TALLINNA TEHNIKAÜLIKOOL

Majandusteaduskond

Õiguse instituut

Priit Davel

PROAKTIIVSETE TEENUSTE ANDMETÖÖTLUSE KODANIKULE NÄHTAVAMAKS MUUTMINE

Magistritöö

Õppekava HAJM08/15, Eesti avalik ja eraõigus

Juhendaja: Kristi Joamets, PhD

Tallinn 2020

Deklareerin, et olen koostanud lõputöö iseseisvalt ja
olen viidanud kõikidele selle koostamisel kasutatud
teiste autorite töödele, olulistele seisukohtadele ja andmetele,
ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on 15 631 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Priit Davel

.....

(allkiri, kuupäev)

Üliõpilase kood: 162915HAJM

Üliõpilase e-posti aadress: priit@davel.ee

Juhendaja: Kristi Joamets, PhD:

Töö vastab kehtivatele nõuetele

.....

(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:

Lubatud kaitsmisele

.....

(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Elame ajastul, mil enamus riigi poolt pakutavad teenused on kolinud internetti ning andmete jagamine, info otsimine, edastamine ja salvestamine on saanud igapäeva lahutamatuks osaks kodanikuga suhtlemisel.

Magistritöö eesmärgiks on välja selgitada kas teenuste korraldamise ja teabehalduse alused määrus (TKTA) on kooskõlas 2016 aastal kehtestatud Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46EÜ kehtetuks tunnistamise kohta (üldmäärus), eelkõige siis kas avalike teenuste pakkumine TKTA toodud tingimustel tagab isikuandmete töötlemise läbipaistvuse.

Töös on kasutatud võrdleva kvalitatiivse analüüsi meetodit. Töös käsitletakse avaliku sektori asutuse õigusliku aluse põhimõtteid isikuandmete töötlemisel ja sellega kaasnevat teavitamise kohustust. Analüüsitakse, kas kodanikul on lihtsasti leitav tema isikuandmete töötlemisega seotud info ja kas asutused, kes lähtuvad oma teenuste pakkumisel TKTA tingimustest, täidavad seeläbi üldmääruses kehtestatud nõudeid. Töös analüüsitakse erinevaid rahvusvahelisi, Euroopa Liidu ja siseriiklikke õigusakte, kasutatakse teemaga seonduvat kirjandust ja teema kohaseid juhendeid.

Püstitatud hüpotees, et TKTA §2 lõige 3 proaktiivse teenuse osutamine asutuse omal initsiatiivil, isiku nõusolekul ja eeldataval tahtel ei ole kooskõlas üldmääruse artikkel 12 läbipaistvuse põhimõttega, leidis kinnitust. Valitsusasutused tohivad oma ülesannete täitmisel isikuandmeid töödelda ainult avalikes huvides oleva ülesande täitmiseks ja vastutava töötleja avaliku võimu teostamiseks. Seda leidu toetab ka siseriiklik avaliku teabe seadus (AvTS).

Sellest tulenevalt annab töö autor omapoolsed soovitused mida tuleks rakendada, et TKTA oleks kooskõlas üldmäärusega selles osas, mis puudutab isikuandmete töötlemist proaktiivsete teenuste pakkumisel.

Võtmesõnad: proaktiivne teenus; andmekaitse üldmäärus; andmekogu põhimäärus, andmeladu

SISSEJUHATUS

Käesoleva magistritöö eesmärgiks on välja selgitada, kas teenuste korraldamise ja teabehalduse alused määruse (TKTA) § 2 lõikes 2 sätestatud otsese avaliku teenuse ja lõikes 3 sätestatud proaktiivse teenuse pakkumine valitsusasutuste ja nende hallatavate asutuste (asutused) poolt on kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46EÜ kehtetuks tunnistamise kohta (üldmäärus). Majandus- ja Kommunikatsiooniministeerium (MKM) algatas TKTA eelnõu menetluse 25.11.2015 kui kehtis Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selle vaba liikumise kohta (direktiiv) ning selle alusel siseriiklikult vastu võetud isikuandmete kaitse seaduse (IKS) 01.01.2015 jõustunud redaktsioon[1]. Eesti Vabariigi Valitsus võttis TKTA vastu 25.05.2017 ja vastav määrus jõustus 03.06.2017. On aga oluline kohe välja tuua, et TKTA eelnõu algatamise ja selle jõustumise aja sees võeti vastu üldmäärus, mis oluliselt täiendas asutustele esitatavaid nõudeid ja kohustusi isikuandmete töötlemisel. Kuna siseriiklikud õigusaktid tuleb kooskõlla viia Euroopa Parlamendi ja nõukogu määrustega siis on töö eesmärgiks võimalike muudatusettepanekute tegemine TKTA § 2 lõike 2 ja 3 sätestatu osas, kui ilmneb, et need sätted ei vasta üldmääruses esitatud uutele nõuetele.

TKTA § 2 lõige 2 lubab asutustel otsest avaliku teenust osutada füüsilistele isikule (isik) tema eeldataval tahtel ja sarnaselt lõige 3 lubab proaktiivset teenust osutada asutuse omal inistatiivil, isikute nõusolekul või eeldataval tahtel ja riigi infosüsteemi kuuluvate andmekogude andmete alusel. Üldmäärus, millega kaitstakse isikute põhiõigusi- ja vabadusi, eriti nende õigust oma isikuandmete kaitsele, kohustab asutusi teavitama isikuid nende andmetega tehtavast igast isikuandmete töötlemisest ja vastav teave töötlemise kohta tuleb esitada kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt. Sest sellise teabe olemasolul saab isik teada tema andmete kasutamisest ja selle põhjal tekib tal ka võimalus üldmääruses isikutele omistatud õigusi teostada.[2]

---

[1] IKS redaktsiooni kehtivuse tuvastamine on vajalik, et hinnata kas TKTA eelnõu esitamise hetkel oli selles toodud tingimustel isikuandmete töötlemine kooskõlas kehtiva õigusega.

[2] Salumaa, K. (2018). Andmesubjekti õigused uue isikuandmete kaitse üldmääruse foonil. *Juridica*, 2, 83-93, 85.; Mahieu, R., van Hoboken, J., Asghari, H. (2019). Responsibility for Data protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10 (3), 85-105, 88.

Kuna üldmäärust kohaldatakse isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes ja ka automatiseerimata töötlemise suhtes, siis on asutustel väga oluline jälgida, et igasugune isikuandmete töötlemine oleks seaduslik. Seaduslikkuse tagab isiku nõusolek või tema osalusel sõlmitav ja sõlmitud leping ning asutuse juriidilise kohustuse või avalikes huvides oleva ülesande täitmine ning asutuse avaliku võimu teostamine.

Lisaks üldmääruse põhimõtetele tuleb asutusel arvestada ka kehtiva siseriikliku õigusega nagu Eesti Vabariigi põhiseaduse (PS) § 3 riigivõimu teostamine üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel ja PS § 14 õiguste ja vabaduste tagamine on seadusandliku, täidesaatva ja kohtuvõimu ning kohalike omavalitsuste kohustus. Samuti ka avaliku teabe seaduse (AvTS) § 1 tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus, lähtudes demokraatliku ja sotsiaalse õigusriigi ning avatud ühiskonna põhimõtetest, ning luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle, AvTS §28 lõige 31^1 kohustusega teha kättesaadavaks info isikuandmete töötlemise kohta ja isiku poolt enda andmetega tutvumise õigus ja kord ning AvTS $§43^1$ andmekogudes olevate andmete kasutamine on lubatud ainult seaduse või selle alusel antud õigusaktis sätestatud ülesannete täitmiseks.

Eeltoodud lähtuvalt on käesoleva magistritöö hüpoteesiks: **TKTA § 2 lõige 3 sätestatud proaktiivse teenuse osutamine asutuse omal initsiatiivil, isiku nõusolekul ja eeldataval tahtel ei ole kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 (üldmäärus) artikkel 12 läbipaistvuse põhimõttega.**

Magistritöös on kasutatud kvalitatiivse analüüsi meetodit. Töös analüüsitakse erinevaid rahvusvahelisi, Euroopa Liidu ja siseriiklikke õigusakte, kasutatakse teemaga seonduvat kirjandust ja teema kohaseid juhendeid. Antud töös käsitletav isikuandmete töötlemise kaitse hõlmab endas lisaks üldmäärusele ka AvTS-i ja selle alusel väljaantud asjakohaseid määruseid tulenevalt andmekogude kasutamisest. Õigusaktidest tulenevaid norme kontrollitakse kontrollpäringute teostusega praktikas, et veenduda kas tegelikkus vastab õigusnormidele. Samas ei uurita käesolevas töös isikuandmete töötlemist osas mis tuleneb Euroopa Parlamendi ja nõukogu direktiivist (EL) 2016/680 mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba

liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK ning ei analüüsita teenuste pakkumist isikutele erasektori poolt.

