasutuselevõtuga veelgi eskaleeruda (vt punktis 2.6 läbipaistmatus). Artiklis 32 täpsustatakse konkreetseid meetmeid, mida vastutav töötleja peab arvestama. Näiteks tuleks vastutaval töötlejal võtta kasutusele erinevad tehnoloogilised ja organisatoorsed lahendid, mille valimisel tuleks arvestada kõige uuemaid tehnoloogilisi lahendusi, seejuures on aga valikuvõimalus jäetud vastutava töötlejale lähenedes valiku langetamisel nö täida või põhjenda põhimõtet.

Lisaks eelnevalt toodud piirangutele tuleb terviseandmete edastamisel kolmandatesse riikidesse täita täiendavad andmekaitse üldmääruse V peatükist tulenevaid nõudeid. Erandina võib järgida samu reegleid, mis kehtivad Euroopa Liidu siseselt, kui riigi kohta, kuhu edastatakse on Euroopa Komisjon võtnud vastu andmekaitsetaseme piisavuse otsuse. Muul juhul võib kolmandatesse riikidesse edastada andmeid üksnes siis, kui andmekaitse üldmääruses toodud tingimused on täidetud[178] ja rakendatakse piisavaid kaitsemeetmeid, et tagada andmekaitse üldmääruses toodud eesmärke. See on vajalik selleks, et andmesubjektil võib kolmandas riigis olla raskem oma õigusi kaitsta, eelkõige võimalusi kaitsta oma isikuandmete ebaseadusliku kasutamise ning avaldamise eest.[179] Täpsemalt nähakse andmekaitse üldmääruse artiklis 46 (2) b) võimalus kasutada siduvaid kontsernisiseseid eeskirju või rakendada artiklis 46 (2) c)- d) nimetatud Euroopa Komisjoni poolt vastu võetud või AKI poolt vastuvõetud ja Euroopa Komisjoni poolt heaks kiidetud standardseid andmekaitseklausleid.

3.2. Olemasolevate piirangute piisavus terviseandmete edastamise ja edasise töötlemise kontekstis

Andmekaitsealastes õigusaktides isikuandmete töötlemisele, sh konkreetsemalt terviseandmete töötlemisele kehtestatud piirangute eesmärk on anda andmetöötlejatele rikkumiste vältimiseks nö tegutsemisraamid ja juhised ja samal ajal üksikisikule kindlus, et ta võib oma andmed volitatud töötlejale usaldada. Seega selleks, et hinnata kas terviseandmete edastamise ja edasise töötlemise kontekstis on kehtivas õiguses sätestatud piirangud piisavad pole oluline analüüsida mitte üksnes terviseandmete edastamisele kui kitsalt ühele töötlemistoimingule seatud piirangu või täiendavate tingimuste seadmine, vaid vaadata edastamise konteksti laiemalt. Konkreetselt andmete edastamine hõlmab endas turvariske, aga isegi kui isoleeritult selle protsessi juures ei saa andmesubjekti õigused rikutud, siis võib see juhtuda hiljem. Kui terviseandmete edastamine toimub andmesubjekti nõusoleku alusel riiklikust andmekogust, siis on oluline hinnata edastamisega kaasnevat töötlemisprotsessi tervikuna ehk kas ja milmääral toodud piirangud aitavad vältida käesoleva töö 2. peatükis käsitletud riskide realiseerumist.

178 Andmekaitse üldmääruse selgituspunkt 115.
179 Andmekaitse üldmääruse selgituspunkt 116.

Enne terviseandmete edastamise kontekstis kohalduvate piirangute piisavuse hindamist on oluline rõhutada hetkel Eestis esinevat praktilist probleemi andmekaitse üldmäärusest tulenevate karistuste määramise osas. Enne andmekaitse üldmääruse jõustumist kardeti hiigeltrahve ning rahvusvahelisel tasemel on mõned neist ka realiseerunud.[180] Näiteks Prantsusmaa andmekaitse inspektsioon määras ettevõttele Google LLC 50 miljonit trahvi muuhulgas seetõttu, et ettevõtte poolt kogutavad andmesubjekti nõusolekud ei olnud konkreetsed ja üheselt mõistetavad.[181] Austria andmekaitse inspektsioon määras Austria postiteenuse pakkujale 18 miljonit trahvi, kuna ettevõte müüs ilma õigusliku aluseta profileeritud isikuandmeid mitmetele ettevõtetele ja erakondadele.[182] Sama ei saa öelda aga Eesti kohta. Isikuandmete kaitse seaduse 6. peatükis (§§ 62-70) sätestatud rikkumiste eest võib karistuseks määrata 10-20 miljonit eurot või kuni 4% ettevõtte eelmise majandusaasta ülemaailmsest aastasest kogukäibest, kuid Eesti praktikas jäävad hoolimata sellest karistusummad piinlikult väikeseks.[183] Peamine põhjus seisneb selles, et isikuandmete kaitse seaduse 6. peatükis sätestatud rikkumised on sätestatud süütegudena ning menetletakse väärteomenetluses.[184] Andmekaitse üldmääruses sätestatud trahvide ülemmäärad ulatuvad aga kümnetesse miljonitesse ning ületavad oluliselt väärtegude eest kohaldatavate rahatrahvide ülemmäärasid.[185] Eelnimetatud asjaolu on äramainitud ka andmekaitse üldmääruse selgituspunktis 151 ning rõhutatud, et hoolimata sellest peaksid määratavad trahvid olema tõhusad, proportsionaalsed ja heidutavad.[186] Seetõttu tuleb nentida, et isegi kui andmekaitse üldmääruses toodud piirangud on teoreetiliselt piisavad, siis sellest üksi ei piisa, sest paraku ei ole kõik turuosalised õiguskuulekad. Järelvalveorganil peab olema reaalne võimalus ja võimekus kontrollida kas nõudeid täidetakse ning kui ei, siis rakendada efektiivselt

180 Peep, V. Kas isikuandmete kaitse üldmäärus toob tõesti kaasa hiigeltrahvid? 15.11.2017. Kättesaadav: https://www.aki.ee/et/uudised/kas-isikuandmete-kaitse-uldmaarus-toob-toesti-kaasa-hiigeltrahvid (28.04.2021).

181 The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. 21.01.2019. Kättesaadav: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (28.04.2021).

182 Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG (Austrian Postal Service), 23.10.2019. Kättesaadav: https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_en (28.04.2021).

183 Vt täiendavalt: Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr 2.1.-6/20/31, 07.10.2020, ja Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr 2.1.-6/20/27, 07.08.2020, ja Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr 2.1.-6/20/21, 08.05.2020. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).

184 Haldustrahvimenetluse seaduse eelnõu seletuskiri. 19.08.2020, lk 5. Kättesaadav: https://eelnoud.valitsus.ee/main#8JNeIBvd (28.04.2021).

185 Vastavalt karistusseadustiku §-le 47 võib füüsilisele isikule määrata väärteo eest trahvi kuni 1200 eurot ja juriidilisele isikule kuni 400 000 eurot.

186 Andmekaitse üldmääruse selgituspunkt 151.

sunnimehhanismi. St meedet, mis juhib isiku tähelepanu eksimusele (karistab) ja samal ajal hoiab ära uute rikkumiste toimepanemise ühiskonnas laiemalt (preventatiivne).[187] Eelmainitud probleemi lahendamiseks koostas Justiitsministeerium haldustrahviõiguse kontseptsiooni,[188] mis on käesoleva töö kirjutamise hetkel seaduse eelnõu faasis. Haldustrahvimenetluse seaduse jõustumisel on võimalik määrata isikuandmetega seotud rikkumiste eest trahve, mis on andmekaitse üldmääruse kohaselt ette nähtud ning teha seda kiiremini ja väiksema menetlusliku koormusega võrreldes senise olukorraga. Edasisel analüüsil on lähtutud eeldusest, et Euroopa Liidu õiguses ettenähtud rahaliste karistuste ülevõtmiseks mõeldud haldussanktsiooni liik – haldustrahv – on Eesti õiguskorda üle võetud.

Kuidas saab andmesubjekt olla kindel, et ettevõte x täidab andmekaitse nõudeid pidevalt ehk igal ajahetkel. Andmesubjektile töötlemistoimingute seaduspärasuse ja läbipaistvuse tagamine oli uue isikuandmete kaitse regulatsiooni väljatöötamise ettepaneku kohaselt andmekaitse üldmääruse üks eesmärke.[189] Samas tekib küsimus, kas see eesmärk on realiseerunud ja kui mitte, siis kas käesoleva töö teises peatükis toodud riske on üldse võimalik täielikult maandada, st mis hetkel võib öelda, et piirangud on piisavad?

Punkti 2.2. kohaselt on peamiseks probleemiks see, et ettevõtted nagu kindlustusandjad või krediidiandjad võivad hakata seadma terviseandmete edastamist nõusolekuteenuse kaudu üheks lepingu sõlmimise eeltingimuseks ning muuhulgas siduma seda näiteks madalamate hindadega. Kuna eelnimetatud riski osas on sisuliselt küsitav kas krediidiandja või kindlustusandja võiks iga laenu või kindlustuslepingu puhul üldse nõusolekut kasutada terviseandmete töötlemiseks, siis aitab esmajoones nimetatud riski maandada andmekaitse üldmääruse artiklist 7 (4) tulenev vajalikkuse hinnang. Käesoleva töö autori hinnangul ei ole see risk piisavalt maandatud eelkõige seetõttu, et tegemist on suuresti tõlgendusliku küsimusega ning lepingu ja nõusoleku olemusliku vastuolu tõttu. Eelkõige eriliigiliste andmete töötlemisel, kus puudub võimalus kasutada õigusliku alusena andmekaitse üldmääruse artiklis 6 (1) b) toodud sätet, kuna neile kohaldub erisäte artiklist 9. Siiski, nagu

187 Haldustrahvimenetluse seaduse eelnõu seletuskiri. 19.08.2020, lk 10.
188 Haldustrahviõiguse kontseptsioon. 05.05.2020. Kättesaadav: https://eelnoud.valitsus.ee/main#VZU4bXWV (28.04.2021).
189 Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu Määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus). Brüssel: 2012, lk 4. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52012PC0011&from=ET (28.04.2021).

varasemalt selgitatud, siis autori hinnangul ei pruugi olla võimalik käsitleda krediidivõimelisuse hindamiseks või kindlustusriski hindamiseks antavad nõusolekut põhiteenusega olemuslikult niivõrd seotuna, et ilma selleta pole võimalik teenust osutada. Kui nii, siis ei saa öelda, et terviseandmete töötlemine on tingimata vajalik ning ei saa jaatada nõusoleku lubatavust andmekaitse üldmääruse artikli 7(4) järgi. Arvestades nõusoleku õiguslikult problemaatilist konstruktsiooni seoses eriliigiliste andmete töötlemisega lepingu kontekstis, siis autori hinnangul ei aita riski maandada see, kui keelata nimetatud ettevõtetel nõusolekuteenusega liitumine. Kuna probleem eksisteerib ka praegu, siis aitaks riski maandada avalik ja aktiivne teavitustöö AKI poolt ning ka see, et andmesubjektid ise oleksid aktiivsed oma õigusi kaitsma pöördudes järelevalve poole.

Punkti 2.3 kohaselt on probleemiks kogutud terviseandmete, sh profileeritud kasutaja andmete müük andmemaakleritele ja seda ilma andmesubjekti nõusolekuta. Samuti see, et küsitakse nn kobarnõusolekuid või liiga üldiseid nõusolekuid, mis sisuliselt hõlmavad ka muid varjatud eesmärke peale müügi, mille kohta andmesubjekt ei saanud osanud nõusolekut andes aru saada. Terviseandmete töötlemise kuritarvitust esialgsest töötlemiseesmärgist erineval eesmärgil aitab esmalt tagada andmekaitse üldmääruse artiklist 7 tulenev tingimus, et iga eesmärgi kohta tuleb terviseandmete puhul võtta eraldiseisev nõusolek. Selle eelduseks on aga see, et vastutav töötleja teab milliseid töötlemistoiminguid ta teeb. Selleks tuleks koostada nn töötlemistoimingu ülevaade, mille nõue tuleneb andmekaitse üldmääruse artiklitest 30 ja 39. Kui kolmandad osapooled ausalt järgiksid kõiki andmekaitse üldmääruses toodud reegleid nõusoleku kohta, st selliselt et iga eesmärgi kohta on eraldiseisev nõusolek ning andmesubjektil on seetõttu reaalne võimalus valida, siis oleks kolmandal osapoolel kehtiv õiguslik alus. Probleemiks on aga see, et praktika kohaselt on isikuandmete töötlemine, sh terviseandmete töötlemine ilma õigusliku aluseta muutumas järjest enam probleemiks ning järelevalve ei jõua pidada tehnoloogia arenguga sammu.

Punkti 2.4 kohaselt on peamiseks probleemiks see, et kolmas osapool kes saab nõusolekuteenuse kaudu andmesubjekti terviseandmed ei rakenda kas üldse või ei rakenda piisavalt anonüümimistehnikaid ning seetõttu võib anonüümitud andmestiku müümise asemel müüa tegelikkuses andmestikku, millest on üksikisik tuvastatav. Terviseandmete anonüümimise kohta puudub ajakohane juhis ning alus: millal ja kuidas peavad kolmandad

osapooled rakendama anonüümimistehnikaid. Andmekaitse töörühma soovituse kohaselt ei tuleks andmete anonüümimisel kasutada mitte üksnes ühte anonüümimise meetodit, vaid kombinatsiooni mitmest erinevast tehnikast, et tagada piisav turvalisus ning vähendada andmesubjektide taasidentifitseerimise võimalikkust.[190] Muuhulgas peaks vastutav töötleja anonüümimismeetodi valikul hindama tehnika sobivust järgmiste kriteeriumite alusel: 1) kas on võimalik isik välja selgitada; 2) kas on siiski võimalik omavahel siduda ühe ja sama isiku andmeid; 3) kas on võimalik tuletada teavet konkreetse isiku kohta.[191] Töö autori hinnangul ei ole privaatsustehnoloogia ebapiisavusega seotud risk piisavalt maandatud. Eelnevalt viidatud andmekaitse töörühma juhend anonüümimistehnika kasutamisest on küll olemas aastast 2014, kuid tehnoloogia on viimase 7 aastaga palju edasi arenenud, mistõttu ei pruugi see kõiki olulisi detaile arvestada. Ühtlasi on Andmekaitse töörühma kritiseeritud puudulikus arusaamises anonüümimisega seotud probleemidest. On leitud, et konkreetsed anonüümimismeetodid pole kõige olulisemad, vaid pigem on oluline jälgida kui suur on andmemaht, mida soovitakse anonüümida.[192] Teisest küljest leitakse, et ka andmestiku massiivsus mõjutab küll anonüümimise efektiivsust ja on väga oluline, aga selleks et tagada efektiivset anonüümimise protsessi tuleb ka korrektseid anonüümimistehnikaid rakendada.[193] Andmekaitse üldmääruses seevastu on käsitletud anonüümimist väga põgusalt – öeldes üksnes seda millal ei tuleks andmeid enam isikuandmetena käsitleda.[194] Autori hinnangul ei ole see piisavalt selge juhis turuosalistele maandamaks punktis 2.4 käsitletud riski. On vajalik konkreetseid ja selgeid rakendavaid juhiseid, mida (idu)ettevõte peab minimaalselt tegema ja milliseid privaatsustehnoloogiaid eelistatult rakendama, et andmesubjektidele ei tekiks ettevõtte poolt puudulikult rakendatavate anonüümimistehnikate tõttu kahju.

Punkti 2.5 kohaselt on riskiks see, et kolmanda osapoole poolt pakutavat terviseandmetel põhinevat teenust soovivad kasutama hakata alaealised, kuid ilma vanemliku nõusolekuta ei ole alaealistel võimalik kehtivat nõusolekut oma terviseandmete töötlemiseks anda. Samuti ei tohiks kolmas osapool võimaldada oma teenust kasutada siis, kui alaealine saab teenust

190 Artikli 29 alusel asutatud andmekaitse töörühma arvamus anonüümimistehnikate kohta, lk 4.
191 Samas, lk 3.
192 Korff, D. New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments . European Commission DG Justice, Freedom and Security Report. 15.01.2010, lk 48. Kättesaadav: https://ssrn.com/abstract=1638949 (28.04.2021).
193 Hon, W. K., Millard, C., Walden, I., The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1 (March 10, 2011). International Data Privacy Law (2011) 1 (4): 211-228, Queen Mary School of Law Legal Studies Research Paper No. 75/2011, lk 22. Kättesaadav: https://ssrn.com/abstract=1783577 (28.04.2021).
194 Andmekaitse üldmääruse selgituspunkt 26.

kasutada nii, et sisestab andmeid ise manuaalselt ja ilma, et veenduks lapse vanuses või tagaks tehnoloogiliste vahenditega seadusliku esindaja poolt nõusoleku andmise. Autori hinnangul annab seda riski efektiivselt maandada sellega, et nõusoleku teenuse kaudu tuvastatakse läbi ID-kaarti, mobiil-id või smart-id konkreetse isiku vanus. Samuti peaksid kolmandad osapooled kasutama pelgalt märkeruutu täitmise asemel rakendama andmesubjektide tugeva autentimise nõudeid ehk juba nimetatud ID-kaarti, mobiil-id või smart-id lahendust, kus on võimalik isikukoodist lihtsalt tuvastada andmesubjekti vanus. Selle rakendamine võimaldaks teenusepakkujatel olla kindel, et teenuse kasutaja on täisealine.