Töö on jaotatud kolmeks peatükiks. Esimeses peatükis antakse ülevaade üldmääruse kujunemisest ja tuuakse välja põhilised punktid millele tänane üldmäärus tugineb, et tagada isikuandmete kaitse. Lisaks tutvustatakse riigi poolt pakutavate teenuste põhimõtteid ning millistest andmekaitse alastest kriteeriumitest peavad asutused oma teenuste pakkumisel lähtuma. Digitaalsete andmete kasutamise õigusliku poole pealt analüüsitakse ka AvTS andmekogudega seonduvaid piiranguid.

Peatükis 2 selgitatakse proaktiivse teenuse olemus ja analüüsitakse millistel alustel tohib asutus selliseid teenuseid pakkuda. Samuti tuuakse välja proaktiivse teenuse sarnasused automatiseeritud andmetöötlusele ja sellest tulenevale kohustusele tagada isikutele teave andmete töötluse kohta. Lisaks analüüsitakse Maanteeameti juhiloa vahetuse e-teenuse ja Maksu- ja tolliameti (MTA) tuludeklaratsiooni veebipõhise andmetöötluse aluseid, et leida kinnitust proaktiivse teenusega kaasneva aruandluskohustuse täitmisest ehk kas on tagatud teenuse pakkumisel üldmääruse mõistes läbipaistvus. Peatükis 3 tuuakse välja analüüsi tulemused ja vajadusel antakse põhjendatud soovitusi hetkel kehtivate riigisiseste õigusaktide täiendamiseks. Kokkuvõttes tuuakse välja olulisemad järeldused ja soovitused, et asutused saaksid proaktiivseid teenuseid edasi pakkudes tagada läbipaistvuse.

1. PRIVAATSUS JA E-RIIK

Eesti Infoühiskonna Arengukava 2020, mis koostati 2013 aastal on ühe prioriteet projektina toodud välja, et „luuakse nii tehnoloogilised kui ka organisatoorsed tingimused selleks, et inimestel oleks alati võimalik teada ja ka suunata, kes, millal ning milleks nende riigi käes andmeid kasutab“.[3] Aastal 2020 seda arengukava lugedes saab väita, et see punkt sai täidetud aastal 2016 kui võeti vastu üldmäärus mille artikkel 12 kohustab isikuandmete töötlejaid esitama isikutele teavet isikuandmete töötlemisest selges ja lihtsas keeles, kokkuvõtlikult, arusaadavalt ning lihtsasti kättesaadavas vormis.

Aastal 2007, kui kirjutati alla Lissaboni leping[4] ja muudeti Euroopa Ühenduse alusleping Euroopa Liidu toimimise lepinguks (ELTL) siis lisati sellesse varasema aluslepinguga võrreldes ka üks oluline täiendav põhimõte „Igaühel on õigus oma isikuandmete kaitsele“[5]. Sellega algas Euroopa Liidu liikmesriigi kodaniku jaoks uus ajastu, mis tähendas, et isikuandmetega tehtavad toimingud ja isikuandmete kaitse sai põhiõiguseks. Seoses sellise uue põhimõtte lisamisega ELTL-i pandi Euroopa Parlamendile ja nõukogule kohustus kehtestada isikuandmete töötlemisega ja andmete vaba liikumisega seotud eeskirjad ning määrata nende eeskirjade täitmist kontrollivad sõltumatud asutused, et Euroopa üleselt kehtestatud nõuded andmete töötlejatele ja õigused isikutele oleks tagatud igas liikmesriigis. Selline muudatus aga ei tähendanud seda, et varasemalt ei oldud isikute põhiõigusi ja isikuandmeid kaitstud vaid seda, et tegu on olulise kaitse täiendava tagamisega isikutele. Ka varasemalt oli Euroopa Komisjoni kehtestatud Euroopa Liidu põhiõiguste harta[6], mille artikkel 8 lõige 1 kohaselt on igaühel õigus oma isikuandmete kaitsele[7] ja lõige 2 kohaselt tuleb töödelda isikuandmeid asjakohaselt, kindlaksmääratud eesmärkidel ja seaduses ettenähtud õiguslikul alusel.

Lisaks põhiõiguste hartale oli Euroopa Nõukogu juba 1950 aastal vastu võtnud inimõiguste ja põhivabaduste konventsiooni[8] mille artikkel 8 lõige 1 tagab õiguse era- ja perekonnaelu ning kodu

[3] Majandus- ja Kommunikatsiooniministeerium (2018). E*esti infoühiskonna arengukava 2020.* Kättesaadav: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2020.pdf 23. märts 2020, 1.
[4] ELT C 306, 17.12.2007.
[5] ELT C 202, 07.06.2016, ELTL artikkel 16B lõige 1.
[6] Esimene versioon hartast võeti vastu 07.12.2000.
[7] ELT C 326, 26.10.2012.
[8] ETS nr 5. võeti vastu 04.11.1950 ja jõustus 03.09.1953.

puutumatuse ja lõige 2 mis keelab ametivõimudel seda õigust rikkuda[9]. Antud konventsioon põhines omakorda aga Ühinenud Rahvaste Organisatsiooni (ÜRO) poolt 1948 aastal vastu võetud resolutsioonile A/RES/217 mis on tuntud kui inimõiguste ülddeklaratsioon.

Aastal 1981 andis Euroopa Nõukogu välja isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni[10] mis kehtestab juba täpsemad nõuded justnimelt isikuandmete automatiseeritud andmete töötlemisele. Sellise konventsiooni vastuvõtmine oli tingitud eelarvamusest, et digitaliseeritud ja automatiseeritud andmete kasutus võib anda ka põhjendamatut juurdepääsu isiku krediidi, eluaseme ja kindlustuse andmetele.[11] Sellele järgnes juba 1995 aastal Euroopa Parlamendi ja nõukogu poolt vastu võetud direktiiv[12] millesse oli koondatud põhimõtteid nii eelmainitud õigusaktidest kui ka näiteks Prantsuse andmekaitse õigusest[13]. Seega saab väita, et isiku õigusi on kaitstud juba aastast 1948 ja isikuandmetega seonduvat infot aastast 1981, mis tähendab, et isikute andmete ja selliste andmete automatiseeritud töötlemisel on pakutud õiguslikku kaitset ligi 40 aastat.

Lisaks Euroopas kehtivale isikuandmete töötlemisel kehtivale õigusele võttis ÜRO täiendavalt 2014 aastal vastu resolutsiooni A/RES/69/166 õigus privaatsusele digitaalajastul, millega sooviti kinnitada põhimõtet, et ka internetis tuleb eraelu puutumatuse aspekte käsitleda sarnaselt kõikidele teistele rahvusvaheliselt tunnustatud inimõigustele. Resolutsioonis rõhutati, et kõik valitsused kes juba omavad või tulevikus juurutavad digitaalseid isikuandmete töötlemise süsteeme, peavad tagama rahvusvaheliselt tunnustatud fundamentaalseid isiku põhiõigusi ja -vabadusi ning tagama isikuandmete privaatsuse.[14]

[9] ETS nr 5 artikkel 8 lõige 2 lubab era- ja perekonnaelu ning kodu puutumatus riivata erandiga, kui on oht riigile või kui saaks kahjustada teiste isikute põhiõiguseid.
[10] ETS nr 108. 28.01.1981 – jõustus alles 01.10.1985.
[11] Veale, M., Edwards, L. (2017). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision- making and profiling. *Computer Law & Security Review: The International Journal of Technology Law and Practice*,34 (2), 398-404, 398.
[12] ELT L 281, 23.11.1995.
[13] Veale, Edwards, *supra nota* 11, 399.
[14] Tsulukidze M., Nyman-Metcalf K., Tsap V., Pappel I., Draheim D. (2019) Aspects of Personal Data Protection from State and Citizen Perspectives – Case of Georgia. In: I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie (Eds.), *Digital Transformation for a Sustainable Society in the 21st Century*, (476–488). Cham:Springer, 476.

1.1. Direktiivist üldmääruseni

Kui 1995 aastal rakendatud direktiivis olid esitatud ainult miinimum nõuded isiku andmete kaitseks siis uue üldmääruse väljatöötamisel pidi arvestama juba sellega, et Euroopa Liidu (EL) seadusi rakendatakse üha enam horisontaalsete ja vertikaalsete koostöömehhanismide kaudu EL ja liikmesriikide asutuste vahel.[15] Veelgi olulisemaks tuli aga pidada aastate jooksul toimunud info- ja kommunikatsioonitehnoloogia (IKT) jõulist arengut ning paralleelselt toimunud majanduse ja ühiskonna digitaliseerumist. Sellel ajavahemikul on kasutusele võetud erinevaid IKT lahendusi, mis hõlmavad endas nii andmete töötlemist, edastamist, salvestamist kui ka võimalikku kuritarvitamist. Kuigi sarnaselt üldmäärusele oli ka direktiivis kehtestatud nõuded isikuandmete töötlejale ja õigused isikutele[16] olid just „kasutamisega ja kuritarvitamisega kaasnevad tegevused need, mis tõstatasid täiendavaid küsimusi selle kohta, kas isikuandmete 'traditsiooniline' kaitse on ikka endiselt piisav"[17].

2016 aastal vastu võetud üldmäärusega, mis rakendus 25. mail 2018 aastal, on seatud selgeks eesmärgiks kaitsta kõikide kodanike[18] põhiõigusi ja -vabadusi nende isikuandmete töötlemisel ja edastamisel. Samuti sooviti kehtestada sellega EL-is ühtsed andmete töötlemise põhimõtted ja tingimused ning anda kodanikele suurem võimalus kontrollida enda isikuandmete kasutamist.[19] „Üldmäärus peab tagama isikuandmete tõhusama ja järjepidevama kaitse dünaamilises ja haavatavas digitaalses keskkonnas"[20], nõnda võttis kokku erinevused Demetzou, kes võrdles ja analüüsis üldmäärust varem kehtinud direktiiviga ning leidis, et on toimunud oluline lähenemisviisi muutus milleks on aruandekohustuse tekkimine isikule ja sellega loodetakse saavutada ka päriselt andmete kaitstus.

Asutustele on seevastu aga üldmäärusega seonduvalt lisandunud täiendavat dokumenteerimise kohustust, sest vastavalt üldmääruse põhimõtetele tuleb neil üle vaadata ja dokumenteerida kõik isikuandmete töötlemisega seonduv, sealhulgas töötlemise eesmärgid ja alused ning põhimõtted.[21]

---

[15] Eliantonio, M., Galli, F., Schaper, M. (2016). A Balanced Data Protection in the EU: Conflicts and Possible Solutions. *Maastricht Journal of European and Comparative Law*, 23 (3), 391-403, 392.
[16] Vt nt 95/45/EÜ artikkel 12 ja üldmääruse artikkel 15 - õigus tutvuda andmetega.
[17] Eliantonio *et al.*, *supra nota* 15, 392.
[18] Euroopa Liidu ja Euroopa Majanduspiirkonna territoorium ja nende kodanikud.
[19] Larsson, A., Lilja, P. (2019). GDPR: What are the risks and benefits? In: A. Larsson, R. Teigland (Eds.), *The Digital Transformation of Labor: Automation, the Gig Economy and Welfare*, 187-199, 187.
[20] Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review*, 35 (6), 1-14, 1.
[21] Täielik nimekiri isikuandmete töötlemise põhimõtetest on kirjeldatud üldmääruses artikkel 5 lõige 1.

Ja seda seetõttu, et üldmääruse artikkel 5 lõige 2 paneb sellise dokumentatsiooni olemasolu eest vastuse asutusele, kellel peab olema ka reaalselt võimalik tõendada, et on täidetud kõik üldmääruse artikkel 5 lõige 1 toodud põhimõtted. Lisaks on kohustus asutustel tulenevalt üldmääruse artikkel 30 kohustus isikuandmete töötlemise toimingud registreerida, mis tähendab kõigi asutuse ülesannete täitmiseks vajaminevate andmete kasutuse ja andmekogumite analüüsi ja kirjeldust.[22] Üldmääruse kohaselt peab töötluse seaduslikkust tõendama asutus ja tal on kohustus kõik need dokumendid hoida aja- ja asjakohased ning vajadusel peavad olema need ka ettenäidatavad järelevalveasutusele kui ka isikutele, kelle andmeid töödeldakse. Sarnased nõuded ei ole uued ja olid juba olemas nii ETS nr 108 artikkel 8 lisatagatised andmesubjektile kui ka 1995 aasta direktiivis artikkel 2 kataloogimine, lihtsalt üldmääruses on need kohustused selgemini sõnastatud ja omavad otsekohalduvat nõuet. Üldmäärusele eelnevalt kehtinud direktiiv tuli aga riikidel enda seadusandlusesse integreerida mis andis mõningast tõlgendamise vabadust.[23]

1.2. Läbipaistvus üldmääruse põhimõte järgi

Üldmääruse artikkel 5 lõige 1 punkt a järgi peab olema tagatud, et isikuandmete töötlemine on seaduslik, õiglane ja andmesubjektile läbipaistev, mis tähendab, et isikuid puudutavate isikuandmete kogumine, kasutamine, lugemine või muu töötlemine ja nende andmete töötlemise ulatus peab olema isikute jaoks läbipaistev.[24] Läbipaistvuse põhimõte omakorda eeldab, et isikuandmete töötlemisega seotud aja- ja asjakohane teave on avalikult ja lihtsalt kättesaadav ning isikule arusaadavalt, selgelt ja lihtsasti sõnastatud. See tähendab asutusele kohustust teavitada isikud kogutavate andmete detailsusest ja millist seadusest tulevast ülesannet nende andmete töötlemisega täidetakse. Lisaks tuleb asutusel esitada täiendav teave selle kohta, kuidas isikud saavad enda üldmääruses toodud õigusi realiseerida[25]. Samuti peavad asutused lisaks isikuandmete õiglase ja läbipaistva töötlemisele tagama ka isikuandmete hoidmisel ja edastamisel turvalisuse[26], millega oleks välistatud potentsiaalse ohtu tekkimine isikute andmetele, eraeluliste huvide ja õiguste riivele.

---

[22] Larsson, Lilja, *supra nota* 19, 194.
[23] Kuner, C. (2012). *European Data Protection Law: Corporate Compliance and Regulation* (2nd ed.). Oxford, UK: Oxford University Press, 140.
[24] Üldmäärus põhjenduspunkt 39.
[25] Isiku õigused on kirjeldatud üldmääruses artikkel 15-18, 20-22, 77-79 ja 82.
[26] AvTS §43[3] lõige 3.

Täiendavalt on lubatud liikmesriikidel kehtestada konkreetsemaid sätteteid[27], et kohandada ja aidata kaasa üldmääruses toodud sätete kohaldamisele. Seda eriti juhtudel, kui isikuandmete töötlejaks on asutus, kes täidab avalikes huvides olevat ülesannet või teostab oma ülesannetest tulenvalt avalikku võimu. Selline meede on arusaadav ja vajalik, sest avaliku ülesannete täitmise aluseks olev liikmesriigi kohaldatav õigus erineb riigiti ning sellised toetavad meetmed on igati põhjendatud ja asjakohased, et tagada üldmääruses toodud nõuetekohane täitmine.[28]

Andmetöötluse põhimõtted pärinevad aasast 1980[29] ning õiglase ja läbipaistva isikuandmete töötlemise tagamise põhimõte üldmääruses ei ole uus kohustus vaid seda on võrreldes varasemalt kehtinud andmekaitse direktiiviga oluliselt täpsustatud. Ka direktiivis oli õiglase töötlemise säte olemas klausliga „Teave tuleb esitada juhul ... kuivõrd selline teave on vajalik, et tagada isikute suhtes õiglane andmete töötlemine“[30]. Pigem oli erinevus selles, et varasemalt andmekaitset reguleeriv akt oli välja antud direktiivi vormis, mis on oma õiguslikkuse seisukohalt liikmesriigile siduv teisene õigusakt. Seega vajalike tulemuste saavutamiseks tuli direktiiv kehtivasse siseriiklikusse õigusesse üle võtta aga direktiivi eesmärkide saavutamiseks jäeti vastav vormi ja meetodite valik iga liikmesriigi enda otsustada.[31] Sellest lähtuvalt, kontrollis autor, kas direktiivi alusel vastu võetud siseriiklikus IKS-is[32] oli viiteid või sarnaseid kohustusi õiglasele isikuandmete töötlemisele, siis sellisel kujul nagu seda on esitletud üldmääruses vanas IKS-is ei leidu. Samuti ei ole direktiivis ja vanas IKS-is mõisted läbipaistev andmetöötlus, millele on üldmääruses pühendatud terve III peatüki 1. ja 2. jagu.[33]