Punkti 2.6 kohaselt on riskiks see, et kolmas osapool ei taga terviseandmete töötlemisel läbipaistvuse põhimõtet. Näiteks annab andmesubjektile eesmärgi deklaratsiooni kaudu ühte infot oma edasiste töötlemiseesmärkide kohta ja tegelikult küsib mobiilirakenduses näiteks kobarnõusolekut või hoopis vastuolus eesmärkidega, mida oli edastanud nõusolekuteenusesse. Seda aitab andmekaitse üldmääruse kohaselt tagada see, et kolmas osapool annab andmesubjektile tõest ja selget teavet oma töötlemiseesmärkide kohta ning täidab nõusolekule seatud tingimusi (artikkel 7 (3)). Samuti on läbipaistvuse osas suureks probleemiks see, et andmesubjekt ei tea kui palju ja kellele tema andmeid tegelikult edastatakse. Enamus vastutavaid töötlejaid ei kajasta ka oma kodulehel infot, et kellele ning mis eesmärkidel andmeid edastatakse. Sisuliselt võib olla andmesubjektil võimatu teha kindlaks teha kes võivad olla potentsiaalsed vastuvõtjad tema terviseandmetele. Andmekaitse üldmääruse artikli 25 kohaselt aitaks seda tagada lõimitud ja vaikimisi andmekaitse rakendamine. Nende meetmetega tagatakse eelkõige see, et isikuandmeid ei tehta vaikimisi ilma asjaomase isiku sekkumiseta määramata füüsiliste isikute ringile kättesaadavaks. Üks võimalus läbipaistvust tagada on ka isikuandmete töötlemisülevaate koostamine. Töö autori hinnangul on läbipaistvuse põhimõte seotud väga mitmete tingimuste järgimisega ning kui kolmas osapool ei ole endale koostanud töötlemistoimingute ülevaadet, siis on oht, et tal puudub igasugune arusaam enda poolt tehtavatest töötlemistoimingutest, nende eesmärkidest ja õiguslikest alustest. Lisaks on probleem sellest, üldmääruse artikkel 30, millest tuleneb töötlemistoimingute ülevaate kohustus on ebaõnnestunud sõnastusega selles osas, et ei saa täpselt aru kellele see kohustus on suunatud. Sama artikli lõige 5 loob esmalt väära mulje, nagu kehtiks see vaid andmetöötlejatele, kellel on 250 ja enam töötajat.[195] Tegelikult on aga öeldud, et säte töötlemis ülevaate peavad koostama kõik, kelle andmetöötlus ei ole juhuslik.

195 Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend, lk 20.

Kui aga ettevõttel, kes töötleb nõusolekuteenuse kaudu saadud terviseandmeid on vähemalt üks töötaja või vähemalt üks füüsilisest isikust klient, siis ei saa väita, et andmete töötlemine on juhuslik. Lisaks sätestab artikli 30 lg 5, et töötlemisülevaade tuleb teha, kui töödeldakse eriliigi isikuandmeid ning kui andmetöötlus kujutab tõenäolist ohtu. Seega nõusolekuteenuse kaudu terviseandmeid saavate ettevõtete puhul peaks sellise ülevaate koostamine olema kohustuslik. Töötlemisülevaate koostamine tegelik kasutegur maandamismeetmena ei pruugi aga olla piisav, sest kui AKI ei jõua omaalgatuslikke menetlusi algatada, vaid jõuab tegeleda üksnes sissetulevate kaebustega ja teabenõuetega, siis ei ole tegelik olukord turul efektiivselt tagatud. Esiteks esineb ettevõtteid kes ei teagi, et tal on kohustus koostada töötlemisülevaade või siis ei saa juba eelnevalt mainitud ebaõnnestunud andmekaitse üldmääruse artikli 30 sõnastuse tõttu aru, et nõue kohaldub ka temale. Euroopa Liidu Põhiõiguste Agentuuri poolt 2019. aastal läbiviidud uuringu kohaselt (edaspidi FRA) leidsid 77% vastanutest, et neil oli andmekaitse üldmääruse rakendamisega probleeme, see nõudis keskmist või väga suurt pingutust.[196] Teiseks seepärast, et järelevalve omal initsiatiivil kontrollima tuleku tõenäosus on statistikat vaadates äärmiselt väike ja seega üritab (idu)ettevõte tulla toime minimaalse võimaliku ressursi kuluga. FRA uuringus toodi küsitletute poolt ressurssi vähesus üheks põhjuseks, miks andmekaitse üldmäärusest tulenevaid nõudeid ei suudeta rakendada.[197]

Punkti 2.7 kohaselt on peamiseks riskiks see, et andmesubjektide informeerituse tase oma õigustest ja kohustustest seoses andmetöötlusega on madal, kuigi Justiitsministeeriumi poolt tellitud aruande kohaselt hindavad nooremad inimesed oma teadlikkust pigem heaks.[198] Kuigi, võib öelda, et andmekaitse üldmääruse rakendamise järgselt on teadlikkus tõusnud,[199,200] siis see ei ole veel piisav ning selle tõttu on üheks probleemiks ka andmesubjekti hooletus oma andmetega ringikäimisel. Uuringu kohaselt on iga kolmas elanik arvamusel, et mure isikuandmete kaitstuse pärast on ületähtsustatud ja, et nad ei muretse enda andmete pärast,

196 The General Data Protection Regulation – one year on Civil society: awareness, opportunities and challenges. European Union Agency for Fundamental Rights, 2019, lk 2. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-gdpr-one-year-on_en.pdf (28.04.2021).

197 Samas, lk 6.

198 Inimeste privaatsusõigused ja isikuandmete kaitsmine 2020. uuringuaruanne. Kantar Emor. September-oktoober 2020, lk 10. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/uuringud/privaatsusoigused_ja_isikuandmete_kaitsmine_2020_aruanne.pdf (28.04.2021).

199 European Union Agency for Fundamental Rights (FRA) (2020), Your rights matter: Data protection and privacy, Fundamental Rights Survey. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf (28.04.2021).

200 Andmekaitseinspektsioon. Avaliku teabe seaduse täitmisest ja isikuandmete kaitse tagamisest aastal 2018. Soovitused aastaks 2019, lk 43. Kättesaadav: https://issuu.com/andmekaitse/docs/aastaraamat_2018_kohta._soovitused_ (28.04.2021).

kuna neil pole midagi varjata.[201] Andmesubjekti teadmatuse ja hooletuse tõttu võib juhtuda, et andmesubjekt võtab riikliku andmekogu vastutavale töötlejale antud nõusoleku tagasi arvates ekslikult, et sellega lõppeb andmetöötlus automaatselt ka kolmanda osapoole poolt, kuigi tegelikkuses ei ole ta kolmandale osapoolele antud nõusolekut tagasi võtnud. Andmekaitse üldmääruse kohaselt aitab seda vältida kolmanda osapoole poolt väga selge kommunikatsioon andmesubjekti võimalusest nõusolek tagasi võtta (artikkel 13 (2) c) ja 14 (2) d)). Üksnes see ei maanda aga seda riski piisavalt, sest kui nõusolek antakse nö muuseas ja süveneta mille kohta täpselt nõusolek antakse, siis pole teavitusest enne nõusoleku andmist kasu. Küll aga ei ole selle jaoks tingimata vajalik täiendavaid piiranguid seada. Vastavalt Andmekaitse Inspektsiooni põhimääruse (edaspidi AKI põhimäärus) §-le 9 punktile 1 on AKI üheks põhiülesandeks teavitus- ja ennetustöö korraldamine ning käesoleva töö autori hinnangul tuleks antud probleemi lahendada peaasjalikult intensiivsema teavitustööga selliselt, et info jõuab sihtrühmani. Üksnes AKI kodulehele üleslaetud info ei ole kindlasti piisav, et öelda teavitustööd on piisavalt tehtud.

Punkti 2.8 kohaselt on peamiseks riskiks see, et terviseandmeid võidakse edastada madalama andmekaitse tasemega riiki. Novembris 2020 esitas EDPB uued lepingu tüüptingimuste ja standardsete andmekaitseklauslite eelnõud, mis asendavad olemasolevad rahvusvahelise andmeedastuse andmekaitseklausleid.[202] Pärast Euroopa Liidu Kohtu otsust Schrems II[203] osas tuli standardsed andmekaitseklauslid ajakohastada, et viia need kooskõlla andmekaitse üldmääruse nõuetega ja Schrems II väljatoodud nõuetega, kuna standardsed andmekaitseklauslid või siduvad kontsernisisesed eeskirjad ei taganud seni piisaval tasemel kaitsemeetmeid.[204] Uued Euroopa ülesed lepingu tüüptingimused tagaksid parema ühtlustamise ja õiguskindluse.[205] EDPB ja EDPS ühisarvamuses 1/2012 on leitud, et piisavaks

201 Inimeste privaatsusõigused ja isikuandmete kaitsmine 2020. uuringuaruanne. Kantar Emor, lk 47.

202 Euroopa Andmekaitsenõukogu – täiskogu 42. istungjärk. 20.11.2020. Kättesaadav: https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en%C2%A0_et (28.04.2021).

203 EKo C-311/18, *Data Protection Commissioner* versus *Facebook Ireland Ltd, Maximillian Schrems*, ECLI:EU:C:2020:559

204 Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*. 24.07.2020, lk 5. https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_et.pdf (28.04.2021)

205 Euroopa Andmekaitsenõukogu ja Euroopa Andmekaitseinspektori ühisarvamus 1/2021, milles käsitletakse Euroopa Komisjoni rakendusotsust vastutavate töötlejate ja volitatud töötlejate vaheliste lepingute tüüptingimuste kohta määruse (EL) 2016/679 artikli 28 lõikes 7 ja määruse (EL) 2018/1725 artikli 29 lõikes 7 osutatud küsimustes. EDPB, lk 6. Kättesaadav: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_et (28.04.2021).

ei tohiks pidada näiteks selliseid tingimusi, milles pelgalt korratakse andmekaitse üldmääruse artikli 28 (3) ja (4) toodud sätteid, vaid tuleks selgitada kuidas neid sätteid täidetakse.[206] Ühtlasi on tehtud mitmeid muid ettepanekuid, kuna EDPB ja EDPS-i hinnangul ei ole praeguse eelnõu kohaselt veel piisavad ning jätavad liiga palju tõlgendusruumi. See on oluline seetõttu, et need tüüptingimused kolmandatesse riikidesse andmete saatmisel kujutavad endast tagatisi, mis peavad kaitsma andmesubjekte ja maandama konkreetseid andmekaitse aluspõhimõtetega seonduvaid riske.[207] Arvestades seda, et kõige suurem probleem andmete edastamisega kolmandatesse riikidesse on seotud USA-ga ja kolmandad osapooled paratamatult soovivad oma teenuseid reklaamida Facebookis või kasutades mõnda muud USA-s servereid omava ettevõtte poolt, siis on see kindlasti probleem, mis ei ole hetkel andmekaitse üldmäärusest tulenevate piirangute osas piisavalt kaetud. Kui kolmandad osapooled saadavad andmeid kolmandatesse riikidesse, mille osas on võetud vastu Euroopa Komisjoni poolt andmekaitsetaseme piisavuse otsus, siis selles osas on risk maandatud. Ehk hetkel ei ole alust pidada andmete edastamisega seotud riske nende kolmandate riikide osas kõrgemaks kui mujale Euroopa Majanduspiirkonda edastamisel. Lisaks on käesoleva töö punktis 2.8 toodud välja, et andmesubjektid on tihtipeale liiga usinad uut toodet proovima ning annavad kergekäeliselt oma „jah" sõna kõigele, mida teenusepakkuja küsib ning ei süvene muuhulgas näiteks võimalusse, et tema andmetele võib olla ligipääs USA ametiasutustel. Töö autori hinnangul ei ole reaalne, et Eesti keelaks ära nõusolekuteenuse kaudu terviseandmeid saavatel ettevõtetel reklaami kasutamise, mille tõttu liigub andmestik USA serveritest läbi, aga seda riski on võimalik maandada intentsiivsema teavitustööga järelevalve asutuse poolt, mis suunaks inimesi siiski teenusetingimusi lugema.

Punkti 2.9 kohaselt on peamiseks riskiks erinevad turvalisusega seotud rikkumised. Nagu eelnevalt mainitud, siis andmekaitse üldmäärus võimaldab vastutaval töötlejal valida ise organisatoorsed ja tehnilised lahendused arvestades teaduse ja tehnoloogia uusimaid arenguid ja rakendamise kulusid, kuid ka isikuandmete töötlemise laadi, ulatust, konteksti ja eesmärke, samuti erineva tõenäosuse ja suurusega ohte füüsiliste isikute õigustele ja vabadustele. Eestis on toodud üheks heaks privaatsustehnoloogia näiteks Sharemind'i lahendust,[208] mis on ehitatud üles selliselt, et osapooli ei saa de-idenfitseerida, sh ükski osapool ei tea millised

206 Samas, lk 6.
207 Samas, lk 6.
208 Bogdanov, D., Siil, T. (2018a). Anonymisation 2.0: Sharemind as a Tool for De-Identifying Personal Data – Part 1: Definitions. Cybernetica. 17.08.2018.Kättesaadav: https://sharemind.cyber.ee/anonymisation-2_0-part-1-definitions/ (28.04.2021).

andmed täpselt keegi sisestas ega võimalda tuletada seda töötluse tulemusel saadud vastusest.[209] Sharemind tehnoloogia võimaldaks süsteemi kasutajatel ühendada tundlikke andmekomplekte nagu terviseandmed ilma, et peaks usaldama kedagi kolmandat andmeid ühildama.[210] Teiseks uudseks privaatsustehnoloogia lahenduseks võib pidada plokiahela kasutamist ettevõtte andmehaldussüsteemides,[211] kuid hetkel veel õiguslikult põhjalikult analüüsimata. Teaduskirjandusest võib leida arutelusid, et plokiahela tehnoloogia rakendamine võimaldaks tagada efektiivsemalt andmekaitse üldmäärusest tulenevaid nõudeid.[212] Euroopa Parlamendile koostatud uuringuraportis on leitud, et plokiahela kasutamine võib pakkuda küll selgeid eeliseid teatud andmekaitse üldmäärusest tulenevate vastavusnõuete täitmisel, kuid on rõhutatud, et enne seda on tarvilik jõuda selgusele kuidas andmekaitse üldmäärust plokiahela tehnoloogia valguses tõlgendada.[213] Esmapilgul tekib üksjagu õiguslikke küsitavusi näiteks hajusraamatu kasutamine vastutavate töötlejate kontekstis või kuidas on tagatud nn õigus olla unustatud põhimõte, samuti plokiahela tehnoloogia vastavus andmekaitse üldmääruses toodud põhimõtetele nagu minimaalsus, eesmärgi piirang ning läbipaistvus.[214] Siiski on tegemist ühe uusima lahendusega millel võib olla potentsiaali lahendada vastutavale töötlejale teatud andmekaitsega seotud probleemid, kuid iga uusim lahendus toob kaasa kulud. (Idu)ettevõtetel ei pruugi olla piisavalt ressursse ning seetõttu on oht, et valitakse odavamalt ülalpeetavaid IT lahendusi[215] ning täidetakse üksnes seadusest tulenevaid minimaalseid nõudeid. Punktis 2.2 nimetatud krediidiandjate ja kindlustusandjate puhul võiks pidada turvalisusega nimetatud riskid piisavalt maandatuks, sest lisaks andmekaitse üldmäärusele kehtivad neile täiendavad KüTS-st tulenevad nõuded võrgu- ja infosüsteemide kohta. Küll aga võivad (idu)ettevõtted põhjendada näiteks, et kõige

209 Riigikogu toimetised. - Riigikogu kantselei väljaanne, RiTo 42/2020, lk 115. Kättesaadav: https://rito.riigikogu.ee/wordpress/wp-content/uploads/2020/12/RiTo_42.pdf (28.04.2021).

210 Spindler, G., Schmechel, P. Personal Data and Encryption in the European General Data Protection Regulation, punkt 2.2.3.4.

211 Banerjee, A., Joshi, K.P. Link before you share: Managing privacy policies through blockchain. 2017 IEEE International Conference on Big Data (Big Data), 2017, pp. 4438-4447. Kättesaadav: https://www.researchgate.net/publication/320357405_Link_Before_You_Share_Managing_Privacy_Policies_through_Blockchain (28.04.2021).

212 Truong, N.B etc. GDPR - Compliant Personal Data Management: A Blockchain-based Solution. IEEE transaction on information forensics and security, 03.10.2019, lk 14. Kättesaadav: https://arxiv.org/pdf/1904.03038.pdf (28.04.2021).

213 European Parliament. Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? Study Panel for the Future of Science and Technology. European Parliamentary Research Service. July 2019, p 7. Kättesaadav: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (28.04.2021).