Kuid mida siiski tähendab isikuandmete kaitse kontekstis mõiste andmed, mida on vaja kaitsta ning miks on vaja, et andmetöötlus oleks õiglane ja läbipaistev? „Andmekaitse, kui õigusharu ei keskendu mitte andmete kaitsele, vaid kaitseb inimest, keda kaitstavad andmed identifitseerivad.“[34] Andmed on informatsioon kellegi või millegi kohta ning faktid, mida kellegi või millegi kohta teada saadakse või juba teatakse.[35] Isikuandmeteks on seega igasugune isikut

[27] Üldmäärus artikkel 6 lõige 2.
[28] Vt üldmäärus artikkel 6 lõige 3 punkt a ja b.
[29] Peep, V. (2018). Andmekaitseõigusest andmekaitseasutuse pilguga. *Juridica,* 2, 116-124, 117.
[30] Direktiivi artikkel 10 ja 11.
[31] Sein, K., Mikiver, M., Paloma K. T. (2018). Pilguheit andmesubjekti õiguskaitsevanditele uues isikuandmete kaitse üldmääruses. *Juridica,* 2, 94-114, 94.
[32] IKS, RT I 2007, 24, 127, 15.02.2007. Jõustumine 01.01.2008, redaktsioon 16.01.2016-14.01.2019.
[33] Üldmäärus artikkel 12-14. Lisaks on üldmääruse 2. jaos artikkel 15 „Andmesubjekti õigus tutvuda andmetega“ aga sarnane artikkel on olemas ka andmekaitse direktiivis artikkel 12.
[34] Männiko, M. (2011). *Õigus privaatsusele ja andmekaitse.* Tallinn: Juura, 42.
[35] Eesti keele seletav sõnaraamat. Arvutivõrgus: https://www.eki.ee.

kaudselt või otseselt tuvastav teave.[36] Andmekaitse inspektsiooni (AKI) peadirektor on kirjutanud „inimesed vajavad kindlustunnet, et nende kohta käivat teavet kogutakse ja kasutatakse ausalt, õigesti ja turvaliselt. Ilma selleta ei teki usaldust. Kui inimesed ei usalda, kuidas nende andmeid kasutatakse, siis digimajanduse ja e-riigi areng seiskuks."[37] Riigi poolt andmete töötlemisel tähendab usaldus seda, et isikud teavad miks ja kuidas nende andmeid töödeldakse ja neid kogudes, kasutades ja hoides toimitakse vastavalt kehtivatele õigusaktidele ja turvanõuetele. „Just sellist professionaalselt ja õiguspäraselt käituvad organisatsiooni saab ka päriselt usaldada."[38]

1.3. Läbipaistvusest praktiliselt, asutusele

Euroopa Liidus kehtib *expressis verbis* põhimõte, et kõik asutused peavad kodanikuga avatud ja läbipaistvat dialoogi[39] ning kõik otsused tuleb teha nii avalikult ja kodanikulähedaselt kui võimalik[40]. Lisaks on ELTL artikkel 15 kehtestanud põhimõtted, mille järgimisel saavad asutused tagada avatuse ja läbipaistvuse. Neid samu põhimõtteid on üldmääruse kolmandas peatükis[41] detailsemalt avatud, sest nende alusel kehtestatakse töötleja kohustused, isiku õigused ja võimalikud erisused isikuandmete töötlemisele.

Autori arvates on aga termin „läbipaistvus" sarnaselt mõnele teisele terminile[42] määratlemata õigusmõiste[43], mille tunnuste täpne loetelu võib olla väga lai. Sellistele määratlemata õigusmõistetele on omane, et nad on ajast, asukohast ja subjekti vaatest muutuvad ja ka erinevalt tajutavad. Seetõttu nõuaks selliste mõistete täpne defineerimine ebamõistlikku pingitust ning mõiste avamiseks tuleb lähtuda konkreetsest ajast ja ruumist.[44] Ka artikli 29 alusel asutatud andmekaitse töörühm üksikisikute kaitseks seoses isikuandmete töötlemisega (töörühm)[45] kinnitab

---

[36] Üldmäärus artikkel 4 lõige 1.
[37] Andmekaitse inspektsioon (2019). *Isikuandmete töötleja üldjuhend*. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf 20. veebruar 2020, 4.
[38] Larsson, Lilja, *supra nota* 19, 190.
[39] ELT C 202, 07.06.2016, ELL artikkel 11 lõige 2.
[40] *Ibid.* artikkel 1 lõige 2.
[41] Üldmäärus artikkel 12-23.
[42] Ikkonen, M. (2005). Avalik huvi kui määratlemata õigusmõiste. *Juridica, 3*,187-199, 187. Nt avalik huvi, head kombed, hea usk, kõlvatu konkurents.
[43] *Ibid.*
[44] *Ibid.*
[45] Autori täpsustus, et sellenimeline töörühm lakkas eksisteerimast alates 25.05.2018 kui jõustus üldmäärus. Üldmääruse kohaselt on see asendunud andmekaitsenõukoguga (vt. üldmääruse põhjenduspunk 139). Kuna aga kõik isikuandmeid puudutavad juhised kannavad endiselt nime „Artikkel 29 alusel välja antud …" siis selguse huvides kasutab autor siin ja edaspidi terminit „töörühm".

oma juhendis sama ning lisab, et läbipaistvus antud üldmääruses ei ole juriidiline mõiste vaid kasutajakeskne mõiste ja töötlejatele on kehtestatud pigem praktilised kui juriidilised nõuded.[46] Selline praktiline lähenemine on ka põhjendatud tulenevalt üldmääruse soovist katta kogu liidus toimuv isikuandmete töötlemine ühe õigusaktiga. Kõiki asutusi hõlmav täpne loetelu oleks aga ammendamatu, sest vastavalt asutuse ülesannetele erineb ka andmete töötlemine ning töötlemise õiguslik alus[47] ja vastavalt ka sellistele erinevustele tuleb igal asutusel esitada enda spetsiifiline teave mis on töötlemisele kohane.

Nagu eelmises peatükis tuvastati, ei ole läbipaistvuse nõue oma olemuselt uudne andmekaitse põhimõte vaid varem kehtinud erinevate nõuete kogum, mis on viidud ühe termini alla ja seda on täiendatud. Kuna direktiivis sellist terminit nagu läbipaistvus ei olnud *expressis verbis* välja toodud siis on selle mõistega kaasneva võimaliku määratlematuse vähendamiseks AKI ja töörühm pidanud vajalikuks täiendavalt selgitada läbipaistvusest tulenevaid põhimõtteid ja andnud välja täiendavad ja täpsustavad juhised[48] asutustele. Kuigi läbipaistvus hõlmab endas osaliselt neid samu põhimõtteid mis olid kirjas ka direktiivis, näiteks nagu andmesubjektile esitatav teave[49] või õigus tutvuda enda andmetega[50], on ülevaatlikud juhendid asutustele abimeheks ka üldmääruses toodud tingimuste täitmisel.

Läbipaistvuse mõistes on tegu oma olemuselt andmekaitsetingimustega[51], milles peab olema välja toodud teave isikult otse või muudest allikatest kogutud andmete töötlemise osas, nende andmete võimalike edasiste töötlejate ja töötlemise viiside kohta ning millistel õiguslikel alusetel on andmed kogutud, millistel õiguslikel alustel andmeid edastatakse ja millised õigused on isikul tema kohta kogutud andmete edasise töötlemise osas. Samuti tuleb esitatavas andmekaitsetingimustes lisaks eelnevale välja tuua töötlemisega seonduvad võimalikud ohud ja kaasnevad kohustused.[52] Isikutele esitatavad andmekaitsetingimused peavad olema kokkuvõtlikud, selged[53] ja arusaadavad ning lihtsasti leitavad. Vastav info tuleb esitada kirjalikult

---

[46] Artikli 29 töörühm (2018). *Suunised määruse 2016/679 kohase läbipaistvuse kohta*. Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_maaruse_2016679_kohase_labipaistvuse_kohta.pdf 20. veebruar 2020, 5.
[47] Üldmääruses artikkel 6 on toodud erinevad õiguslikud alused töötluse seaduslikkusest.
[48] AKI (2019), *supra nota* 37, peatükk 10; Töörühm (2018), *supra nota* 46.
[49] Võrdle direktiiv artikkel 10 ja 11 ning üldmäärus artikkel 13 ja 14.
[50] Võrdle direktiiv artikkel 12 ning üldmäärus artikkel 15.
[51] AKI (2019), *supra nota* 39, 43.
[52] Üldmäärus põhjenduspunkt 39.
[53] Euroopa Komisjon (2012). *Kirjuta selgelt*. Kättesaadav: https://op.europa.eu/en/publication-detail/-/publication/bb87884e-4cb6-4985-b796-70784ee181ce/language-et 11. aprill 2020. Selles on toodud juhised, millest asutused peavad lähtuma, kui esitavad teavet kodanikule.

või muude vahendite abil.[54] Seda võib esitada ka suuliselt, kui isik seda taotleb aga AKI soovitab esitamise vahend ja kanal valida vastavalt sellele, millist on kasutatud ka andmete kogumiseks.[55] Samas peab järgima põhimõtet, et vastavad tingimused peavad olema tehtud avalikuks *ex ante* ja nendes peab olema ka välja toodud info, kas isikul on kohustus enda kohta olevaid andmeid esitada ja selliste andmete esitamata jätmise võimalikest tagajärgedest.[56] Samuti tuleb esitada vastav info enne sellise töötlemise teostamist, mille osas isikul puudus algselt teave.[57] *Ex ante* põhimõte kehtib ka siis, kui andmeid võib õiguspäraselt avaldada teisele asutusele ja seda kavatsetakse teha esmakordselt.[58] Samas lubab üldmäärus *ex post* esitada töötlemise tingimused ühe kuu jooksul juhul, kui andmeid ei ole saadud isikult endalt.[59] Autor näeb siin aga mõningast ebaselgust, sest üldmääruse mõistes on ka andmete saamine ja hoidmine, mis üldjuhul on eelduseks edastamisele, ka töötlemine, mis tähendaks, et tingimusi tuleks esitada kaks korda: saamisel ja hoidmisel *ex post* ja samade andmete edastamisel *ex ante*. Siin aga lubab üldmäärus teavitamise tingimuse kohustust eirata selles osas, kui asutus on võimalikku edastamist avaldanud juba varasemalt ehk siis kogumise järgselt sellest teavitanud oma andmekaitsetingimustes ja eeldusel, et isikul on vastav teave olemas ja ta on sellest aru saanud.[60]

Autor peab siin vajalikuks täpsustada, et üldmääruses on lisaks edastamise õigusele olemas ka õigus andmete ülekandmisele[61] mis antud kontekstis ei tähenda edastamist vaid isiku enda poolt esitatud andmete ühelt vastutavalt töötlejalt ülekandmise võimalust teisele vastutavale töötlejale. Seda õigust saab isik kasutada vaid juhul, kui esijalgsete andmete kogumine oli toimunud kas tema enda nõusolekul või isiku ja vastutava töötleja vahel sõlmitud lepingu täitmisel. Kuna riik ei töötle isikuandmeid avalikes huvides oleva ülesande täitmisel nõusoleku ega ka lepingu alusel vaid seadusest tulenevate ülesannete täitmisel, siis asutustele antud ülekandmise punkt ei kohaldu.

Selleks, et asutus saaks tagada ja veenduda andmete töötlemise läbipaistvuses on üldmääruses kohustus asutustel igasugune isikuandmete töötlemine asutuse siseselt registreerida[62] ja kohustus

[54] Üldmäärus artikkel 12 lõige 1.
[55] AKI (2019), *supra nota* 37, 46.
[56] Üldmäärus põhjenduspunkt 60; Wachter, S., Mittelstadt, B., Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 7 (2), 76-99, 79.
[57] AKI (2019), *supra nota* 37, 43; Üldmääruse põhjenduspunkt 61.
[58] Üldmäärus põhjenduspunkt 61.
[59] *Ibid.*
[60] Üldmäärus põhjenduspunkt 62.
[61] Üldmäärus artikkel 20.
[62] Üldmäärus artikkel 30.

andmete töötlemise reeglid ja andmekaitsetingimused perioodiliselt läbivaadata[63]. Üldmääruse artikkel 30 kajastab miinimum kohustused mida asutused peavad kaardistama, et kõik asutuses kasutusel olevad andmed ja nendega tehtavad toimingud saaks registreeritud. Selle vajalikkus seisneb ka selles, et asutused saaks enda andmeid „puhastada" ja siin ei tehta vahet, kas töödeldakse eriliigilisi isikuandmeid või mitte. Andmete puhastamine (*data cleansing*) on protsess, mille käigus asutus tuvastab ja vajadusel eemaldab või muudab andmeid andmekogudes, mis on kas vananenud, valed, puudulikud või topelt. Üldmääruses on lisaks veel säte, et ka ebaolulised ja ebavajalikud andmed tuleks eemaldada ja sellist puhastamist tuleks teha regulaarselt.[64]

Kuigi üldmääruse artikkel 30 lõige 5 järgi kehtiks selline isikuandmete töötlemise registreerimise kohustus ainult asutustele, kus on vähem kui 250 töötajad, siis AKI on täpsustanud, et selle punkti sõnastus on ebaõnnestunud ja tegelikult puudub asutustel kaalutustõigus kas nad peavad isikuandmete töötlemist registreerima või mitte. Seega on AKI seisukohal, et sellise registri loomine on kohustuslik kõikidele isikuandmete töötlejatele ja viitab üldmääruse artikkel 30 lõige 5 viidatud töötlemisele, mis ei ole juhtumipõhine.[65]

Lisaks seisneb sellise puhastamise olulisus veel selles, et see sunnib asutusi juba ennetavalt kaaluma, millist tüüpi andmeid nad peavad koguma ja säilitama. Kuna ajaga suureneb salvestatud andmete maht siis võib sellega kaasneda ka asutuse sisese bürokraatia suurenemine, kõrgemad kulutused IKT seadmetesse ja ka andmelekke risk.[66] Kuna isikutel on ootus lisaks läbipaistvusele ka turvalisusele, siis riske peab asutus ise hindama ja nad saavad seda teha kahe põhilise näitaja alusel „tõenäosus" ja „haavatavus".[67] Isikuandmete kaitse tagamisel tuleb hinnata tõenäosusust kui võimalikku ohtu andmete kättesaadavusele ehk juurdepääsu ja haavatavuse osas tuleb hinnata millist kahju kaotatud andmetega teha saab.[68] Lisaks riskide hindamisele tuleb ka analüüsida, kas kõik olemasolevad süsteemid ja andmed on ka asutuse jaoks asja- ja ajakohased või piirneb see võimaliku halli alaga ja kus töötlemise täpset alust on keeruline määrata aga oma mugavuse mõttes on andmete hoidmist õigustatud.[69] Kui tuvastatakse, et tegu võib olla sellise võimaliku andmete

[63] Üldmäärus põhjenduspunkt 39.
[64] Larsson, Lilja, *supra nota* 19, 192; Üldmäärus põhjenduspunkt 39.
[65] AKI (2019), *supra nota* 37, 20.
[66] Larsson, Lilja, *supra nota* 19, 192.
[67] *Ibid.*
[68] *Ibid.*
[69] Larsson, Lilja, *supra nota* 19, 193.

hoidmise halli alaga, siis tuleb leida selliste andmete hoidmiseks õiguslik alus või nende töötlemine lõpetada.

Üldmäärus kohustab läbipaistvust tagama ja tõendama isikuandmete vastutava töötleja ehk siis asutuse, kes isiku andmeid töötleb[70]. Siin peab asutus aga arvestama ka sellega, et selline põhimõte laieneb ka selliste isikuandmete töötlemistele, mida teostati ka enne üldmääruse jõustumist. Sellisel juhul peab asutus alates 25. mai 2018 suutma tõendada, et antud hetkest alates on edaspidine uute kui ka varasemalt kogutud ja salvestatud andmete töötlemine üldmäärusega kooskõlas ja läbipaistev.[71] Selline üldmääruse läbipaistvuse põhimõte teabe esitamisel on kirjas ka siseriiklikus õiguses, mis on kehtestatud AvTS § 28 lg 1 p 31^1 kohustusena teabevaldajal avalikustada isikuandmete töötlemise eesmärk, ulatus ja viis, kolmandatele isikutele, sealhulgas teisele asutusele, isikuandmete edastamise ja avalikkusele kättesaadavaks tegemise ning isiku poolt enda andmetega tutvumise õigus ja kord.