214 Samas, lk 6.

215 Oprysk, L. The Forthcoming General Data Protection Regulation in the EU: Higher Compliance Costs Might Slow Down Small and Medium-sized Enterprises' Adoption of Infrastructure as a Service. - Juridica International. Law Review. University of Tartu, 24/2016. lk 23.

uuemad tehnilised lahendused on liiga kulukad rakendada ja kasutavad vanemaid või odavamaid lahendusi ja samas teades, et varasemad või odavamad lahendused pole terviseandmete töötlemise tundlikkust arvestades piisavad. Kas AKI-l on sellises olukorras piisav alus piiramaks ajutiselt (IKS § 56 lg 3 p 7) või keelamaks (IKS § 56 lg 3 p 5) ettevõttel eriliigiliste andmete töötlemine öeldes, et võtke kasutusele uuem või kallim tehnoloogia, kuna praegu ei ole turvalisusega seotud riskid maandatud. Siinjuures arvestades, et ettevõttele, kelle kogu majandustegevus põhinebki nõusolekuteenuse kaudu saadavate terviseandmete alusel teenuse pakkumises, võib see tähendada tegevuse lõpetamist. Ehk sisuliselt öeldaks - kui ettevõttel pole ressurssi terviseandmete turvaliseks töötlemiseks, siis ei ole neil ressurssi ka tundlike andmete töötlemist hõlmavat tegevusala valida. Objektiivselt võttes tuleb nõustuda, et andmekaitse üldmääruse artikli 32 tegelik eesmärk ongi seda tagada. Ehkki sõnastuse järgi on ettevõttel kaalutlusruumi, siis tegelik eesmärk on isikuandmetele adekvaatse kaitse tagamine ja kui seda ei suuda, siis ei tohiks andmete töötlemine lubatud olla.[216] Turvalisuse põhimõtet aitab tagada mainitud andmekaitse üldmääruse artikkel 32, kuid kuid autori hinnangul jääb siin kolmandale osapoolele liiga suur tõlgendamise võimalus. Teatav proportsionaalsus usaldusväärsuse ja konfidentsiaalsus põhimõte tagamiseks vajalike meetmete rakendamiseks on mõistetav ja vajalik. Kuna nõusolekuteenuse kaudu hakkavad riigi poolt sunduslikult kogutud terviseandmed liikuma erasektorisse hetkel ilma täiendavate nõueteta, siis peaks käesoleva töö autori hinnangul riik tagama, et nõusolekuteenusega liituvad ettevõtted saaksid info ja teabe vähemalt minimaalsete nõudete kohta, mida rakendada. Seda ka põhjusel, et nooremad inimesed ei tunne piisavalt ohtu andmetöötlusrikkumiste osas „meil pole midagi varjata." See on koht, kus riigil peaks olema õigus ja vajadus inimest oma informatsioonilise enesemääramisõiguse realiseerimisel piirata[217] ja seda tehnoloogiliste arendustega kaasnevate isikuandmete töötlemisega seotud ohtude tõttu.[218]

Eelnevalt on toodud välja ühe andmekaitse üldmäärusest tuleneva piiranguna ka andmekaitsealane mõjuhinnang. Üheks oluliseks faktoriks mõjuhinnangu kohustuslikkuse juures on see, kas töötlemise ulatus on ulatuslik või mitte. Ulatuslikkuse kohta ei ole toodud

216 Arvestades siiski mõistlikkuse põhimõtet, sest absoluutset kaitset potentsiaalsete ennustamatute küberintsidentide vastu on kiire tehnoloogiaarengu tõttu pigem võimatu tagada.

217 Andmesubjekti piiramiseks võiks antud juhul käsitleda seda, et mõne teenuse puhul ei ole võimalik inimesel nõusolekut nõusolekuteenuse kaudu anda, kuna ettevõtel pole piisavalt ressurssi, et andmekaitse üldmäärusest tulenevaid ja siseriiklikult seatud täiendavaid piiranguid adekvaatselt täita.

218 Alexy, R. Põhiõigused Eesti põhiseaduses.

välja ühest numbrit ja see on tõlgenduslik, kuid autori hinnangul tuleks antud juhul lähtuda ulatuslikkuse hindamisel näiteks sellest kui suurele hulgale teenust pakutakse. Kui pakutakse teenust määramata isikute ringile, siis on vähemalt töötlemise tuleviku eesmärk ulatuslik. Kas andmekaitse üldmääruse artiklis 35 on öeldud, et tuleks arvestada kavandatavate töötlemistoimingute mõju. Seega tuleks arvestada terviklikult kogu planeeritavat tegevust. Kui ettevõtte äriplaan näeb ette, et sihtturg on kogu Eesti täisealine elanikkond, mida planeeritakse x perioodi jooksul hõlmata ning töödeldakse eriliigilisi isikuandmeid, siis tuleks jaatada mõjuhinnangu kohustuslikkust. Hetkel on see hindamine jäetud konkreetse vastutava töötleja kätte ning ressursi kokkuhoiu mõttes jätta mõjuhinnang tegemata. Andmekaitse üldmääruse artikli 35 (4) kohaselt peab järelevalve koostama ja avalikustama selliste isikuandmete töötlemise toimingute tüüpide loetelu, mille suhtes kohaldatakse lõike 1 kohast nõuet teha andmekaitsealane mõjuhinnang. Hetkel ei ole seda Eesti poolt teadaolevalt tehtud, aga töö autori hinnangul oleks see nõusolekuteenusest tulenevate turvalisuse riskide maandamiseks hädavajalik, et teenust osutavad ettevõtjad teaksid väga selgelt enda kohustusi.

Üheks põhjuseks miks andmekaitse üldmääruses sätestatud piirangud ei ole efektiivsed on autori hinnangul põhjus, et ettevõtjad suhtuvad andmekaitsesse leigelt ning ei pea rikkumist liiga suureks probleemiks. Teiseks põhjuseks on hetkel nõrk järelevalve. AKI-l on andmekaitse üldmääruse artiklist 57 ja täiendavalt IKS § 56 tulenevalt üsna suur tegutsemisvõimalus isikuandmete kaitsel, kuid praktikas ei ole järelevalve efektiivne. Seda juba eelnimetatud põhjustel andmekaitse üldmäärusest tulenevate trahvide rakendamise võimaluse osas, mida peaks oluliselt parendama haldustrahviseaduse vastuvõtmine. Kuid teine ja autori hinnangul suurem põhjus on selles, et järelevalveasutusel on väga palju ülesandeid, ressursse nende kõigi täitmiseks aga vähe.[219] Sellele probleemile on korduvalt tähelepanu juhitud[220] ning käesoleva töö autori hinnangul ei ole pea 10 aasta jooksul olukord selles osas suurt paranenud. AKI hindas enne andmekaitse üldmääruse jõustumist, et nende töökoormus hüppab üles eelkõige uue andmekaitseõiguse rakendamise eel ning sellele järgnevalt.[221] Töökoormusega toimetulekuks on planeeriti vähendada ajutiselt omaalgatusliku järelevalvetöö mahtu.[222] Kui aastal 2015 algatati 384 omaalgatuslikku järelevalve asja, 2016 algatati 86 ja 2017 algatati 149, siis 2018 langes omaalgatuslike järelevalvete maht 15 peale

219 Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. - Juridica 2002 nr VII, lk 445.
220 Samas.
221 Isikuandmete kaitse seaduse eelnõu seletuskiri. SE 679. 22.08.2018, lk 71. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5c9f8086-b465-4067-841e-41e7df3b95af (28.04.2021).
222 Isikuandmete kaitse seaduse eelnõu seletuskiri, lk 71.

ning 2019 aastal tõusis marginaalselt 29 peale. Samal ajal võib näha, et kaebuste, vaiete ja väärteoteadete maht kasvas ka pärast 2018. aastat.[223] Seletuskirjas on viidatud, et omaalgatuslikku järelevalvet vähendatakse ajutiselt. Sellest võiks arvate, et loodeti teabenõuete vähenemist mõni aeg pärast uue andmekaitse üldmääruse rakendamist. Autori hinnangul ei ole see realiseerunud ning statistika kohaselt on kaebuste arv jätkuvalt väga suur, samuti selgitustaotluste ja märgukirjade peale kuluv maht (2017 .a 1520 tk ja 2019.a 2343 tk).[224] Kontrollkäike aga ei jõutud 2019. aastal mitte ühtegi teha, mis on võrreldes varasemate aastatega suur erinevus: 2017. a 45 kontrollkäiku ja 2018. a 17 kontrollkäiku.[225] Seega võib öelda, et kui AKI töömaht oli juba enne andmekaitse üldmäärust suur, siis pärast seda tõusis veelgi ning trendi kohaselt on rikkumiste arv kasvavas trendis. Seetõttu võib öelda, et arvestades üksikuid erandeid ei ole praegused meetmed piisavad tagamaks nõusolekuteenuse kaudu erasektorisse edastatavate terviseandmete turvalisust ja andmekaitse üldmäärusest tulenevate nõuete järgimist.

Seega autori hinnangul ei ole nõusolekuteenuse kaudu terviseandmete edastamisel riiklikest andmebaasidest kolmandatele osapooltele kõikide analüüsitud riskide raames andmekaitse üldmääruses toodud kaitsemeetmed piisavad, et maandada kolmandate osapoolte poolt edasise andmetöötlusega kaasnevaid riske. Kuna praegune lahendus ei enneta piisavalt andmekaitsealates rikkumiste toimepanemist ega likvideeri nende algpõhjust, siis oleks õigustatud kehtestada terviseandmete töötlemisele erasektori poolt vähemalt minimaalsed nõuded, mis tagaksid selle, et pärast riiklikust andmekogust terviseandmete väljumist jääks näiteks turvalisuse tase sarnasele tasemele, et andmetöötlus oleks läbipaistev ja oleks tagatud ka muude andmekaitse üldmäärusest tulenevate nõuete tagamine.

223 Andmekaitse Inspektsiooni veebileht. Statistika. 2012-2019. Kättesaadav: https://www.aki.ee/et/teavitus-uudised/statistika (28.04.2021).
224 Samas.
225 Samas.

3.3. Andmekaitse üldmääruse artikkel 9 (4) kohased täiendavad piirangud erasektorile EL liikmesriikide näitel

Pärast andmekaitse üldmääruse jõustumist ei olnud liikmesriikidel võimalik sätestada täiendavaid erandeid eriliigiliste andmete töötlemiseks, kuid võib säilitada senised või kehtestada eriliigiliste töötlemisele täiendavad tingimused, sealhulgas piirangud terviseandmete töötlemiseks. Lühidalt tähendab see seda, et liikmesriikidel on võimalik siseriiklikult leppida kokku üksnes karmimates töötlemistingimustes. Seni ei ole Eesti pidanud vajalikuks täiendavaid tingimusi artikli 9 (4) kohaselt kehtestada.[226] Gercke, M. toob välja, et üks võimalus on kriminaliseerida identiteedivargus (nagu Eesti on ka teinud), kuid see on ainult üks lähenemine ning sama oluline kui mitte olulisem on pöörata rohkem tähelepanu andmekaitset reguleerivate õigusaktide parendamisele, mis on ennetavaks meetodiks.[227] Käesolevas peatükis on analüüsitud kolme liikmesriigi ja ühe endise liikmesriigi andmekaitse regulatsiooni: Läti, Soome, Rootsi ja Ühendkuningriigid.

Kehtiva Läti andmekaitseseaduse[228] § 25 (2) kohaselt on andmekaitse üldmääruse artiklis 9 nimetatud eriliigiliste andmete töötlemine lubatud, kui esineb mõni artiklis 9 (2) toodud alustest või tuleneb alus mõnest Läti siseriiklikust õigusaktist ja kooskõlas andmekaitse üldmääruse artikliga 9 (4). Kehtiva Läti kindlustuslepingu seaduse §7 (6) kohaselt on kindlustusandjal õigus üldjuhul lepingu kehtivuse ajal kontrollida kas kindlustusobjektiga seoses on toimunud muudatusi, sealhulgas muudatusi riskide osas. Sama paragrahvi viimase lause kohaselt on terviseandmete osas sätestatud erisus. Kindlustuslepingu kehtivusajal, pärast lepingu sõlmimist ei tohi kindlustusandja enam isiku terviseandmete kontrollimist teostada.[229] Oluline on ka see, et Läti kindlustuslepingu seaduse § 7 (1) ei erista terviseandmete töötlemise õiguslikku alus selle järgi kas tegemist on kohustusliku või vabatahtliku kindlustusega: kindlustuslepingu sõlmimisel kohustub kindlustusvõtja ja kindlustatud isik andma kindlustusandjale info, mis on vajalik kindlustusriski hindamiseks, sealhulgas info, mis on seotud kindlustatu tervisliku seisundiga kui sõlmitakse isikukindlustus ja tervisega seotud info on vajalik kindlustuslepingu sõlmimiseks. Läti isikuandmete kaitse seaduse eelnõu

226 Isikuandmete kaitse seaduse eelnõu seletuskiri.
227 Gercke, M. Internet-related identity theft, lk 32.
228 Fizisko personu datu apstrādes likums (Läti andmekaitseseadus). Latvijas Vēstnesis, 132, 04.07.2018. Kättesaadav: https://likumi.lv/ta/en/en/id/300099 (28.04.2021).
229 Apdrošināšanas līguma likums (Läti kindlustuslepingu seadus). Latvijas Vēstnesis, 97, 18.05.2018. Kättesaadav: https://likumi.lv/ta/en/en/id/299053-insurance-contract-law (28.04.2021).

mõjuanalüüsis on leitud, et kindlustustegevusega seotult on vajalik kehtestada eriliigiliste, sh terviseandmete töötlemisele täiendavad tingimused. Vastav õigusakt peaks andmete väärkohtlemise või loata ligipääsu vältimiseks sisaldama sätteid vähemalt töötlemise eesmärkide, isikuandmete kategooriate ja täiendavate tingimuste kohaldatavuse ulatuse kohta.[230] Seega erinevalt Eesti KindlTS §-st 218 on Lätis lubatud eriliigilisi terviseandmeid töödelda ka vabatahtliku kindlustuslepingu puhul ilma andmesubjekti nõusolekuta, kui terviseandmed on vajalikud lepingu sõlmiseks. Samuti ei näe Eesti KindlTS ette, et kindlustuslepingu kehtivusajal, pärast lepingu sõlmimist ei tohi kindlustusandja enam isiku terviseandmete kontrollimist teostada.

Soome on võtnud vastu andmekaitseseaduse,[231] millega täpsustatakse ning täiendatakse andmekaitse üldmäärusest tulenevaid sätteid. Näiteks on Soome andmekaitse seaduse § 6 (1) kohaselt täpsustatud andmekaitse üldmääruse artikli 9 (2) alapunkte b) g)-h) ja j). Käesoleva töö raames on neist oluline Soome andmekaitseseaduse §-s 6 (1) 1) toodu, mis reguleerib kindlustustegevuse raames eriliigiliste isikuandmete töötlemist: andmekaitse üldmääruse artikli 9 lõiget 1 ei kohaldata „kui kindlustusandja töötleb kindlustustegevuse käigus saadud teavet kindlustatu ja soodustatud isiku tervisliku seisundi, haiguse või puude kohta või tema kohta vajalike ravimeetmete või tema suhtes rakendatud võrreldavate meetmete kohta selleks et määrata kindlaks kindlustusandja vastutus."[232] Seaduse väljatöötamise ettepanekus on täiendavalt selgitatud, et andmekaitse üldmäärus ei anna kindlustusseltsile otseselt õigust töödelda eriliigilisi isikuandmeid oma vastutuse kindlaks tegemiseks, mistõttu peaks kavandatav seadus sätestama vastava õigusliku aluse.[233] Lisaks on Soome andmekaitseseaduse §-s 6 (2) sätestatud, et kindlustusandjad peavad vastutavate töötlejatena, sh ka nende volitatud töötlejad, järgima asjakohaseid erimeetmeid andmesubjekti eriliigiliste andmete töötlemisel. See tähendab, et kindlustusandjad ja nende volitatud töötlejad peavad andmesubjektide

230 Preliminary Impact Assessment Report of the Draft Law "Personal Data Processing Law" (annotation), 14.03.2018. Kättesaadav: http://titania.saeima.lv/LIVS12/SaeimaLIVS12.nsf/0/C74799DB57161C61C225825000483C5F?OpenDocument#b (28.04.2021).

231 Tietosuojalaki (Soome andmekaitseseadus). 5/5/2018/1050. Kättesaadav: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050 (28.04.2021).

232 Autori tõlge, vt lähemalt Soome andmekaitseseadusest nr 1050/2018, 6 p 1): *"Tietosuoja-asetuksen 9 artiklan 1 kohtaa ei sovelleta: 1) vakuutuslaitoksen käsitellessä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka sellaista häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista, jotka ovat tarpeen vakuutuslaitoksen vastuun selvittämiseksi;"*

233 Hallituksen esitys HE 9/2018 vp. (Soome valitsuse ettepanek parlamendile õigusaktide kohta, mis täiendavad ELi üldist andmekaitse määrust). 01.03.2018. Kättesaadav: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx (28.04.2021).