1.4. Asutus, tema ülesanded ja teenused

Asutuste ülesandeks on seaduse alusel täidesaatva riigivõimu teostamine[72]. Igal asutusel peab olema oma põhimäärus milles peab olema kajastatud asutuse tegevusvaldkond ja ülesanded ning asutuse tegevuse korraldamise olulised sätted.[73] Seega on igal asutusel väga selge ülesanne mida ta täidab ja millistel tingimustel tohib töödelda ka avaliku teavet.[74] Nende ülesannete täitmisel on asutustel seega seadusega antud volitus, millega nad võivad isikutele määrata hüvesid ja soodustusi ning kehtestada piiranguid ja kohustusi.

Nendeks asutusteks võivad olla ametid, inspektsioonid, avalik-õiguslikud isikud ja ministeeriumid kus teenuste osutamine ei ole delegeeritud valitsemisala allasutustesse.[75] Kuna aga asutustel on teenustest väga erinev arusaam siis on tihti ka kasutatud mõisteid nagu „funktsioon“, „protsess“,

[70] Üldmäärus artikkel 5 lg 2.
[71] Üldmäärus põhjenduspunkt 171.
[72] Vabariigi Valitsuse seadus. RT I, 12.12.2018, 8, §39 lõige 1.
[73] VVS §42 lõige 2 sisaldab veel täiendavaid tingimusi aga mis ei ole autori arvetes antud töö puhul relevantsed.
[74] Avalik teave on AvTS § 3 lõige 1 mõistes mis tahes viisil ja mis tahes teabekandjale jäädvustatud ja dokumenteeritud teave, mis on saadud või loodud seaduses või selle alusel antud õigusaktides sätestatud avalikke ülesandeid täites.
[75] Vabariigi Valitsus (2015). *Avalike teenuste omanike määratlemise analüüs ja ettepanekud.* Kättesaadav: https://www.mkm.ee/sites/default/files/avalike_teenuste_omanike_maaratlemise_analyys_ja_ettepanekud.pdf 23. märts 2020, 1.

„põhiprotsess“, „menetlus“ ja „ülesanne“.[76] „Üldistatult mõistetakse avaliku teenusena teenust, mida osutatakse avalikes huvides ning mida rahastatakse riigi või kohaliku omavalituse (KOV) eelarvest.“[77] Teenuse osutamisel peab olema konkreetse sihtrühma vajadus ja võimekus asutuse poolt seda vajadust rahuldada.[78] „Avaliku teenusena on Eesti Vabariigi strateegiadokumentides nimetatud teenust, mida riik või kohalik omavalitsus või avalikku ülesannet täitev eraõiguslik isik osutab isiku tahtel (sh eeldataval tahtel) tema seadusest tulenevate kohustuste täitmiseks või õiguste kasutamise võimaldamiseks.“[79]

Aga kuidas defineerida asutuse teenust ja kas kõik teenused kuuluvad üldmääruses toodud põhimõtete kohaldamisalasse. Üldistatult võib öelda, et kõik mida asutus teeb on avaliku sektori ehk riigi poolt pakutav teenus ja isikud ei pruugi teha vahet erinevatest teenuse liikidest kui räägitakse politsei või päästjate tööst, isikut tõendava dokumendi vahetusest, lasteaiakoha avaldusest, tuludeklaratsiooni täitmisest või haiglatest.[80] Avalike teenuste korraldamise rohelises käsiraamatus on defineeritud avaliku teenust kui „avalike ülesannete täitmisel üldistes huvides osutatavat teenust, mis on suunatud avalike hüvede pakkumisele, avaliku ülesandega kaasnevate kohustuste täitmisele või põhiõiguste ja -vabaduste ning huvide kaitsele.“[81] Riigikantselei pakub täpsemat selgitust avaliku teenuses osas ja on need jaganud üldisteks hüvedeks milleks võivad olla näiteks riigikaitse või õiguskord ning teenusteks, mida riik pakub isikule tema seadusest tulenevate kohustuste täitmiseks või õiguste kasutamise võimaldamiseks ehk transaktsioonilisteks teenusteks.[82] Transaktsioonilised teenused on need on teenuseid, mille puhul teenuse kasutaja pöördub omal algatusel teenuse pakkuja või teenuse vahendaja poole.[83] Selle põhjal saab järeldada, et ainult transaktsioonilised riigi poolt pakutavad teenused kuuluvad üldmääruse põhimõte kohaldamisalasse.

Trend näitab, et üldine suund on nii uute kui ka olemasolevate teenuste arendamisel nende viimine elektroonilistesse kanalitesse (e-teenused) ja taustal toimivate teenuste arendamisse (proaktiivsed

---

[76] Riigikantselei (2014). *Avalike teenuste ühtse portfellijuhtimise kokkuvõte.* Kättesaadav: https://mkm.ee/sites/default/files/avalike_teenuste_uhtne_portfellijuhtimine_-_kokkuvote.pdf 23. märts 2020, 34.
[77] *Ibid.*
[78] Vabariigi Valitsus (2015), *supra nota* 75, 1.
[79] *Ibid.*
[80] Majandus- ja Kommunikatsiooniministeerium (2013). *Avalike teenuste korraldamise roheline raamat*. Kättesaadav: https://mkm.ee/sites/default/files/avalike_teenuste_korraldamise_roheline_raamat.pdf 23. märts 2020, 5.
[81] *Ibid.*
[82] Riigikantselei, *supra nota* 76, 8.
[83] *Ibid.*

teenused) aga samas ei tohi ka ära unustada näiteks letiteenuseid.[84] Riigikantselei põhjendusel tuleb see sellest, et igal teenusel on oma eripära ja ka teenuste tarbijaskonnast kelle eelistusi ja võimalusi tuleb arvesse võtta.[85] Statistikaameti andmetel ei kasuta 2017 aasta seisuga pea 12% Eesti elanikkonnast interneti ühendust.[86] See tähendab, et kui 100% elanikkonnast ei ole kaetud interneti ühendusega ja ei ole tagatud kõikide isikute oskused digitaalselt teenuseid kasutada, peab jääma oma koht ka füüsilistele teenuse kanalitele.[87]

1.5. Avalik e-teenus

e-kirjad, digitaalne muusika, internetipank, veebimaksed, eID, eesti.ee: need on ainult vähesed näited elektroonilistest teenustest ehk e-teenustest.[88] E-teenus on teenus, mille pakkumisel kasutatakse tehnoloogial põhinevat IKT komponenti. Vastavalt teenuse pakkuja sektorile, saab eristada kahte liiki e-teenuseid, nendeks on majandussektoris e-äri ja avalikus sektoris e-valitsus.[89] e-valitsus tähendab elektroonilist asjaajamist valitsuse töös ja kodanike elektroonilist suhtlemist valitsusasutustega.[90] Engin ja Treleaven toovad välja, et „avalikud e-teenused on sellised teenused, mida riigid saavad kasutada suhtluseks kodanikuga ja teenuste osutamisel nii üldsusele kui ka kodanikele kasutatakse mingisugust tehnoloogilist lahendust.“[91] Selle tulemusena saavad tekkida digitaalseid teenuseid pakkuvad valitsused, kes võivad kasutada ka arukaid virtuaalseid abistajaid.[92] Digitaalsete teenuste pakkumine üle interneti võimaldab riigi teenuseid kasutada igalt poolt üle maailma[93] ööpäevaringselt. Lisaks vähendab see oluliselt isikute kohustust ilmuda füüsiliselt asutusse kohapeale mis annab võimaluse teenuseid kasutada ka nendel isikutel kes elavad asukohas, kus asutusse jõudmine võtaks väga kaua aega.[94] Samuti aitab digitaalne suhtlus

---

[84] *Ibid.*
[85] *Ibid.*
[86] Statistikamet. N03: Sidus ühiskond (2004-2017), interneti kasutamise määr % [e-andmebaas]. Kättesaadav: http://andmebaas.stat.ee/ 07. mai 2020.
[87] Riigikantselei, *supra nota* 76, 8.
[88] Kvasnicova, T., Kremenova, I., Fabus, J. (2016) From an analysis of e-services definitions and classifications to the proposal of new e-service classification. *Procedia Economics and Finance*, 36, 192-196, 192.
[89] *Ibib.*,193.
[90] Eesti keele seletav sõnaraamat. Arvutivõrgus: https://www.eki.ee.
[91] Engin, Z., Treleaven, P. (2018). Algoritmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies. *The Computer Journal*, 62 (3), 448–460, 449.
[92] Nt on Eestis, MKM-i eestvedamisel loodav „KRATT“, mis on autonoomne, õppimisvõimeline ja tarkvara algoritmidega programmeeritav tehisintellekti süsteem.
[93] Eelduseks on interneti olemasolu.
[94] Alan, N., Hasan, M. (2015). . A Review of E-Government Services. *Advances in Social Sciences Research Journal*, 2 (8), 48-65, 50.

neid inimesi, kellel on kas vanadusest või mõnest muust põhjusest mõni liikumist raskendav puue[95] ning teatud e-teenuste puhul ei ole vaja enam kinni pidada asutuse lahtioleku aegadest, sest internetipõhised teenused on üldjuhul avatud ka peale asutuse lahtioleku aegasid.