õiguste kaitseks:

1) rakendama meetmeid, mis võimaldavad igal ajal kontrollida ja verifitseerida isiku, kes on isikuandmeid säilitanud, muutnud või edastanud;
2) rakendama meetmeid isikuandmeid töötleva personali pädevuse tõstmiseks;
3) määrama andmekaitseametniku;
4) rakendama sisemised meetmed isikuandmetele juurdepääsu piiramiseks;
5) rakendama isikuandmete pseudonüümimist;
6) krüpteerima isikuandmeid;
7) rakendama meetmeid isikuandmete töötlemisega seotud töötlussüsteemide ja teenuste jätkuva konfidentsiaalsuse, terviklikkuse, kättesaadavuse ja tõrketaluvuse tagamiseks, sealhulgas füüsilise või tehnilise rikke korral tagama andmete kiire taastamise ja juurdepääsu võimaldamise;
8) kehtestama sise-eeskirjad korrapäraseks testimiseks, uurimiseks hindamaks tehniliste ja korralduslike meetmete tõhusust andmetöötluse turvalisuse tagamisel;
9) kehtestama sise-eeskirjad andmekaitse üldmääruse ja Soome andmekaitseseaduse täitmise tagamiseks isikuandmete edastamisel või muul eesmärgil isikuandmete töötlemisel;
10) koostama andmekaitse mõjuhinnangu vastavalt andmekaitse üldmääruse artiklile 35;
11) rakendama muid tehnilisi, menetluslikke ja organisatsioonilisi meetmeid.

Kuna Soome kindlustuslepingute seadusega[234] ei ole isikuandmete, sh terviseandmete töötlemist täiendavalt reguleeritud, siis tuleb autori hinnangul kohaldada eeltoodud sätteid nii kohustuslikke kui ka vabatahtlikke kindlustuslepinguid pakkuvatele kindlustusandjatele ja nende volitatud töötlejatele, kes töötlevad kindlustustegevuse raames andmesubjekti terviseandmeid oma vastutuse kindlaksmääramiseks, sh tuleb arvestada, et §-s 6 (1) 1) on eraldiseisev õiguslik alus terviseandmete töötlemiseks, mistõttu andmesubjekti nõusolek selleks pole vajalik. Seega, analüüsitud seaduste järgi on Soomes lubatud kindlustusandja vastutuse väljaselgitamiseks töödelda terviseandmeid ilma andmesubjekti nõusolekuta ja on kehtestatud täiendavad tingimused ettevõtjatele andmetöötluse osas.

234 Vakuutussopimuslaki (Soome kindlustuslepingu seadus). 28.6.1994/543. Kättesaadav:https://www.finlex.fi/fi/laki/ajantasa/1994/19940543 (28.04.2021).

Rootsi on võtnud vastu andmekaitse üldmäärust täiendava seaduse nr 2018:218.[235] Nimetatud seaduse kolmandas peatükis täpsustatakse andmekaitse üldmääruse artiklis 9 sätestatud eriliigiliste andmete töötlemise aluseid, mis hõlmavad järgmist: tööõigus, sotsiaalkindlustus ja sotsiaalkaitse (artikkel 9 (2) b)); oluline avalik huvi (artikkel 9 (2) g)); tervishoid ja sotsiaalhooldus (artikkel 9 (2) h)); ja arhiveerimine, teadustöö ning statistika (artikkel 9 (2) j)). Seaduse nr 2018:218 neljandas peatükis on sätestatud kasutuspiirangud, mis hõlmavad eriliigiliste andmete töötlemist avalikes huvides toimuva arhiveerimise, statistika ja teadustöö raames. Ehkki seaduses ei ole eraldi mainitud, siis tuleks autori hinnangul lugeda neid andmekaitse üldmääruse artikli 9 (4) mõttes täiendavateks siseriiklikult kehtestatud piiranguteks eriliigiliste andmete töötlemisel. Analüüsitud seaduse järgi ei ole aga Rootsi erinevalt Lätist, Soomest ja Ühendkuningriikidest, näinud vajadust kehtestada täiendavaid piiranguid või tingimusi ettevõtetele, kes töötlevad terviseandmeid väljaspool tervishoiuteenuse osutamist.

Ühendkuningriikide andmekaitseseadusega[236] (edaspidi UK andmekaitseseadus) on eriliigiliste andmete töötlemist täpsustatud üsna ulatuslikult. Seaduse lisas nr 1 esimeses ja teises osas on kirjeldatud, mis tingimustel võib eriliigilisi isikuandmeid töödelda töö, olulise avaliku huviga seotud põhjusel või tervishoiu, arhiveerimise, rahvatervise, teadus- või ajaloouuringute või statistilisel eesmärgil ehk täpsustatakse andmekaitse üldmääruse artikli 9 (2) punkte b) ja g)-j). UK andmekaitseseaduse väljatöötamisel leiti, et kindlustuslepingute sõlmimiseks, mille jaoks on terviseandmete töötlemine vajalik, peaks olema lubatud ilma andmesubjekti nõusolekuta, sest vastasel juhul võetaks sisuliselt tingimuslik nõusolek.[237] UK andmekaitseseaduse lisa nr 1 artikli 20 (1) kohaselt on olulise avaliku huvi tingimus täidetud kui töötlemine a) on vajalik kindlustuse eesmärgil, b) hõlmab terviseandmete töötlemist ja c) on vajalik avaliku huvi tõttu. UK andmekaitse seaduse artikli 20 (4) (a) kohaselt on täpsustatud, et töötlemist võib ilma nõusolekuta viia läbi juhul, kui vastutav töötleja ei saa mõistlikult võttes eeldada nõusoleku küsimist. Lisaks, UK andmekaitseseaduse lisa 1 artikkel 5 kohaselt peab olulisele avalikule huvile tuginemiseks kehtestama vastutav töötleja

235 Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Rootsi andmekaitseseadus). Välja antud: 19.04.2018. Kättesaadav: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218 (28.04.2021).

236 Data Protection Act 2018. United Kingdom. 23.05.2018. Kättesaadav: https://www.legislation.gov.uk/ukpga/2018/12/data.pdf (28.04.2021).

237 Practical problems in processing medical information under the GDPR. 11.08.2017. Kättesaadav: https://kennedyslaw.com/thought-leadership/article/practical-problems-in-processing-medical-information-under-the-gdpr/ (28.04.2021).

isikuandmete töötlemise korra ja võtma kasutusele spetsiifilised kaitsemeetmed, mida on täpsustatud artiklis 38-41. Peamiselt tähendab see vastutava töötleja kohustust kehtestada isikuandmete töötlemise kord, vastavalt vajadusele uuendada, kehtestada dokumendi säilitusekord ning ICO nõudmisel edastama dokumendi neile ilma tasu küsimata. Käesoleva töö autori hinnangul on pigem tegemist andmekaitse üldmäärusest tuleneva vastutava töötleja kohustusega anda andmesubjektile artiklites 12-14 nimetatud teavet. Võrreldes Soome andmekaitseseadusega on UK andmekaitseseaduse alusel näiteks kindlustusandjatele esitatud hulga vähem nõudmisi, kui töödeldakse andmesubjekti terviseandmeid, kuid samuti ei ole Ühendkuningriigid seadnud täiendavaid piiranguid kolmanda osapoole poolt terviseandmete töötlemiseks, kui seda tehakse väljaspool tervishoiuteenuse pakkumist ning andmesubjekti nõusoleku alusel.

Kokkuvõtvalt võib öelda, et kõikide käesolevas alapeatükis analüüsitud riikide andmekaitsealased õigusaktid sisaldavad vähemalt mõnda andmekaitse üldmääruse artikliga 9 seotud täiendust ja täpsustust hõlmates artikli 9 (2) punkte b) - j). Arvestades eelnevalt analüüsitud liikmesriikide andmekaitsealaseid õigusakte saab öelda, et ühelgi juhul ei kohalduks sätestatud piirangud kolmanda isiku poolt andmesubjekti terviseandmete töötlemisele, mis toimub andmesubjekti nõusoleku alusel, v.a Soome, ja väljaspool tervishoiuteenuse osutamist. Lätis ja Ühendkuningriigis on küll sätestatud täiendavad tingimused kolmanda osapoole poolt terviseandmete töötlemisele, aga kui terviseandmete töötlemine on vajalik kindlustuslepingu sõlmimisel kindlustusriski hindamiseks, siis ei ole vajalik andmesubjekti nõusolek selleks. See hõlmab ka näiteks vabatahtlikku elukindlustust. Rootsis ei ole seatud andmekaitseseaduse alusel täiendavaid terviseandmetega seotud piiranguid. Analüüsitud liikmesriikidest on kõige põhjalikumad piirangud terviseandmeid töötlevatele eraettevõtetele, täpsemalt kindlustusandjatele sätestanud Soome. Arvestades, et analüüsitud riikides ei ole olemas ega autorile teadaolevalt plaanis nõusolekuteenusega sarnast riiklikku lahendust, siis on ka mõistetav, et terviseandmete töötlemisega seotud piiranguid, mis kehtiksid kõigile eraõiguslikele ettevõtjatele, kes töötlevad terviseandmeid väljaspool tervishoiuteenust ja nõusoleku alusel, ei ole kehtestatud.

3.4. Võimalikud täiendavad tingimused ja/ või piirangud terviseandmete töötlemiseks Eestis andmekaitse üldmääruse artikli 9 (4) alusel

Kehtiva isikuandmete kaitse seaduse eelnõu seletuskirjas ei peetud vajalikuks kehtestada ega adresseerida andmekaitse üldmääruse artiklis 9 (4) sätestatud võimalust seada siseriiklikult eriliigiliste andmete töötlemisele (sh edastamisele) täiendavaid piiranguid.[238] RIA poolt arendatava nõusolekuteenuse sarnast lahendust ei ole autorile teadaolevalt Euroopas varasemalt rakendatud. Autori hinnangul on äärmiselt vajalik hinnata õiguslikku olukorda andmekaitse üldmääruse artikkel 9 (4) kontekstis, kuna nõusolekuteenuse kaudu terviseandmeid vastuvõttev vastutav töötleja ei ole avalik sektor ega ka tegevusloaga tervishoiuteenust pakkuv ettevõte, vaid tervishoiuteenust mitte osutav erasektori ettevõte. Käesolevas peatükis toodud soovituste osas on võetud arvesse töö teises peatükis kirjeldatud riske, mis paratamatult kaasnevad andmete edastamisega ja andmete edasise töötlemisega kolmandate osapoolte poolt (täpsemalt p 2.1). Samuti on arvestatud eelnevas peatükis käsitletud olemasolevate piirangute piisavust (p 3.2) ja liikmesriikide näiteid terviseandmete töötlemise osas (p 3.3).

Arvestades analüüsitud riske ning andmekaitse üldmäärusest tulenevaid piiranguid, mis peaksid efektiivselt ära hoidma punktis 2 toodud riskide realiseerumise, siis ei saa hetkel täie veendumusega öelda, et kõik riskid on maandatud ning täiendavaid piiranguid ei ole andmekaitse üldmääruse artikli 9 (4) alusel vajalik kehtestada. On siiski mõni risk, mida annaks maandada parema teavitustöö -ja ennetustegevusega järelevalve asutuse poolt. Selleks on näiteks punktis 2.7 kirjeldatud andmesubjekti madal teadlikkus andmekaitsest, sh jättes seetõttu näiteks enda nõusoleku tagasi võtmata kui lõpetab kolmanda osapoole teenuse kasutamise, kuid ei lõpeta lepingut. Samuti aitaks teavitus töö kaasa punktis 2.8 kirjeldatud probleemile, et andmesubjektid ei kiirustaks liigselt igale uuele teenusele ilma tingimusi lugemata „jah" ütlema, kõige osas nõusolekut andma ilma läbi lugemata, eelkõige olukorras, kus on võimalik valida.

Selleks, et vältida spetsiifiliselt kindlustusandjate poolt liigset terviseandmete töötlemist oleks mõistlik sätestada Eesti õigusesse sarnane terviseandmete töötlemisega seotud piirang nagu

238 Isikuandmete kaitse seaduse eelnõu seletuskiri.

on ettenähtud Läti kindlustuslepingu seaduse §-s7 (6): kindlustuslepingu kehtivusajal, pärast lepingu sõlmimist ei tohi kindlustusandja enam isiku terviseandmete kontrollimist teostada. Nimetatud piirang peaks kehtima vähemalt vabatahtlike kindlustuslepingute puhul, et vältida andmetöötluse kuritarvitamist kuivõrd tervisega seotud kindlustuslepingute puhul ei tohiks pidada tervise halvenemist või raske diagnoosi saamist pärast lepingu sõlmimist VÕS § 443 kohaseks kindlustusriski võimalikuks suurenemiseks. Tervisega seotud kindlustuse puhul on tegemist riskiga, mida kindlustusvõtja soovis kindlustada, et tulla toime ootamatute kuludega. Ehk leping sai just sellel põhjusel sõlmitud, et tervise ootamatu halvenemise korral võiks kindlustushüvitis katta ootamatud kulud. Tervisekindlustusega seotud kindlustusriski suurenemiseks võiks pigem pidada näiteks seda, kui kindlustusvõtja on korduvalt liikluses kiiruse ületamise eest trahvi saanud või sattunud varem liiklusõnnetusse, milles oli õnnetuse põhjustaja. Seega, täiendavat terviseandmete töötlemist pärast kindlustuslepingu sõlmimist tuleks pidada pigem ülemääraseks töötluseks, v.a KindlTS § 218 lg 2 punktis 2 ettenähtud olukordades.

Ülejäänud riskide osas on võimalik järelevalvel teostada pistelisi omaalgatuslikke kontrolle, nõustada kui seda küsitakse või vajadusel määrata haldustrahv (pärast haldustrahvi seaduse vastuvõtmist ja jõustumist). Võib oodata, et andmekaitse üldmäärusest tuleneva karistusliku elemendi rakendamine muudab andmekaitse küsimused ettevõtete jaoks olulisemaks kui seni. Kuna käesoleva töö eesmärk ei ole analüüsida seda, mida on võimalik võtta ette pärast seda kui rikkumine on toimunud, vaid saada aru kas täiendavate meetmete, piirangute rakendamise tõttu oleks võimalik paremini ennetada töö teises peatükis käsitletud riskide realiseerumist, siis on hinnatud järgmisena võimalikke andmekaitse üldmääruse artikli 9(4) alusel kehtestatavaid siseriiklikke piiranguid.

Käesoleva töö autori hinnangul näitab andmekaitsealaste riskide analüüs, et tugevam, süstemaatilisem ja korrapärasem siseriiklik järelevalvet võiks olla asjakohane meede, millega maandada mitmeid käsitletud probleeme. Praeguse olukorra üks suurimaid puudujääke näib olevat see, et puudub korrapärane järelevalve ning isegi kui andmekaitse üldmäärus paneb vastutavatele töötlejatele kohustuse midagi teha, siis ei pruugi ettevõte reaalselt andmekaitse üldmääruses ettenähtud kaitsemeetmeid tegelikkuses rakendada, olgugi et kodulehel on olemas isikuandmete töötlemise kord. Seda suuresti põhjusel, et ettevõttel pole piisavaid

ressursse andmekaitsega tegelemiseks ning ka seetõttu, et nõuete mittetäitmisega ei pruugi kaasneda midagi enne kui mõni klient esitab AKI-le kaebuse, andmesubjekt esitab kuriteoteate või realiseerub mõni küberintsident. Kõigi nende olukordade puhul on oht juba realiseerunud ja kahju andmesubjektile tekitatud. Lisaks, andmekaitse üldmäärusest tulenevad AKI-le piisavalt laiad volitused järelevalveks, kuid nagu eelnevalt punktis 3.3 kirjeldatud, siis AKI-l pole piisavalt haldusressurssi, et kõigi rikkumistega ükshaaval tegeleda. Samas, andmekaitse üldmäärusest tulenevate nõuete mõju aitab tagada just efektiivne – piisava haldusvõime ja kompetentsiga järelevalve.[239] Ka rahvusvaheline praktika näitab, et üksnes nõuetest ei ole kasu, on vaja efektiivset vastavuskontrolli järelevalvet tõhususe tagamiseks.[240] Terviseandmete töötlemise puhul on äärmiselt oluline teada, kuidas ja kas tegelikult ka konkreetne vastutav töötleja andmekaitse üldmäärusest tulenevaid nõudeid täidab, sh kas saab aru talle tegelikult esitatud nõuetest ja vastutuse ulatusest. Pistelise rutiinse kontrolli käigus suudaks AKI seda kindlasti tuvastada, kuid see lahendaks vaid üksikuid probleeme. Reaalsuses pole AKI-l piisavalt ressurssi, et tegeleda lisaks andmekaitse üldmääruse järgselt suurenenud kaebustele omaalgatuslike kontrollidega.[241]

Arvestades, et nõusolekuteenuse raames on võimalik inimesel anda nõusolek oma andmete edastamiseks kolmandale osapoolele, kellele praegu ei kohaldu siseriiklikult täiendavaid piiranguid ja et andmekaitse üldmäärusest tulenevad nõuded on kohati liiga kahetimõistetavad, siis on õigustatud rangema järelevalve korraldamine ning täiendavate piirangute kehtestamine eelkõige ettevõtetele, kes hakkavad töötlema inimeste terviseandmeid väljaspool tervishoiuteenust ja nõusoleku alusel.

Töö autori hinnangul on üheks võimalikuks kehtestada kolmandatele osapooltele, kes töötlevad nõusolekuteenuse kaudu terviseandmeid kohustuslikud tingimused, sealhulgas iga-aastane raporteerimise kohustus. Nõuete valiku puhul on arvestatud, et: terviseandmetele tuleb säilitada sama või kõrgema taseme turbeaste; terviseandmete töötlemisel tuleb rakendada lõimitud ja vaikimisi andmekaitse nõudeid, et tagada läbipaistvus; nõusolekud peavad olema konkreetsed, ühemõttelised ja selged ning iga eesmärgi suhtes eraldi antavad;

239 Sein, K., Mikiver, M., Tupay, P. K. Pilguheit andmesubjekti õiguskaitsevahenditele uues isikuandmete kaitse üldmääruses. Juridica 2/2018, lk 115.

240 Neto, N.N., Madnick, S., de Paula, M. G., Borges, N. M. A Case Study of the Capital One Data Breach. Working Paper CISL# 2020-16. 01.03.2020, lk 16. Kättesaadav: https://ssrn.com/abstract=3570138 (28.04.2021).

241 Andmekaitse Inspektsiooni veebileht. Statistika. Kättesaadav: https://www.aki.ee/et/teavitus-uudised/statistika (28.04.2021).

andmete privaatsustehnoloogia, sh anonüümimistehnoloogiate kasutamisele on vajalik kehtestada selged juhised minimaalsete nõuetega; terviseandmetel põhinevad teenused peaksid rakendama kliendile tugevat autentimist, et vältida kliendiga seotud kasutajaprofiilile lubamatut ligipääsu kõrvalistel isikutel ning ühtlasi veenduda andmesubjekti vanuses. Arvestades eeltoodut ja punktis 3.3. toodud liikmesriikide näiteid on üheks võimaluseks sätestada IKS-i alltoodud kohustused. Kolmandas osapool, kes liitub nõusolekuteenusega ja töötleb terviseandmeidkohustub:

1) rakendama meetmeid isikuandmeid töötleva personali pädevuse tõstmiseks;
2) kehtestama sise-eeskirjad andmetöötlustoimingute turvalisuse tagamiseks, sealhulgas nende korrapäraseks testimiseks, et hinnata meetmete tõhusust andmetöötluse turvalisuse tagamisel;
3) kehtestama sise-eeskirjad andmekaitse üldmääruse täitmise tagamiseks isikuandmete, sealhulgas terviseandmete edastamisel või muul eesmärgil isikuandmete töötlemisel;
4) koostama andmekaitse üldmääruse artiklile 30 vastava andmetöötlustoimingute ülevaate ning rakendama meetmeid, mis võimaldavad igal ajal kontrollida ja verifitseerida isiku, kes on isikuandmeid säilitanud, muutnud, vaadanud või edastanud, sealhulgas kuhu on edastatud (logiraamat);
5) viima läbi ja esitama AKI-le andmetöötluse riskide hindamine ja nende maandamiseks rakendatavate meetmete hinnangu vastavalt andmekaitse üldmääruse artiklile 35 (mõjuhinnang);
6) määrama andmekaitseametniku;
7) viima läbi ja esitama AKI-le andmekaitsealanse vastavusauditi tulemuse, mille alusel on hinnatud ettevõtte isikuandmete süsteemi, sh dokumentatsiooni andmekaitse üldmääruses toodud nõuetele vastavuse osas;
8) viima läbi ja esitama AKI-le iga-aastaselt andmekaitsealase valmidusauditi, mille koostamisel on võetud aluseks ettevõtte igapäevaseid ja tegelikke andmetöötluspraktikaid, arvestades sealhulgas töötlemistoimingute ülevaates sätestatut, ning nende vastavust ettevõtte poolt kehtestatud andmekaitsealaste siseprotseduuride, isikuandmete töötlemiskorraga;
9) rakendama asjakohaseid privaatsustehnoloogiaid isikuandmete pseudonüümimisel ja anonüümimisel, arvestana sealjuures järelevalveasutuse (AKI või EDPB) asjakohaseid juhiseid ning andmekaitse üldmääruse artiklitest 25 ja 32 tulenevaid nõudeid isikuandmete turvalisuse tagamisel;
10) tagama isikuandmete, sealhulgas terviseandmete säilitamisele, edastamisel

kolmandatele osapooltele ja muule töötlemisele sama või kõrgema tasemega turbeastet, kui riiklikul andmebaasil, millest tervisega seotud andmed kolmandale osapoolele nõusolekuteenuse kaudu on edastatud;

11) rakendama andmesubjekti poolt terviseandmetel põhineva teenuse kasutamisel tugeva autentimise nõudeid ehk meetodit, mis põhineb vähemalt kahe teineteisest sõltumatult toimiva ja autentimisandmete konfidentsiaalsust tagava turvaelemendi kasutamisel, mida teab või omab üksnes teenust kasutav andmesubjekt või mida saab omistada üksnes talle.

Nimetatud kohustuste täitmisele kuluv ajaline maht on kahtlemata suur, kuid seda eelkõige esimesel korral. Lisaks, mitmed nimetatud kohustustest võivad osutuda terviseandmeid töötlevatele ettevõtetele kohustuslikuks ka juba praegu, kuid andmekaitse üldmäärusest tulenev sõnastus on jätnud piisava kaalutlusruumi, mistõttu ettevõte võib otsustada mõnda nõuet mitte täita. Tehnoloogia võib ühest küljest suurendada eraelu riivele, kuid teisest küljest võimaldab just tehnoloogia mitmeid piiranguid maandada.[242] See on eelkõige oluline just väikeste (idu)ettevõtete puhul, kelle poolt arendatavad teenused võivad osutuda populaarseks ning Global Privacy Enforcement Network (edaspidi GPEN) 2018. a uuringu kohaselt oli üheks suuremaks probleemiks see, et ettevõtetel puudus tegelik sisemine kontroll ning monitooring väidetavate meetmete rakendamise ning piisavuse osas.[243] Kui pangad või kindlustusandjad töötlevad terviseandmeid, siis nende osas oleksid turvalisusega seotud andmekaitseriskid maandatud, kuna peavad osalised juba praegu andmekaitsega seotud nõuete ja nende täitmise kohta Finantsinspektsioonile rutiinse kontrolli käigus informatsiooni andma. Andmekaitseametniku määramist toetab autori hinnangul asjaolu, et praktikast on teada mitmeid näiteid, kus kohtu- ja omavalitsusametnikudki on korduvalt teinud lubamatuid päringuid rahvastikuregistrist ning peamiseks põhjuseks uudishimu.[244] Võimaldades erasektorile riiklikest andmekogudest terviseandmeid tuleb arvestada, et andmesubjektil puudub Digilooga sarnane võimalus kontrollida millal ja kes tema andmeid töötles.

Töötlemistoimingute ülevaade, andmekaitseametniku kohustus ning nn logiraamatu kohustus

242 Riigikogu toimetised. - Riigikogu kantselei väljaanne, RiTo 42/2020, lk 115. Kättesaadav: https://rito.riigikogu.ee/wordpress/wp-content/uploads/2020/12/RiTo_42.pdf (28.04.2021).

243 GPEN Sweep 2018 'Privacy Accountability' October 2018. Office of the Privacy Commissioner, New Zealand, Information Commissioner's Office, UK. Kättesaadav: https://ico.org.uk/media/about-the-ico/documents/2614435/gpen-sweep-2018-international-report.pdf (28.04.2021)

244 Pärgmäe, R. jt. Õiguse ja eetika töörühma raport, lk 27.

annaks andmesubjektidele suurema kindluse, et tema andmeid kasutatakse üksnes teenuse osutamise eesmärgil mitte mõne üksiku töötaja uudishimu rahuldamiseks. Kui ettevõttes on olemas andmekaitse toimingute eest vastutav isik, kes peab vastavalt andmekaitse üldmääruse artiklile 38 olema oma ametis sõltumatu, siis tagaks see ka andmesubjektidele konkreetse kontaktisiku, kelle poole andmekaitset puudutava küsimusega pöörduda.

Pakutud lahendused andmekaitse üldmääruse artikli 9 (4) alusel terviseandmete töötlemise piiramiseks tõstaks esmalt tõenäoliselt AKI kulutusi ning töömahtu, kuid pikemas vaates võiks oodata töömahu kahanemist kaebuste arvelt. Süstemaatiline kontroll turuosaliste üle võimaldab saada parema ülevaate andmekaitse nõuete täitmisest ning seda kokkuvõtlikult auditi raporti näol. Seejuures nõusolekuteenusega liituvatel ettevõtetel on võimalik saada sisulisemat tagasisidet enda poolt valitud meetmete piisavuse, töötlemistoimingute õiguspärasuse kohta. Samuti võimaldaks antud lahendus ühtlasemat turuosaliste teadlikkuse tõstmist.

KOKKUVÕTE

Käesoleva magistritöö peamine eesmärk oli analüüsida nõusolekuteenusega kaasnevaid andmetöötlusriske ning hinnata kas andmekaitse üldmäärusest tulenevad piirangud on piisavad nende maandamiseks või oleks vajalik kehtestada täiendavaid siseriiklikke piiranguid andmekaitse üldmääruse artikli 9 (4) alusel. Nõusolekuteenus on uus innovaatiline teenus, mida RIA arendab erasektori äriühingutele, kellel puudub seadusest tulenev alus pääseda ligi tervise infosüsteemis olevatele andmetele ning kes soovivad pakkuda füüsilistele isikutele nende terviseandmetel põhinevaid teenuseid. Seejuures aga ei kvalifitseeruks nimetatud teenused TTKS § 2 mõttes tervishoiuteenusteks.

Analüüsi alguses sai püstitatud kaks uurimisküsimust: kas nõusolekuteenuse kaudu terviseandmete edastamisel riiklikest andmebaasidest kolmandatele osapooltele, on andmekaitse üldmääruses toodud kaitsemeetmed piisavad, et maandada kolmandate osapoolte poolt edasise andmetöötlusega kaasnevaid riske? Kas ja milliseid täiendavaid tingimusi oleks Eestil vajalik andmekaitse üldmääruse artikli 9 (4) alusel kolmandate osapoolte poolt terviseandmete töötlemiseks kehtestada?

Töö esimeses peatükis käsitleti seda, milliseid andmeid loetakse andmekaitse üldmääruse alusel täpsemalt terviseandmete mõiste alla. Ilmselgelt käsitletakse nendena andmeid, mis on kogutud tervishoiuteenuse osutamisega seoses, samuti andmed, mis viitavad haigestumisohule. Näiteks info füüsilise isiku kohta, kes on Covid-19 kontaktne. Euroopa Kohus on selgitanud, et terviseandmeid tuleb tõlgendada laialt ning nii võivad mõned andmed osutuda terviseandmeteks ka ristviitamise teel, sest olenevalt kontekstist võivad andmed koosmõjus teiste andmetega avaldada konkreetse isiku terviseriske.

Lisaks käsitleti esimeses peatükis terviseandmetega seotud innovatsiooni ning kasvavat trendi *mHealth*-i ja personaalmeditsiini suunas. Nõusolekuteenus ei ole küll tervishoiuteenus ega tervishoiuteenust otseselt toetav teenus, kuid eesmärk on võimaldada füüsilisele isikule enda isikuandmete, sealhulgas terviseandmete teisest kasutamist väljaspool tervishoiuteenust.

Selleks, et kolmandad osapooled saaksid teenuseid pakkuda on vajalik tuvastada ka kohane õiguslik alus. Kui nõusolekuteenuse kaudu annab andmesubjekt enda nõusoleku andmete edastamiseks riikliku andmekogu vastutavale töötlejale, siis kolmandale osapoolele annab andmesubjekt enda nõusoleku konkreetsete terviseandmetel põhinevate teenuste pakkumiseks. Analüüsis käsitleti seda kas saab pakkuda terviseandmetel põhinevat teenust nõusoleku alusel kui sellega paralleelselt kaasneb ka leping. Kuna andmekaitse üldmääruse artikli 9 (2) toodud säte on erinorm artikli 6 suhtes, siis ei saa antud juhul lähtuda sellest, et terviseandmed on vajalikud lepingu täitmiseks. Küll aga tuleks hinnata terviseandmete töötlemise vajalikkust andmekaitse üldmääruse artikli 7(4) alusel. Autor jõudis järeldusele, et kui tegemist on teenusega, kus terviseandmed on põhiteenuse olemuslik osa, mitte üksnes abistavad, siis on artiklis 7 (4) toodud „vajalikkuse" tingimus täidetud ning tuleks jaatada nõusoleku lubatavust ning selle kehtivust.

Täiendavalt on analüüsitud seda kas andmesubjekt saab enda nõusoleku anda riikliku andmekogu vastutavale töötlejale, sest andmekaitse üldmääruse kohaselt ei saa avalikus sektoris osapoolte ebavõrdse olukorra tõttu üldiselt rääkida nõusolekust kui kehtivast õiguslikust alusest. Siiski, nõusolek ei ole avalikus sektoris täielikult välistatud. Eelkõige siis, kui võib öelda, et tegemist on mugavusteenusega ning täidetud järgmised tingimused: andmesubjekt saab vabalt otsustada kas nõusolekut anda või mitte ehk puudub sundus, andmesubjektil on olemas alternatiiv kasutada mõnda muud lahendust sama või sarnase tulemuse saavutamiseks, nõusoleku mitteandmisega ei kaasne andmesubjektile ei otsest kahju ega kaudsemat kahju põhiõiguste riive näol, mida avalik sektori rakendab suurele grupile või tervele ühiskonnale. Näiteks avaliku sektori poolt arendatud koroona mobiilirakenduse puhul on õiguskirjanduses leitud, et kahe esimese puhul tuleks vastata eitavalt ning viimase puhul eksisteerib tugev põhiõiguste riive ehk kahjulik mõju avaldub üldise liikumispiirangu näol. Seega ei saaks pandeemia kontrollimiseks kasutatava mobiilirakenduse puhul olla tegemist kehtiva nõusolekuga. Nõusolekuteenuse puhul saab autori hinnangul vastata igale tingimusele jaatavalt ning seega võib pidada nõusolekut nõusolekuteenuse raames lubatavaks õiguslikuks aluseks.

Töö teises peatükis käsitleti nõusolekuteenusega potentsiaalselt kaasneda võivaid riske, kuna nõusolekuteenuse kaudu väljastatakse riigi poolt sunduslikult kogutud terviseandmed

erasektori ettevõtetele, v.a tervishoiuteenuse osutajad või muud teenusepakkujad, kellel on Tervise infosüsteemis olevatele andmete seadusest tulenev ligipääs. Sellistel ettevõtetel ei ole käesoleval hetkel kehtestatud terviseandmete seotult täiendavaid piiranguid või tingimusi, aga kuna terviseandmed on väga tundlikud isikuandmed ja tegemist on olulise innovatsiooniga terviseandmete teisese kasutamise võimaldamisel, siis pidas autor analüüsida erinevaid andmekaitse õiguslikke riske.

Üheks terviseandmete oluliseks tingimuseks on kolmandate osapoolte poolt konkreetse töötlemiseesmärki järgimine ning see, et oleks iga töötlemiseesmärgi kohta võimalik nõusolek küsida. Praktikas esineb aga juhtumeid, kus andmesubjektilt küsitakse nn kobarnõusoleku alusel mitme töötlemiseesmärgi täitmiseks luba. Samuti on probleemiks liiga üldised ning üldmäärased töötlemiseesmärgid, mille varju peidetakse ära järjest enam probleemseks muutuv andmemüük andmemaakleritele. Samuti käsitleti seda kuivõrd probleemseks võib saada see, et kindlustusandjad ja krediidiandjad ütlevad, et nõusolek terviseandmete edastamiseks krediidivõimelisuse hindamiseks või vabatahtliku kindlustuslepingu kindlustusriski hindamiseks on vabatahtlik, aga sisuliselt pakutakse vastutasuks soodsamaid lepingutingimusi. Sellest, et isikuandmeid käsitletakse kui uut varaklassi on ammu räägitud ja ka õiguskirjanduses leidub erinevaid seisukohti Peamiselt leitakse siiski, et isikuandmete kaitse on üks inimese põhiõigustest ning seda ei saa monetiseerida. EDPB on võrrelnud isikuandmete turu olemasolu lausa iniorganite müügiga, millele on küll turg olemas, aga see ei tähenda, et see peaks õiguslikult lubatav olema.

Järgmiseks on analüüsitud lühidalt potentsiaalset lapse terviseandmete ebaseadusliku töötlemist. Kuna andmekaitse üldmääruse kohaselt ei või alaealine terviseandmete töötlemisele iseseisvat nõusolekut anda, siis ei tohiks lastel nõusoleku andmist võimaldada. Juhul kui seda siiski soovitakse teha, siis peab olema tagatud laste seaduslike esindajate poolt nõusoleku andmise võimalus. Sellest tulenevalt peaks kolmas osapool tagama, et riiklikust andmekogust saabunud andmete edasiseks töötlemiseks annab nõusoleku lapse seaduslik esindaja. Töö autori hinnangul ei ole üksnes linnuse tegemine märkeruutu kinnitamaks vanust või seadusliku esindaja poolset nõusolekut ei ole piisav meede, sest võimaldab lihtsat võltsimist.

Samuti on käsitletud andmesubjekti vähese teadlikkusega kaasnevaid riske, mille kohaselt võetakse andmete edastamiseks riiklikust andmebaasist nõusolek tagasi, aga ei tehta sama kolmanda osapoolt pakutavas teenuses. Juhul, kui soov ongi üksnes edastamine ära lõpetada ja teenust saab ilma jätkuva andmevahetuseta edasi pakkuda, siis ei teki probleemi. Küll aga tekib probleem olukorras, kus andmesubjekt tegelikkuses soovis teenusekasutamise ka lõpetada ning kunagi hiljem selgub ebameeldiv üllatus ja teenusepakkuja töötleb jätkuvalt tema andmeid või neid aastaid andmemaakleritele müünud. Teiseks andmesubjekti vähese teadlikkusega seondub see, et kolmandad osapooled võivad edastada andmeid ka kolmandatesse riikidesse, mille kohta ei ole väljastatud Euroopa Komisjoni poolt andmekaitsetaseme piisavuse otsust ning andmesubjektid ei tea, mis see endaga kaasa võib tuua ja teadmatuse tõttu ei pea seda probleemiks.