Kuna teenuste pakkumiseks ja otsuste tegemiseks puudub aga riigil ja seega ka asutusel endal teovõime siis seda saavad teostada vaid inimesed ehk ametnikud kes töötavad asutuses.[96] Seega tuleb meeles pidada, et avalik e-teenus mis on mõeldud ühiskonnale on samas ka töövahendiks ametnikule kes peab teostama asutusele määratud ülesannet. e-teenuse pakkumisel ei tohi paberit asendada arvuti ekraaniga või digitaalse vormiga vaid kogu andmevoog tuleb teha selliseks, et asutused ja isikud võidavad ajas ning toimuks digitaalne andmete analüüs, et teha automatiseeritud otsuseid.[97] Sirendi ja Taveter on rõhutanud, et "tõeliselt avalikuks e-teenusteks saab pidada sellist teenust, millest võidavad nii kodanikud kui ka asutuses töötavad inimesed." Kui asutusel on juba olemas vajalikud andmed, siis ei peaks isik ise vajaliku protsessi algatama vaid seda kõike saaks teha automaatika või tehisintellekt.[98]

Et selleni jõuda, tuleb esmalt käsitsi tehtavad tegevused asendada IKT süsteemi poolt toetatud tegevustega. Selle tulemus peab olemas kas täielik automatiseeritus, kus paberile omased protsessid on eemaldatud, või siis osaline kus oma roll jääb ka ametnikule ja isikule.[99] Selline lähenemine tagaks ka asutusele efektiivse ja kiire protsessi.[100] Selliste üleminekute puhul tuleb alati teostada ka andmete puhastus, et analüüsida andmeid, mida töödeldakse ja uurida, kas teenuse paberil pakkumiseks vajalikud andmed on endiselt täies mahus vajalikud ka digitaalselt teenuse pakkumiseks. Lihtne näide on see, et posti aadressiga ei ole midagi enam teha kui suhtlus toimub läbi infosüsteemide ja elektrooniliselt ning vastupidi, kui isik peab saama paberil dokumendi, siis ei ole jälle e-maili aadress oluline. Samuti tuleb veenduda, et andmeid ei kogutaks topelt ehk siis kui neid kogub juba mõni teine asutuse sisene infosüsteem või teine asutus, siis tuleks kasutada

[95] Dąbrowska, A., Janoś-Kresło, M., Lubowiecki-Vikuk, A. (2019). The Elderly as Participants of the Market of Selected E-services. *Studia Periegetica*, 2 (26), 13-23, 16.
[96] Merusk, K. (1994). Avalikõiguslik juriidiline isik kehtivas õiguskorras. *Juridica*, 4, 85-87, 85
[97] Sirendi, R., Taveter, K. (2016). Bringing Service Design Thinking into the Public Sector to Create Proactive and User-Friendly Public Services. In: F.F.-H. Nah, C.-H. Tan (Eds.), *HCI in Business, Government, and Organizations: Information Systems* (221–230). Cham: Springer, 223.
[98] *Ibid.*
[99] Ernst & Young Baltic AS (2012). *Avaliku sektori äriprotsessid. Protsessianalüüsi käsiraamat*. Kättesaadav: http://dspace.ut.ee/bitstream/handle/10062/45124/protsessianaluusi_kasiraamat.pdf?sequence=1&isAllowed=y 23. märts 2020, 36.
[100] Efektiivse, kiire ja lihtsa menetluse põhimõte on toodud ka haldusmenetluse seaduses § 5 lõige 2.

võimalust andmete ristkasutuseks ja seeläbi vähendada andmete kogumisel isikute koormamist juba esitatud andmete uuesti esitamisega[101].

EL-i e-valitsuse tegevuskava aastateks 2016-2020 seab eesmärgiks, et „e-valitsused toetavad oma halduspro tsesse, on parandatud pakutavate teenuste kvaliteet ja suurendatud asutuste tõhusus läbi sisemiste protsesside optimeerimise ja avalikud e-teenused peavad vähendama isikute halduskoormust ja suhtlus asutustega peab olema mugav, kiire ja tõhus.“[102]

1.6. Digimajandus ja e-majandamine

Digimajanduse ja e-riigi areng on olulisem kui kunagi varem. Teenuste digitaliseerimine on riikides viimastel aastakümnetel muutunud üha aktiivsemaks.[103] Riigi e-teenuste turvalisus, kvaliteet ja kõikjalt kättesaadavus tõstab valitsuse usaldusväärsust, parandab efektiivsust ja vähendab halduskulusid.[104]

Teoorias on eristatavad neli digimajanduse ja e-riikide arengu etappi milleks on kataloogimine, ülekandmine, vertikaalne integratsioon ja horisontaalne integratsioon.[105] Esimese ja teine etapp, milleks on andmete korrastamine ja registritesse suunamine ning korrastatud andmete digitaalne vahetus, on tänaseks juba ajalugu. Siis käesoleva uurimuse raames on olulised just kaks viimast, vertikaalne ja horisontaalne integratsioon, kus asutustel on tekkinud võimalus ristkasutada juba olemasolevaid andmeid, analüüsida erinevatest allikatest saadud andmeid ja pakkuda e-teenuseid. Just need viimased andmetöötluse meetodid peavad tagama ka üldmääruses kirjeldatud andmetöötluse läbipaistvuse.

---

[101] AvTS § 43[1] lõige 3 Andmekogusse andmete kogumisel lähtutakse andmete ühekordse küsimise põhimõttest.
[102] Euroopa Komisjon (2016). *Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele ELi e-valitsuse tegevuskava 2016-2020, Valitsussektori digitaalse arengu kiirendamine*. Kättesaadav: https://eur-lex.europa.eu/legal-content/et/TXT/?uri=CELEX:52016DC0179 26. aprill 2020, 2.
[103] Drogkaris P., Gritzalis A. (2015). A Privacy Preserving Framework for Big Data in e-Government Environments. In: S. Fischer-Hübner, C. Lambrinoudakis, J. López (Eds.), *Trust, Privacy and Security in Digital Business*, (210-218). Cham: Springer, 210.
[104] Agbozo E., Alhassan D., Spassov K. (2019). Personal Data and Privacy Barriers to E-Government Adoption, Implementation and Development in Sub-Saharan Africa. In: A. Chugunov, Y. Misnikov, E. Roshchin, D. (Eds.), *Electronic Governance and Open Society: Challenges in Eurasia*, (1-10). Cham: Springer, 1.
[105] Sirendi, Taveter, *supra nota* 97, 223.