Kõige viimaseks on analüüsitud terviseandmete turvalisusega seotud probleeme, samuti anonüümimistehnika puuduliku rakendamisega seotud probleeme. Esimene neist on oluline risk, kuna ebapiisava turvalisuse tõttu võivad saada terviseandmetele ligi isikud, kellel puudub selleks õiguslik alus ning kelle eesmärk on saada illegaalselt omandatud andmetest majanduslikku kasu, tekitades sellega andmesubjektile varalist või mittevaralist kahju. Kõige kahjulikumaks neist võib pidada stsenaariume, kus kasutatakse ebaseaduslikult raske haiguse või surmaga lõppeva haiguse üksikasju või pannakse toime pikaajaline identiteedivargus. Viimased on nii Eesti statistika andmetel kui ka maailmas laiemalt kasvav trend. Sama saab öelda ka andmelekete ning muude küberintsidentide kohta. Andmete anonüümimisega on seotud kasvab suurandmete töötlemisega järjest enam see probleem, et täielikult anonüümseid andmeid ei eksisteeri. Ehkki andmekaitse üldmääruse mõttes käsitleta absoluutset lähenemist, vaid lähtutakse mõistlike pingutuste kaudu isiku tuvastamist, siis ka see tähendab sisuliselt väga ranget privaatsustehnoloogia rakendamist. Teaduskirjanduses on põhjalikult analüüsitud mitmeid juhtumeid, kus anonüümitud andmestikust oli võimalik tuvastada lihtsa vaevaga mitmed üksikisikud ning samuti osad isikud kaudselt.

Töö kolmandas peatükis käsitleti esmalt ülevaatlikult kehtivaid andmekaitse üldmäärusest tulenevaid piiranguid, mis terviseandmete töötlemise kontekstis on kolmandate osapoolte poolt edasise töötlemise juures olulised. Järgmisena anti hinnang olemasolevate piirangute piisavusele ning jõuti järeldusele, et kõiki käesoleva töö teises peatükis käsitletud riske ei ole

võimalik efektiivselt maandada ning üksnes olemasolevad andmekaitse üldmääruses toodud kaitsemeetmed pole piisavad, v.a üksikud erandid nagu vähese teadlikkuse probleem, mida oleks võimalik maandada süstemaatilisema teavitustööga.

Kolmandaks analüüsiti kolmandas peatükis Läti, Soome, Rootsi ja Ühendkuningriigis kehtivaid andmekaitseseaduseid. Kokkuvõtvalt võib öelda, et kõikide analüüsitud riikide andmekaitsealased õigusaktid sisaldavad vähemalt mõnda andmekaitse üldmääruse artikliga 9 seotud täiendust ja täpsustust hõlmates artikli 9 (2) punkte b) - j). Kuid ainult Soome puhul kohalduks sätestatud piirangud kolmandale isikule, kes töötleb andmesubjekti terviseandmeid nõusoleku alusel ja väljaspool tervishoiuteenuse osutamist. Lätis ja Ühendkuningriigis on küll sätestatud täiendavad tingimused kolmanda osapoole poolt terviseandmete töötlemisele, aga töötlemise õiguslikuks aluseks ei oleks nõusolek. Rootsi on täpsustanud artiklist 9 tulenevaid töötlemisaluseid niivõrd kui see tuleneb andmekaitse üldmäärusest, kuid ei ole seadnud terviseandmete töötlemisele kolmanda osapoole poolt täiendavaid piiranguid. Arvestades, et analüüsitud riikides ei ole olemas ega autorile teadaolevalt plaanis nõusolekuteenusega sarnast riiklikku lahendust, siis on ka mõistetav, et terviseandmete töötlemisega seotud piiranguid, mis kehtiksid kõigile eraõiguslikele ettevõtjatele, kes töötlevad terviseandmeid väljaspool tervishoiuteenust ja nõusoleku alusel, ei ole kehtestatud.

Kuna käesoleva magistritöö eesmärk oli saada aru milliste meetmete, piirangute rakendamise tõttu oleks võimalik paremini ennetada töö teises peatükis käsitletud riskide realiseerumist, siis hinnati kolmanda peatüki viimases peatükis võimalikke andmekaitse üldmääruse artikli 9(4) alusel kehtestatavaid siseriiklikke piiranguid.

Praeguse olukorra üks suurimaid puudujääke kolmanda osapoole poolt terviseandmete edasise töötlemise puhul nõusolekuteenuse raames näib olevat see, et andmekaitse üldmäärusest tulenevad kaitsemeetmed on liiga laialt tõlgendatavad ning puudub korrapärane järelevalve.

Vältimaks spetsiifiliselt kindlustusandjate poolt liigset terviseandmete töötlemist on mõistlik järgida Läti kindlustuslepingu seaduse eeskuju ning sätestada Eesti KindlTS-sse tingimus, et kindlustuslepingu kehtivusajal, pärast lepingu sõlmimist ei tohi kindlustusandja enam

täiendavat andmesubjekti terviseandmete kontrollimist teostada. Nimetatud piirang peaks kehtima vähemalt vabatahtlike kindlustuslepingute puhul, et vältida andmetöötluse kuritarvitamist kuivõrd tervisega seotud kindlustuslepingute puhul ei tohiks pidada ootamatut tervise halvenemist pärast lepingu sõlmimist VÕS § 443 kohaseks kindlustusriski võimalikuks suurenemiseks.

Terviseandmete tundlikkuse tõttu on õigustatud vähemalt järgmiste IKS-i sätestatavate minimaalsete kohustuslike nõuete rakendamine:

Kolmandas osapool, kes liitub nõusolekuteenusega ja töötleb terviseandmeid kohustub:

1) rakendama meetmeid isikuandmeid töötleva personali pädevuse tõstmiseks;
2) kehtestama sise-eeskirjad andmetöötlustoimingute turvalisuse tagamiseks, sealhulgas nende korrapäraseks testimiseks, et hinnata meetmete tõhusust andmetöötluse turvalisuse tagamisel;
3) kehtestama sise-eeskirjad andmekaitse üldmääruse täitmise tagamiseks isikuandmete, sealhulgas terviseandmete edastamisel või muul eesmärgil isikuandmete töötlemisel;
4) koostama andmekaitse üldmääruse artiklile 30 vastava andmetöötlustoimingute ülevaate ning rakendama meetmeid, mis võimaldavad igal ajal kontrollida ja verifitseerida isiku, kes on isikuandmeid säilitanud, muutnud, vaadanud või edastanud, sealhulgas kuhu on edastatud (logiraamat);
5) viima läbi ja esitama AKI-le andmetöötluse riskide hindamine ja nende maandamiseks rakendatavate meetmete hinnangu vastavalt andmekaitse üldmääruse artiklile 35 (mõjuhinnang);
6) määrama andmekaitseametniku;
7) viima läbi ja esitama AKI-le andmekaitsealase vastavusauditi tulemuse, mille alusel on hinnatud ettevõtte isikuandmete süsteemi, sh dokumentatsiooni andmekaitse üldmääruses toodud nõuetele vastavuse osas;
8) viima läbi ja esitama AKI-le iga-aastaselt andmekaitsealase valmidusauditi, mille koostamisel on võetud aluseks ettevõtte igapäevaseid ja tegelikke andmetöötluspraktikaid, arvestades sealhulgas töötlemistoimingute ülevaates sätestatut, ning nende vastavust ettevõtte poolt kehtestatud andmekaitsealaste siseprotseduuride, isikuandmete töötlemiskorraga;
9) rakendama asjakohaseid privaatsustehnoloogiaid isikuandmete pseudonüümimisel ja anonüümimisel, arvestana sealjuures järelevalveasutuse (AKI või EDPB)

asjakohaseid juhiseid ning andmekaitse üldmääruse artiklitest 25 ja 32 tulenevaid nõudeid isikuandmete turvalisuse tagamisel;

10) tagama isikuandmete, sealhulgas terviseandmete säilitamisele, edastamisel kolmandatele osapooltele ja muule töötlemisele sama või kõrgema tasemega turbeastet, kui riiklikul andmebaasil, millest tervisega seotud andmed kolmandale osapoolele nõusolekuteenuse kaudu on edastatud;
11) rakendama andmesubjekti poolt terviseandmetel põhineva teenuse kasutamisel tugeva autentimise nõudeid ehk meetodit, mis põhineb vähemalt kahe teineteisest sõltumatult toimiva ja autentimisandmete konfidentsiaalsust tagava turvaelemendi kasutamisel, mida teab või omab üksnes teenust kasutav andmesubjekt või mida saab omistada üksnes talle.

Sobivate nõuete valiku puhul on arvestatud, et terviseandmetele tuleks säilitada sama või kõrgema taseme turbeaste; terviseandmete töötlemisel tuleb rakendada lõimitud ja vaikimisi andmekaitse nõudeid, et tagada andmesubjektidele maksimaalne läbipaistvus; töötlemistoimingute ülevaade võimaldab kolmandatel osapooltel saada selgelt aru, mis toiminguid tehakse ning seega küsida nõusolekuid üksnes konkreetsetele läbimõeldud eesmärkidele, tagada nende ühemõttelisuse ja võimaluse kategoriseerida nõusoleku küsimine iga eesmärgi suhtes eraldi; andmete privaatsustehnoloogia, sh anonüümimistehnoloogiate kasutamisele on vajalik kehtestada selged juhised, et vältida isikustatud andmete tahtlikku või tahtmatut jagamist; terviseandmetel põhinevad teenused peaksid rakendama kliendile tugevat autentimist, et vältida kliendiga seotud kasutajaprofiilile kõrvaliste isikute, sealhulgas ettevõtte oma töötajate, poolt lubamatut ligipääsu ning ühtlasi ka selleks, et veenduda andmesubjekti vanuses. Lisaks arvestati nõuete valikul liikmesriikide andmekaitseõiguses sätestatud andmekaitse üldmääruse artikli 9 (4) alusel seatud piiranguid.

Ühe olulisema kohustusena on toodud välja, et ettevõte peaks koostama andmekaitsealase mõjuhinnangu, viima läbi korrapärased andmekaitsealased auditid ning esitama vastava tulemuse järelevalveametile, samuti on vajalik koostada töötlemistoimingute ülevaate. Nimetatud meetmed on vajalikud seetõttu, et võimaldavad kolmandal osapoolel oma andmekaitsealaseid riske hallata ning probleeme ennetada. Kui ettevõte ei ole tuvastanud teostatavaid töötlemistoiminguid ega hinnanud nendega kaasnevaid riske ning mõju andmesubjektide õigustele ning kohustustele, siis ei ole võimalik adekvaatselt hinnata ka

sobivate tehnoloogiliste kaitsemeetmete vajadust. Samuti, jättes koostamata töötlemistoimingute ülevaate on ettevõttel ka keeruline eristada erinevaid andmetöötlus eesmärke ning valida sobilikku õiguslikku alust. Seetõttu võib eeldada, et need meetmed maandavad tõhusalt töö teises peatükis välja toodud riske.

Andmekaitse üldmäärusest tulenevalt tuleb kõigil vastutavatel töötlejatel rakendada lõimitud ja vaikimisi andmekaitset, mis tähendab, et ka nõusolekuteenust kasutavad ettevõtted peavad läbinisti neid põhimõtteid rakendama. Eesti on loonud endale tugeva digiriigi kuvandi, ent kahetsusväärselt lahendatakse alles nüüd haldustrahviga seonduvat probleemi. Riigi suhtumine andmekaitsesse kandub üle ka neile, kes peavad seadust täitma. Kui riik suhtub ise andmekaitse panustamisse tunduvalt leigemalt, kui näiteks tehnilisse innovatsiooni, siis on keeruline oodata innukamat suhtumist andmekaitse nõuete täitmisse ka ettevõtjatelt.

THE TRANSFER OF DATA CONCERNING HEALTH TO THIRD PARTIES THROUGH CONSENT SERVICE AND RELATED DATA PROTECTION ISSUES

SUMMARY

The main objective of this master thesis was to analyze the data processing risks associated with the consent service and to assess whether the restrictions under the General Data Protection Regulation (GDPR) are sufficient to mitigate them or whether additional national restrictions would be necessary under Article 9 (4) of the GDPR. The consent service is a new innovative service developed by the Information System Authority of Estonia (RIA) for private sector companies that do not have a legal basis to access data from the national Health Information System and who would like to provide services to individual's health data. However, these services would not qualify as health care services within the meaning of Article 2 of the Health Services Organisation Act.

At the beginning of the analysis, two research questions are presented. Firstly, are the safeguards arising from the GDPR sufficient to mitigate the risks of further processing by third parties who use the consent service to access data subjects health data from Estonian national databases? What kind of additional additional conditions should Estonia implement on the processing of health data by third parties on the basis of Article 9 (4) of the GDPR?

The first chapter of the thesis dealt with the concept of health data under the GDPR. Data collected in connection with the provision of healthcare is considered to be health data as well as data that indicates the risk of illness. For example, information about a natural person who has been in contact with a person who has Covid-19. The European Court of Justice has clarified that health data must be interpreted broadly. Meaning, if data are cross-referenced, then depending on the context it may become health data because it allows to understand potential health risks of an individual.

The first chapter addressed additionally the innovation concerning health data and also current trends towards mHealth and personal medicine. Although the consent service is not a health care service or a service directly supporting the health care service, the purpose is to enable a natural person to use his or her personal data, including health data, for other purposes outside the health care service. In order for third parties to be able to provide services, it is also necessary to identify an appropriate legal basis. If, the data subject gives his or her consent through the consent service, the purpose of this processing is to transfer the health data from the Estonian national database to third party. Secondly, the data subject gives his or her consent to the third party for the provision of specific health data-based services. The analysis considered whether a service based on health data could be provided on the basis of consent if accompanied by a contract. As the provision in Article 9 (2) of the GDPR overrules the Article 6 of the GDPR, the legal ground specified in Article 6 (1) (b) cannot be used. However, the need to process health data should be assessed under Article 7 (4) of the GDPR. It was concluded that in the case of a service where health data is an integral part of the basic service and not merely ancillary, the condition of "necessity" in the Article 7 (4) of the GDPR is met and the admissibility and validity of the consent should be upheld.

It has been further analyzed whether the data subject can give his consent to the controller of the national database, because according to the GDPR, due to the unequal situation of the parties, consent cannot generally be considered as a valid legal basis in public sector. However, consent in the public sector is not completely ruled out. In particular, if it can be said that it is a convenience service and the following conditions are met: the data subject can freely decide whether or not to consent, the data subject has an alternative to use another solution to achieve the same or a similar result; not consenting results in direct damage or indirect damage in the form of an infringement of fundamental rights by the public sector to a large group or to society as a whole. For example, in the case of the corona mobile application, the legal literature has found that the former two should be answered “no” and the latter one relates to a strong violation of fundamental rights, i.e has a detrimental effect in the form of a general restriction on free movement. Therefore, a consent to use mobile application which is in fact used to control a pandemic should not be considered a valid consent. In the case of the consent service, in author's opinion, each condition could be answered “yes”, and thus the consent should be considered as an acceptable legal basis within the consent service.

The second chapter discussed the potential risks associated with the consent service as it provides health data collected by the state to private sector companies, except for health care providers or other service providers who have access to data in the Estonian Health Information System. Such companies do not currently have any additional restrictions or conditions on highly sensitive health data that needs adequate protection.

One of the most important condition for health data is that third parties should comply with a specific processing purpose and that consent should be explicit for each processing purpose. In practice, however, there are cases where the data subject is asked to consent several processing purposes at once. Often too general processing purposes are used and overshadowed by the increasingly problematic sale of data to data brokers. It was also considered if consent service renders any issues with insurers and creditors. Could it be said that the consent to transfer health data to assess creditworthiness or insurance risk of a voluntary insurance contract is freely given. Especially considering the possible counter-offer in the form of a more favorable price. The fact that personal data is treated as a new asset class has long been discussed and there are also different views in the legal literature. However, the protection of personal data is one of the fundamental human rights and thus cannot be monetized. European Data Protection Board has compared the existence of a market for personal data to the sale of human organs, for which there is a market, but this does not mean it should be legally permissible.

Next, the potential of illegal processing of a child's health data was briefly analysed. As the GDPR does not allow minors to give their independent consent for processing health data, children should not be allowed to give their consent through the consent service. However, if this is desired, the possibility of consent being given by the children's legal representatives must be ensured. Consequently, third party should ensure that the legal representative of the child consents to further processing of the data received from the national database. Simply by checking a box to confirm the age or consent of the legal representative is not a sufficient measure to identify one’s age as it allows easy forgery.

The risks of the data subject's low awareness may result in unexpected consequences. For example, a data subject withdraws his or her consent for transfer from the processor of the

Estonian national database, but does not revoke its consent from the third-party. If the desire is to stop only the transmission and the service can be provided without continuous data exchange, then there are no issues. However, a problem arises in a situation where the data subject actually wanted to stop using the service - someday an unpleasant surprise emerges and the service provider continues to process his or her data by selling it to data brokers. Secondly, due to the low awareness by the data subjects they might consent to conditions which allow third parties to transfer their health data to third countries for which no decision on the adequacy of data protection has been issued by the European Commission. A problem may be that data subjects do not know what the transfer entails and thus do not consider it a problem.

Lastly, the risk related to the security of health data has been analyzed as well as risks related to the poor implementation of anonymisation techniques. The first is a significant risk, as insufficient security can lead to access to health data by persons with no legal basis for it and who seek to derive economic benefits from it, thereby causing material or immaterial damage to the data subject. The most harmful of these are scenarios about serious or fatal illness or scenarios that result in long-term identity theft. According to Estonian statistics the latter is a growing trend, also globally. The same can be said for data leaks and other cyber incidents. Data anonymization is associated with the growing problem of big data processing, and the fact that completely anonymous data does not really exist. Although the GDPR does not require an absolute approach to achieve anonymity, rather consider reasonable efforts to identify a person. The scientific literature has thoroughly analyzed a number of cases where it was possible to identify several individuals from anonymous data, as well as some individuals indirectly and thus raised several concerns around it.

The third chapter of the thesis gives first an overview of the existing restrictions arising from the GDPR, which in the context of the processing of health data are important for further processing by third parties. Next, the adequacy of the existing restrictions was assessed and it was concluded that not all risks covered in the second chapter of this thesis could be effectively mitigated and that the existing safeguards in the GDPR alone are not sufficient. With a few exceptions such as low awareness, which could be addressed through more systematic communication by the Supervisor.

Thirdly, Chapter three analyzes the data protection laws in force in Latvia, Finland, Sweden and the United Kingdom. In conclusion, the data protection legislation of all these countries contains at least some additions and clarifications to Article 9 (b) - (j) of the GDPR. However, only in the case of Finland would the restrictions apply to a third party who processes the data subject's health data under consent and outside the provision of healthcare. Although Latvia and the United Kingdom have additional conditions for the processing of health data by a third party, consent would not be the legal basis for processing. Sweden has clarified the grounds for processing under Article 9 of the GDPR insofar as it is needed due to the GDPR, but has not imposed any further restrictions on the processing of health data by third parties. Given that there is no national solution similar to consent in the analyzed countries, it is understandable that there are no restrictions on the processing of health data to all private companies who process health data under data subject explicit consent and not in relation to healthcare.

As the aim of this master's thesis was to understand which measures and restrictions could better prevent the realization of the risks covered in the second chapter, the last part of the third Chapter assessed possible national restrictions under Article 9 (4) of the GDPR.

One of the major shortcomings of the current situation with regard to the further processing of health data by a third party in the context of the consent service seems to be that the safeguards under the GDPR are too broad and there is lack of regular supervisory activities. Thus, the sensitivity of health data justifies the application of at least minimum mandatory requirements.

In order to specifically avoid excessive processing of health data by insurers, it is reasonable to follow the example of the Latvian Insurance Contracts Act and stipulate in Estonian Insurance Activities Act that during the term of the insurance contract, after concluding the contract, the insurer may no longer check the data subject's health data. This restriction should apply at least in the case of voluntary insurance contracts in order to avoid abuse of data processing, as in the case of health insurance contracts unexpected deterioration of health

after the conclusion of the contract should not be considered a possible increase in insurance risk according to the article 443 of the Law of Obligations.

Due to the sensitivity of health data, it is justified to implement at least the following minimum mandatory requirements set out in the Estonian Personal Data Protection Act (PDPA):

The third party who joins the consent service and processes the data subject's health data undertakes to:

1) implement measures to increase the competence of personnel processing personal data;
2) establish internal rules to ensure the security of data processing operations, including their regular testing, in order to assess the effectiveness of measures to ensure the security of data processing;
3) establish internal rules to ensure compliance with the General Data Protection Regulation when transferring personal data, including health data, or processing personal data for other purposes;
4) draw up an overview of the data processing operations in accordance with Article 30 of the GDPR and implement measures to verify and identify at any time the person who has stored, modified, viewed or transmitted personal data, including where they have been transmitted (audit log);
5) carry out and submit to Estonian Data Protection Inspectorate (EDPI) assessment of the risks of data processing and an assessment of the measures taken to mitigate them in accordance with Article 35 of the GDPR (data protection impact assessment);
6) appoint a data protection officer;
7) to carry out and submit to the EDPI the result of the data protection compliance audit, on the basis of which the company's personal data system, including documentation regarding the compliance with the requirements set out in the GDPR, has been assessed;
8) carry out and submit to the EDPI annually a data protection readiness audit based on the company's daily and actual data processing practices, including the provisions of the overview of processing operations, and their compliance with the company's established internal data protection procedures and personal data processing procedures;

9) implement appropriate privacy technologies for the pseudonymisation and anonymisation of personal data, taking into account the relevant instructions of the Supervisory Authority (EDPI or European Data Protection Board - EDPB) and the requirements of Articles 25 and 32 of the GDPR to ensure the security of personal data;
10) ensure the same or a higher level of security for the storage, transfer to third parties and other processing of personal data, including health data, than the national database from which the health data have been transferred to the third party;
11) apply strong authentication requirements to data subject who uses the health data-based service, ie a method based on the use of at least two security elements that operate independently and ensure the confidentiality of authentication data, which are known or possessed only by the data subject or can only be attributed to him or her.

The choice of appropriate requirements has taken into account the need to maintain the same or a higher level of security for health data; data protection by design and by default requirements must be applied to the processing of health data in order to ensure maximum transparency for data subjects; consents must be specific, unambiguous and clear and must be given separately for each purpose; and it is necessary to establish clear guidelines for the use of data privacy technologies, including anonymisation technologies; Health data-based services should implement strong authentication for the customer in order to prevent unauthorized access to the customer's user profile by unauthorized persons, including the company's own employees, as well as to verify the age of the data subject. In addition, the selection of protective additional measures took into account the limitations imposed by Member States' data protection law under Article 9 (4) of the GDPR.

The previous analysis showed that current measures are not enough to mitigate the risks associated with the further processing of health data by a third party and thus possible national restrictions under Article 9 (4) of the General Data Protection Regulation were analyzed. One of the key responsibilities is for the company should be to carry out a data protection impact assessment, to carry out regular data protection audits and to report the result to the Authority. In addition to these, keep record of the processing activities. These are realistic measures by which one could manage its data protection risks and prevent personal data breaches. If the company has not identified the processing activities performed within the company and has

not assessed the risks involved nor the impact on the rights and obligations of data subjects, it is not possible to adequately assess the need for appropriate technological protection measures. Also, by not compiling an overview of processing records, it is difficult for a company to distinguish between different purposes of data processing and to choose a suitable legal basis. Therefore, it can be expected that these measures would effectively mitigate the risks outlined in the second chapter of the thesis.

According to the General Data Protection Regulation, each controllers must apply data protection by design and by default, which means the companies using the consent service must also fully implement these principles. Estonia has created a strong image as a digital state, but unfortunately the problem of administrative fines under the General Data Protection Regulation is only now being solved. The state's attitude towards data protection passes on to those who have to comply by the law. If the state itself is much more lenient about contributing to data protection than to technical innovation, it is difficult to expect a more enthusiastic attitude to comply with data protection requirements from the companies.

LÜHENDID

AKI	Andmekaitse Inspektsioon
API	*Application Programming Interface*
CNIL	*Commission Nationale de l'Informatique et des Libertés* (Prantsusmaa andmekaitseasutus)
EDPB	*European Data Protection Board* (Euroopa Andmekaitsenõukogu)
EDPS	*European Data Protection Supervisor* (Euroopa Andmekaitseinspektor)
EIK	Euroopa Inimõiguste Kohus
EL	Euroopa Liit
FRA	*European Union Agency for Fundamental Rights* (Euroopa Liidu Põhiõiguste Amet)
GPEN	*Global Privacy Enforcement Network* (üleilmne andmekaitse võrgustik)
ICO	*Information Commission Officer* (Ühendkuningriigi andmekaitseasutus)
OWASP	*Open Web Application Security Project*
RIA	Riigi Infosüsteemi Amet
TIS	Tervise infosüsteem
WHO	*World Health Organization* (Maailma Tervishoiuorganisatsioon)

KASUTATUD ALLIKAD

Kasutatud kirjandus ja seaduseelnõud

1. Alexy, R. Põhiõigused Eesti põhiseaduses. - Juridica 2001, eriväljaanne.
2. Banerjee, A., Joshi, K.P. Link before you share: Managing privacy policies through blockchain. 2017 IEEE International Conference on Big Data (Big Data), 2017, pp. 4438-4447. Kättesaadav: https://www.researchgate.net/publication/320357405_Link_Before_You_Share_Managing_Privacy_Policies_through_Blockchain (28.04.2021).
3. Bock, K., Kühne, C.R. jt, Data Protection Impact Assessment for the Corona App. 29.04.2020. Kättesaadav: https://ssrn.com/abstract=3588172 (28.04.2021).
4. Bogdanov, D., Siil, T. (2018a). Anonymisation 2.0: Sharemind as a Tool for De-Identifying Personal Data –Part 1: Definitions. Cybernetica. 17.08.2018.Kättesaadav: https://sharemind.cyber.ee/anonymisation-2_0-part-1-definitions/ (28.04.2021).
5. Bogdanov, D. Sillaste, T. Infotehnoloogilised võimalused põhiõiguste kaitsel. - Juridica 2020/6.
6. Dash, S., Shakyawar, S.K., Sharma, M. et al. Big data in healthcare: management, analysis and future prospects. J Big Data 6, 54 (2019). Kättesaadav: https://doi.org/10.1186/s40537-019-0217-0 (28.04.2021).
7. Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus Euroopa andmehalduse kohta (andmehaldust käsitlev õigusakt). Brüssel 25.11.2020. COM(2020) 767 final. 2020/0340 (COD). Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52020PC0767 (28.04.2021).
8. Euroopa Komisjon. Ettepanek: Euroopa Parlamendi ja Nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus). Brüssel: 2012. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52012PC0011&from=ET (28.04.2021).

9. Euroopa Komisjon. Roheline Raamat mobiilse tervishoiu ehk m-tervise kohta. Eestikeelne väljaanne. Brüssel, 10.04.2014. Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex%3A52014DC0219 (28.04.2021).

10. European Union Agency for fundamental rights and Council of Europe. Handbook on European Data Protection Law, 2018 edition. Luxembourg: Publications Office of the European Union, 2018. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (28.04.2021).

11. Feiler, L., Forgó, N., Weigl, M. The EU General Data Protection Regulation (GDPR): A Commentary. German Law Publishers 2018.

12. Gercke, M. Internet-related identity theft. A discussion paper. Project on Cybercrime. Counsil of Europe. 22.11.2007. Kättesaadav: https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/internet-related-identity-theft%E2%80%93a-discussion-paper.pdf (28.04.2021).

13. Gliklich, R.E., Leavy, M.B., Dreyer, N.A., (eds). Tools and Technologies for Registry Interoperability, Registries for Evaluating Patient Outcomes: A User's Guide, 3rd Edition, Addendum 2. (Prepared by L&M Policy Research, LLC under Contract No. 290-2014-00004-C.) AHRQ Publication No. 19(20)-EHC017-EF. Rockville, MD: Agency for Healthcare Research and Quality. October 2019. Kättesaadav: https://www.ncbi.nlm.nih.gov/books/NBK551879/pdf/Bookshelf_NBK551879.pdf (28.04.2021).

14. Gutwirth, S., Leenes, R. De Hert, P. Data Protection on the Move: Current developments in ICT and Privacy/ Data Protection. Springer 2016.

15. Haldustrahviõiguse kontseptsioon. 05.05.2020. Kättesaadav: https://eelnoud.valitsus.ee/main#VZU4bXWV (28.04.2021).

16. Haldustrahvimenetluse seaduse eelnõu seletuskiri, 19.08.2020. Kättesaadav: https://eelnoud.valitsus.ee/main#afLdD2q3 (28.04.2021).

17. Hallituksen esitys HE 9/2018 vp. (Soome valitsuse ettepanek parlamendile õigusaktide kohta, mis täiendavad ELi üldist andmekaitse määrust). 01.03.2018. Kättesaadav:

https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx (28.04.2021).

18. Hon, W. K., Millard, C., Walden, I., The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated? The Cloud of Unknowing, Part 1 (March 10, 2011). International Data Privacy Law (2011) 1 (4): 211-228, Queen Mary School of Law Legal Studies Research Paper No. 75/2011. Kättesaadav: https://ssrn.com/abstract=1783577 (28.04.2021).

19. Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. - Juridica 2002, nr VII.

20. Isikuandmete kaitse seaduse eelnõu seletuskiri, SE 679, 22.08.2018. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5c9f8086-b465-4067-841e-41e7df3b95af (28.04.2021).

21. Karistusseadustiku eelnõu seletuskiri, SE 530, 11.06.2009. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/2b386832-b657-ab0c-fb52-de02708302bc/Karistusseadustiku%20muutmise%20seadus (28.04.2021).

22. Koll, K. Vastutustundliku laenamise põhimõte. Kättesaadav: https://www.just.ee/sites/www.just.ee/files/kristiina_koll._vastutustundliku_laenamise_pohimote.pdf (28.04.2021).

23. Korff, D. New Challenges to Data Protection Study - Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments. 15.01.2010. European Commission DG Justice, Freedom and Security Report. Kättesaadav: https://ssrn.com/abstract=1638949 (28.04.2021).

24. Kuuskmaa, L. M. Isikuandmete töötlemise õiguslik alus ning andmesubjekti õiguste kaitse tervise infosüsteemi kogutud terviseandmete kasutamisel kliiniliste otsuste tugisüsteemide arendamiseks ja rakendamiseks. Magistritöö. Tartu Ülikool. Õigusteaduskond. Tartu 2020. Kättesaadav: http://hdl.handle.net/10062/68545 (28.04.2021).

25. Mcdonald, M. A, Cranor, F. L. The Cost of Reading Privacy Policies. - I/S: A Journal of Law and Policy for the information society. Vol. 4:3 2008.

26. Neto, N.N., Madnick, S., de Paula, M. G., Borges, N. M. A Case Study of the Capital One Data Breach. Working Paper CISL# 2020-16. 01.03.2020. Kättesaadav:

https://ssrn.com/abstract=3570138 (28.04.2021).

27. Nimmo, M., Identiteedivarguse piiritlemine solvamisest ja laimamisest Eesti õigussüsteemis. - Juridica 10/2017.

28. Nisu, N. Eesti tarbija kui andmesubjekti õiguste kaitse mobiilirakenduse poolt isikuandmete kasutamisel – Endomondo näitel. Magistritöö. Tartu Ülikool 2017. Kättesaadav: https://dspace.ut.ee/bitstream/handle/10062/56497/nisu_ma_2017.pdf?sequence=1&isAllowed=y (28.04.2021).

29. Nõmper, A., Tikk, E. Informatsioon ja õigus, Juura 2007.

30. Oprysk, L. The Forthcoming General Data Protection Regulation in the EU: Higher Compliance Costs Might Slow Down Small and Medium-sized Enterprises' Adoption of Infrastructure as a Service. - Juridica International. Law Review. University of Tartu, 24/2016. pp 23-31.

31. Pormeister, K. Informed consent to sensitive personal data processing for the performance of digital consumer contracts on the example of "23andMe". Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht, 6 (1), 17−23. 2017.

32. Preliminary Impact Assessment Report of the Draft Law "Personal Data Processing Law" (annotation), Riia. 14.03.2018. This is the annotation to Personal data processimg law. Kättesaadav: http://titania.saeima.lv/LIVS12/SaeimaLIVS12.nsf/0/C74799DB57161C61C225825000483C5F?OpenDocument#b (28.04.2021).

33. Riigikogu toimetised. - Riigikogu kantselei väljaanne, RiTo 42/2020. Kättesaadav: https://rito.riigikogu.ee/wordpress/wp-content/uploads/2020/12/RiTo_42.pdf (28.04.2021).

34. Sein, K., Mikiver, M., Tupay, P. K. Pilguheit andmesubjekti õiguskaitsevahenditele uues isikuandmete kaitse üldmääruses. - Juridica 2/2018.

35. Spindler, G., Schmechel, P. Personal Data and Encryption in the European General Data Protection Regulation. – Journal of Intellectual Property, Information Technology and E-Commerce Law, 163(7), 2016. Kättesaadav: https://www.jipitec.eu/issues/jipitec-7-2-2016/4440 (28.04.2021).

36. Sweeney, L. Matching Known Patients to Health Records in Washington State Data.

Harvard University. Data Privacy Lab. White Paper 1089-1. June 2013. Kättesaadav: https://dataprivacylab.org/projects/wa/1089-1.pdf (28.04.2021).

37. Sweeney, L. Patient Identifiability in Pharmaceutical Marketing Data. Data Privacy Lab Working Paper 1015. Cambridge 2011. Kättesaadav: https://dataprivacylab.org/projects/identifiability/pharma1.pdf (28.04.2021).

38. Sweeney, L. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. Kättesaadav: https://dataprivacylab.org/projects/identifiability/paper1.pdf (28.04.2021).

39. Truong, N.B etc. GDPR - Compliant Personal Data Management: A Blockchain-based Solution. IEEE Transaction On Information Forensics And Security, 03.10.2019. Kättesaadav: https://arxiv.org/pdf/1904.03038.pdf (28.04.2021).

40. Varul, P., Kull, I. Kõve, V., Käerdi. M. Sein, K. Võlaõigus II. Kommenteeritud väljaanne. Juura. Tallinn, 2019.

41. Vicente, D. M., Casimiro, S. de V. Data Protection in the Internet. Springer 2020.

Kasutatud normatiivaktid

42. Apdrošināšanas līguma likums (Läti kindlustuslepingu seadus). Latvijas Vēstnesis, 97, 18.05.2018. Kättesaadav: https://likumi.lv/ta/en/en/id/299053-insurance-contract-law (28.04.2021).

43. Data Protection Act 2018. United Kingdom. 23.05.2018. Kättesaadav: https://www.legislation.gov.uk/ukpga/2018/12/data.pdf (28.04.2021).

44. De cohesión y calidad del Sistema Nacional de Salud (Hispaania seadus nr 16/2003 riikliku tervishoiusüsteemi ühtekuuluvuse ja kvaliteedi kohta), artikkel 57. Kättesaadav: https://www.boe.es/eli/es/l/2003/05/28/16/con (28.04.2021).

45. Euroopa Liidu Põhiõiguste Harta. - ELT C 326/02 2012, lk 391-407.

46. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281/31, 23.11.1995.

47. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste

isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, lk 1-88.

48. Fizisko personu datu apstrādes likums (Läti andmekaitseseadus). Latvijas Vēstnesis, 132, 04.07.2018. Kättesaadav: https://likumi.lv/ta/en/en/id/300099 (28.04.2021).

49. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191, 104th Congress. Kättesaadav: https://www.congress.gov/bill/104th-congress/house-bill/3103/text (28.04.2021).

50. Infosüsteemide andmevahetuskiht, määrus. - RT I, 06.08.2019, 17…RT I, 06.08.2019, 6.

51. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. - RT II 2001, 1, 3.

52. Isikuandmete kaitse seadus. - RT I 2007, 24, 127…RT I, 06.01.2016, 1.

53. Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.

54. Karistusseadustik. - RT I 2001, 61, 364...RT I, 03.03.2021, 3.

55. Kindlustustegevuse seadus. RT I, 07.07.2015, 1...RT I, 04.12.2019, 8.

56. Krediidiasutuste seadus. - RT I 1999, 23, 349...RT I, 04.01.2021, 33.

57. Küberturvalisuse seadus. - RT I, 22.05.2018, 1.

58. Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (Rootsi andmekaitseseadus). Välja antud: 19.04.2018. Kättesaadav: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218 (28.04.2021).

59. Portaria n.º 981/95 (Portugali tervishoiu ministri määrus number 981/95). 01.08.1995. Kättesaadav: https://dre.pt/web/guest/pesquisa/-/search/477871/details/normal?q=N%C3%BAmero+de+utente+da+Sa%C3%BAde (28.04.2021).

60. Rahapesu ja terrorismi rahastamise tõkestamise seadus. - RT I, 17.11.2017, 2...RT I, 14.04.2021, 6.

61. Tervishoiuteenuste korraldamise seadus. - RT I 2001, 50, 284...RT I, 17.05.2020, 13.

62. Tervise infosüsteemi põhimäärus. - RT I, 06.12.2016, 11...RT I, 26.02.2021, 31.

63. Tietosuojalaki (Soome andmekaitseseadus). 5/5/2018/1050. Kättesaadav: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050 (28.04.2021).

64. Tsiviilseadustiku üldosa seadus. - RT I 2002, 35, 216 ... RT I, 23.05.2020, 2.

65. Vakuutussopimuslaki (Soome kindlustuslepingu seadus). 28.6.1994/543. Kättesaadav:https://www.finlex.fi/fi/laki/ajantasa/1994/19940543 (28.04.2021).

66. Võlaõigusseadus. - RT I 2001, 81, 487...RT I, 04.01.2021, 2.

Kasutatud kohtulahendid

67. EKo C-362/14, *Maximillian Schrems versus Data Protection Commissioner,* ECLI:EU:C:2015:650

68. EKo C-311/18, *Data Protection Commissioner versus Facebook Ireland Ltd, Maximillian Schrems,* ECLI:EU:C:2020:559

69. EKo C-101/01, *Bodil Lindqvist v Åklagarkammaren i20 Jönköping,* ECLI:EU:C:2003:596

Järelevalve otsused

70. Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr 2.1.-6/20/31, 07.10.2020. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).

71. Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr 2.1.-6/20/27, 07.08.2020. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).

72. Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr. 2.1.-6/20/25, 20.07.2020. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).

73. Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr 2.1.-

6/20/21, 08.05.2020. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).

74. Andmekaitse Inspektsioon. Ettekirjutus-hoiatus isikuandmete kaitse asjas nr. 2.1.-6/20/20, 30.04.2020. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).

75. Vaideotsus avaliku teabe asjas nr 2.1-3/20/4685, Andmekaitse Inspektsioon, 03.02.2021. Kättesaadav: https://www.aki.ee/et/inspektsioon-kontaktid/menetlusotsused/ettekirjutused (28.04.2021).

Kasutatud muu materjal

76. Administrative criminal proceedings of the Austrian data protection authority against Österreichische Post AG (Austrian Postal Service), 23.10.2019. Kättesaadav: https://edpb.europa.eu/news/national-news/2019/administrative-criminal-proceedings-austrian-data-protection-authority_en (28.04.2021).

77. Andmekaitse Inspektsioon. Isikuandmete töötleja üldjuhend. 19.03.2019. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf (28.04.2021)

78. Andmekaitse Inspektsioon. Isikuandmete töötlemine töösuhetes. Abistav juhendmaterjal. Tallinn 26.05.2014. Kättesaadav: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Isikuandmed%20t%C3%B6%C3%B6suhetes%20juhendmaterjal26%2005%202014_0.pdf (28.04.2021).

79. Andmekaitse Inspektsioon. Kantavad seadmed ja privaatsus. Juhis organisatsioonidele ja kodukasutajale seaduse rakendamisel. 09.11.2015. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/juhis-kantavad_seadmed_ja_privaatsus.pdf (28.04.2021)

80. Artikli 29 alusel asutatud andmekaitse töörühm. Arvamus 05/2014 anonüümimistehnikate kohta. Vastu võetud 10. aprillil 2014. Kättesaadav: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/

2014/wp216_et.pdf (28.04.2021)

81. Artikli 29 alusel asutatud andmekaitse töörühm. Suunised määruse (EL) 2016/679 kohase nõusoleku kohta. Vastu võetud 28.11.2017. Viimati muudetud ja muudatused vastu võetud 10. aprillil 2018. Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_nousoleku_kohta_wp259_rev_0.1_et.pdf (28.04.2021)

82. Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013. Kättesaadav: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (28.04.2021)

83. Andmekaitseinspektsioon. Avaliku teabe seaduse täitmisest ja isikuandmete kaitse tagamisest aastal 2018. Soovitused aastaks 2019. Kättesaadav: https://issuu.com/andmekaitse/docs/aastaraamat_2018_kohta._soovitused_ (28.04.2021).

84. Andmekaitse Inspektsiooni veebileht. Statistika. Kättesaadav: https://www.aki.ee/et/teavitus-uudised/statistika (28.04.2021).

85. Compensa Life Vienna Insurance Group SE. Privaatsusteade. Kättesaadav: https://www.compensalife.eu/EE/show.asp?docID=public.company.privacy (28.04.2021).

86. Council of Europe Committee of Ministers. On the protection of Medical Data, Recommendation R (97) 5, 13.02.1997. Kättesaadav: https://rm.coe.int/16804f0ed0 (28.04.2021)

87. E-tervise visioon 2025. E-tervise strateegiline arenguplaan 2020. Riigikantselei. Koostatud 2015. Kättesaadav: https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Eesti_e_tervise_strateegia/e-tervise_strateegia_2020.pdf (28.04.2021).

88. EDPB-EDPS joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act). Kättesaadav: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-edps_joint_opinion_dga_en.pdf (28.04.2021)

89. Eesti infoühiskonna arengukava 2020. Vabariigi Valitsus, uuendatud 2018

Kättesaadav: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2020.pdf (28.04.2021).

90. Euroopa Andmekaitsenõukogu – täiskogu 42. istungjärk. 20.11.2020. Kättesaadav: https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en%C2%A0_et (28.04.2021).

91. Euroopa Andmekaitsenõukogu ja Euroopa Andmekaitseinspektori ühisarvamus 1/2021, milles käsitletakse Euroopa Komisjoni rakendusotsust vastutavate töötlejate ja volitatud töötlejate vaheliste lepingute tüüptingimuste kohta määruse (EL) 2016/679 artikli 28 lõikes 7 ja määruse (EL) 2018/1725 artikli 29 lõikes 7 osutatud küsimustes. EDPB. Kättesaadav: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-12021-standard_et (28.04.2021)

92. Euroopa Andmekaitsenõukogu. Suunised 3/2020 terviseandmete töötlemise kohta teadusuuringute eesmärgil seoses COVID-19 puhanguga. 21.04.2020. Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/edpb_guidelines_202003_suunised_3_2020_terviseandmete_tootlemise_kohta.pdf (28.04.2021)

93. European Data Protection Supervisor. Opinion 4/2017 ton the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content. Kättesaadav: https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf (28.04.2021)

94. European Parliament. Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law? Study Panel for the Future of Science and Technology. European Parliamentary Research Service. July 2019. Kättesaadav: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (28.04.2021).

95. Euroopa Komisjoni andmekaitse taseme piisavuse otsused. Kättesaadav: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_et (28.04.2021).

96. European Union Agency for Fundamental Rights (FRA) (2020), Your rights matter:

Data protection and privacy, Fundamental Rights Survey. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf (28.04.2021).

97. Finantsinspektsiooni soovituslik juhend. Vastutustundliku laenamise nõuete kohta. Tallinn 13.06.2016. Kättesaadav: https://www.fi.ee/et/juhendid/banking-and-credit/vastutustundliku-laenamise-nouded (28.04.2021).

98. Fitbit help manuals. Kättesaadav: https://bit.ly/39JNIXn (28.04.2021).

99. Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*. 24.07.2020. https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_et.pdf (28.04.2021)

100. FTC. Medical Identity theft. January 2011. https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (28.04.2021).

101. Global strategy on digital health 2020-2025. World Health Organization. Kättesaadav: https://cdn.who.int/media/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d_02adc66d-800b-4eb5-82d4-f0bc778a5a2c.pdf?sfvrsn=f112ede5_68 (28.04.2021).

102. GPEN Sweep 2018 'Privacy Accountability' October 2018. Office of the Privacy Commissioner, New Zealand, Information Commissioner's Office, UK. Kättesaadav: https://ico.org.uk/media/about-the-ico/documents/2614435/gpen-sweep-2018-international-report.pdf (28.04.2021)

103. Hamm, N. New Federal Patient Health Data Sharing Rules: The Tradeoffs Between Access and Privacy Protections. Bipartisan Policy Center. 30.03.2020. Kättesaadav: https://bipartisanpolicy.org/blog/new-federal-patient-health-data-sharing-rules-the-tradeoffs-between-access-and-privacy-protections/ (28.04.2021).

104. Hodson, H. Revealed: Google AI has access to huge haul of NHS patient data. - NewScientist. 26.01.2016. Kättesaadav: https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-

haul-of-nhs-patient-data/ (28.04.2021).

105. In-Cyprus, Doctor fined €14,000 for revealing personal data of patient on Instagram. 11.10.2019. Kättesaadav: https://in-cyprus.philenews.com/doctor-fined-e14000-for-revealing-personal-data-of-patient-on-instagram/ (28.04.2021).

106. Information Commissioner's Office. Consultation: GDPR consent guidance. - ICO, 02 March 2017-31 March 2017. Kättesaadav: https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf (28.04.2021).

107. Kuritegevus Eestis 2017. Kriminaalpoliitika uuringud. Justiitsministeerium. Tallinn 2017, lk 144. Kättesaadav: https://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevuseestis_2017_veebi01.pdf (28.04.2021).

108. Küberturvalisuse aastaraamat 2021. Riigi Infosüsteemi Amet. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2021.pdf (28.04.2021).

109. MediKeep ravimikapi teenus. Kättesaadav: https://medikeep.eu/termsofuse/ (28.04.2021).

110. McDougall, S. Blog: ICO Adtech update report published following industry engagement. 20.06.2019. Kättesaadav: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/ (28.04.2021).

111. Murgia, M., Harlow, M. How top health websites are sharing sensitive data with advertisers. - Financial Times. 13.11.2019. Kättesaadav: https://www.ft.com/content/0fbf4d8e-022b-11ea-be59-e49b2a136b8d (28.04.2021).

112. Nõusolekuteenuse analüüs. Analüüsi aruanne, Ernst & Young 05.02.2021

113. OWASP Top 10 Privacy Risks 2014 ja 2021. Kättesaadav: https://docs.google.com/spreadsheets/d/1GstkaCzO7_ok1p4rr1drq0SuPLjg5MlkshG5oS58vAY/edit#gid=0 (28.04.2021).

114. Peep, V. Kas isikuandmete kaitse üldmäärus toob tõesti kaasa hiigeltrahvid? 15.11.2017. Kättesaadav: https://www.aki.ee/et/uudised/kas-isikuandmete-kaitse-

uldmaarus-toob-toesti-kaasa-hiigeltrahvid (28.04.2021).

115. Personal Data: The Emergence of a New Asset Class. An Initiative of the World Economic Forum. January 2011. In Collaboration with Bain & Company, Inc, lk, 32. Kättesaadav: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf (28.04.2021).

116. Practical problems in processing medical information under the GDPR. 11.08.2017. Kättesaadav: https://kennedyslaw.com/thought-leadership/article/practical-problems-in-processing-medical-information-under-the-gdpr/ (28.04.2021).

117. Pärgmäe, R. jt. Õiguse ja eetika vaade Vabariigi valitsuse e-tervise strateegias aastani 2020. Õiguse ja eetika töörühma raport 2015. Kättesaadav: https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Eesti_e_tervise_strateegia/oiguse_ja_eetika_tooruhma_raport.docx (28.04.2021).

118. Riigi Infosüsteemi Ameti aastaraamat 2020. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_48lk_est_veeb.pdf (28.04.2021).

119. Soomlaste vaimse tervise andmed lekkisid taas internetti. - Eestinen. 27.01.2021. Kättesaadav: https://eestinen.fi/2021/01/soomlaste-vaimse-tervise-andmed-lekkisid-taas-netti/ (28.04.2021).

120. Registreeritud kuriteod jaanuar-mai 2016-2020. Baromeeter. Justiitsministeeriumi kriminaalpoliitika osakonna võrgukodu. Kättesaadav: https://www.kriminaalpoliitika.ee/et/statistika-ja-uuringud/kuritegevuse-baromeeter (28.04.2021).

121. Riigi vastu toimusid küberründed, kätte saadi 9158 koroonapatsiendi andmed. 01.12.2020. Kättesaadav: https://www.err.ee/1192309/riigi-vastu-toimusid-kuberrunded-katte-saadi-9158-koroonapatsiendi-andmed (28.04.2021).

122. ScanWatch. Kättesaadav: https://support.withings.com/hc/en-us/articles/360015551577-ScanWatch-Regulatory-statement (28.04.2021).

123. Steger, A. What happens to stolen Healthcare Data? HealthTech magazine. 30.10.2019. Kättesaadav: https://healthtechmagazine.net/article/2019/10/what-

happens-stolen-healthcare-data-perfcon (28.04.2021).

124. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. 21.01.2019. Kättesaadav: https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc (28.04.2021).

125. The General Data Protection Regulation – one year on Civil society: awareness, opportunities and challenges. European Union Agency for Fundamental Rights, 2019. Kättesaadav: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-gdpr-one-year-on_en.pdf (28.04.2021).

126. The OECD Privacy Framework. 2013. Kättesaadav: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (28.04.2021).

127. Tumeveebis tehakse äri võltsitud vaktsineerimistõenditega. Postimees. 26.03.2021. Kättesaadav: https://tervis.postimees.ee/7211071/tumeveebis-tehakse-ari-voltsitud-vaktsineerimistoenditega (28.04.2021).

128. WHO Global Observatory for eHealth. mHealth: new horizons for health through mobile technologies: second global survey on eHealth. World Health Organization. 2011 Kättesaadav: https://apps.who.int/iris/bitstream/handle/10665/44607/9789241564250_eng.pdf?sequence=1&isAllowed=y (28.04.2021).

129. Your Data Is Shared and Sold…What's Being Done About It? Wharton School, University of Pennsylvania, 28.10.2019. Kättesaadav: https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ (28.04.2021).

130. Yednak, C. Providers and payers still grapple with privacy concerns under final interoperability rules. Price Waterhouse Coopers. 13.03.2020. Kättesaadav: https://www.pwc.com/us/en/industries/health-industries/library/privacy-concerns-interoperability-rules-3-13-20.html (28.04.2021).

Litsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Katri Remmelgas,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

   „Terviseandmete edastamine nõusolekuteenuse kaudu kolmandatele isikutele ja sellega kaasuvad andmekaitseõiguslikud küsimused“,

   mille juhendaja on *dr iur* Karin Sein,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace´i lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Tallinn, 28.04.2021