Tänu uute ja täienevate IKT lahenduste kasutusele võtmisega asutuste poolt on ka suurenenud märgatavalt riigi võimekus töödelda nii isikustatud kui ka isikustamata andmeid. Selline võimekus on andnud võimaluse riikidel lisaks üldiste teenuste pakkumisele hakata pakkuma ka isikustatud e-teenuseid.[106] Agbozo *et al.* on oma uurimuses leidnud, et isikustatud e-teenuste pakkumine tagab parema teenuse kvaliteedi ja teeninduse ning vähendab isikutega otsesuhtlust. Ta lisab, et e-teenuste pakkumise viis on isikule mugavam ja ei sõltu enam ajast ega asukohast. Ühtlasi on ta ka arvamusel, et automatiseeritud teenuste pakkumine võib vähendada ka korruptsiooni kuna teenuste automaatikasse on sisse programmeeritud reeglid, mille järgi tehakse otsuseid ja kui etteantud kriteerium ei ole täidetud, on ka otsus negatiivne. Võrreldes olukorraga, kus ametnik, kes on vastutav teenuse pakkumise eest ja peab tegema otsuseid jooksvalt, hindab sarnaseid olukordi subjektiivselt ning tulemused võrdsetel tingimustel ei pruugi alati olla samad.[107]

Tsulukidze *et al.* avastas, et on tõestatud korrelatsioon eduka e-teenuste ja andmekaitsega. Ehk teisisõnu, mida suurem on usaldus ja teadlikkus andmete edasise töötlemise osas, seda kindlamalt ollakse ka altimad oma andmeid riigile loovutama. Samas aga võivad kodanikud hoiduda riigi poolt pakutavate e-teenuste kasutamisest, kui neil ei ole kindlust, et nende andmetega tehakse ainult vajalikke, seaduses välja toodud ja ettenähtud tegevusi.[108] Ka on leitud, et isikutel on skeptiline hoiak riiklike infosüsteemide turvalisuse ja andmetega tehtavate töötluse osas ning arvatakse, et „illegaalsed“ andmetöötlused ongi peamiseks põhjuseks miks osades riikides e-teenuseid kasutusele ei võeta.[109] Digimajandust toetab ka Agbozo *et al.*, et kõige olulisemad ja mõjukamad põhjused, miks asutused peaks kasutusele võtma e-teenuseid ja kasutama infosüsteeme on asjaolu, et see ei ole asi iseeneses vaid sellega saavad asutused oma pakutavate teenuste nimistut ja paljusust uuesti üle vaadata ja hinnata andmete vajadusi ning seeläbi kaasajastada ning mitmekesistada suhtlemist töötajatega, teiste asutustega ja isikutega.[110]

Digitaliseeritud andmed, sealhuldas ka isikuandmed, on iga infosüsteemi aluseks ja nende töötlemiseks kasutatavad erinevad IKT lahendused võimaldavad erinevaid infosüsteeme ja andmete kogumeid omavahel vahetada ja integreerida. Seega tuleb järjest suuremat tähelepanu

---

[106] Tsulukidze *et al., supra nota* 14, 479.
[107] Agbozo *et al., supra nota* 104, 2 viidatud Weerakkody, V., Irani, Z., Lee, H., Osman, I., Hindi, N. (2015). E–government implementation: A bird's eye view of issues relating to costs, opportunities, benefits and risks. *Information systems frontiers*, 17(4), 889–915.
[108] Tsulukidze *et al., supra nota* 14, 479.
[109] *Ibid.*
[110] Agbozo *et al., supra nota* 104, 2.

pöörata selliste süsteemide arendamisel ja nendes hoitavate andmete kasutamisel turvalisusele. Kuna otsuseid asutustes teevad siiski inimesed, siis on turvalisust ja e-riigi arengu võimalusi silmas pidades vajalik ja kohustuslik igal asutusel tõsta ka oma töötajate teadlikkust. Seda siis nii andmekaitse aspektidest kui ka IKT lahenduste kasutamisel kaasnevate võimalike ohtude teadvustamisel ja ära tundmisel. Sest just asutusel lasub vastutus teenuste pakkumisel ja olemasolevate protsesside automatiseerimisel kohustus tagada oma töötajate teadlikkus isikuandmete kasutamisel. Asutused peavad tegema endast kõik oleneva, et andmetöötlus oleks võimalikult läbipaistev ja tagatud oleks isikute privaatsus ning põhiõigused ja -vabadused.

Kuna ajaga koguneb asutustele järjest rohkem andmeid siis tuleb neid omades ja hallates pöörata suuremat tähelepanu isikuandmete kaitsele ja andmete juurdepääsetavusele, et tagada e-teenuste ja e-riigi usaldusväärsus isikute silmis. Samuti ka andmete järjest efektiivsem kasutamine parandab riigi e-teenuste loomist ja pakkumist. Lisaks peavad asutused olema oma teenuste pakkumisel vastutustundlikud, nende toimingud peavad olema läbipaistvad ja teenused usaldusväärsed – see kõik suurendab isikute kindlustunnet, et riik ei kuritarvita tema kätte usaldatud andmeid.[111]

Selleks, et riik saaks oma e-teenustest ja temale loovutatud isikuandmetest võtta maksimumi, tuleb tal tõsta ja hoida usaldust enda tegevuste suhtes. Kuna riik võib tegutseda ainult seaduste ja nende alusel välja antud õigusaktide alusel, on tarvis ka seadusutes ja asjakohastes põhimäärutes selgelt välja tuua isikuandmete töötlemise eesmärgid ja kord, andmekaitse tingimused ja andmete säilitustähtajad, andmete turvalisusega ja juurdepääsetavusega seotud tingimused. Täiendavalt avaldatud juhised ja seletuskirjad ning andmete töötlemisel ja edastamisel kasutatavad turvalised tehnoloogilised lahendused aitavad tõsta isiku kindlustunnet, sest e-riigi ja e-teenuste edu tagab just nimelt kodaniku kindlustunne riigi ja tema poolt asutatud asutuste ja teenuste suhtes.[112]

[111] Angelopoulos, K., Diamantopoulou, V., Mouratidis, H., Pavlidis, M., Salnitri, M., Giorgini, P., Ruiz, J. F. (2017). A Holistic Approach for Privacy Protection in E-Government. *ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security*. 7, 1-10, 1.; Thompson, N., Ravindran, R., Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government information quarterly*, 32 (3), 316-322, 317.
[112] Tsulukidze *et al.*, *supra nota* 14, 479.

1.7. Andmekogud

Avaliku teabe töötlemise lihtsustamiseks ja struktureerimiseks on lubatud kasutada andmekogusid, mis on asutuse infosüsteemis töödeldavate korrastatud andmete kogumid. Need on asutatud ja neid kasutatakse seaduse või selle alusel antud õigusakti ehk vastava andmekogu põhimääruse alusel.[113] Alates 2007 aastast reguleerib siseriiklikult avaliku sektori andmekogudega seonduvat AvTS[114]. Selle seadusega võimaldatakse igaühe juurdepääs avalikkuse kontrolliks avalike ülesannete täitmisel[115] selleks kasutatavate andmekogude haldamise üle[116] ning kohustatakse teabevaldajat andma avalikkusele teavet avalike ülesannete täitmisest[117]. Selleks, et need tingimused saaks täidetud, kehtestas Eesti Vabariigi Valitus määrusega riigi infosüsteemi kindlustavad süsteemid millede seas on riigi infosüsteemi haldussüsteem[118] (RIHA). AvTS 43^2 lõige 1 mõistes koosneb riigi infosüsteem andmekogudest, mis on infosüsteemi andmevahetuskihiga liitunud ja RIHA-s registreeritud. Seega peaks RIHA tagama riigis kasutusel olevate infosüsteemide ja andmekogude haldamise ja kasutamise läbipaistvuse[119], sest selles tuleb kirjeldada kõik riigis kasutusel olevad infosüsteemid.

Kui andmekogudele on andmekogude põhimäärustega seatud konkreetsed piirangud andmete hoidmiseks siis andmekogudest väljaspool hoitavaid andmeid ja nendega tehtavaid töötlusi, mis kuuluvad ka üldmääruse kohaldamisalasse ei reguleerita andmekogude põhimäärustega vaid AvTS-ga. Sellest tulenevalt võib aga tekkida vastupidine olukord, kus andmed pannakse „asutusesiseseks kasutamise“ märgendi alla ja kodanik ei saa nendest midagi teada. Selline olukord võib juhtuda siis, kui mõnest asutuses kasutusel olevast andmekogust on tehtud erinevatel aegadel, asutuse mõne konkreetse ülesande täitmiseks, väljavõtteid ja neid hoitakse andmekogust eraldi paberil, serverites failide või väiksemate korrastatud andmete kogumitena. Kuna selliste väljavõtete tegemine on üldjuhul asutuse mingi konkreetse ülesande täitmiseks vajalik, siis AvTS pakub mitmeid erinevaid aluseid millega saab asutuse siseste dokumentide juurdepääsu piirata[120].

[113] AvTS §43^1 lõige 1.
[114] Varasemalt reguleeris andmekogudega seonduvat eraldiseisev andmekogude seadus mis võeti vastu 12.03.1993.
[115] AvTS § 1.
[116] AvTS § 2 lg 2^1.
[117] AvTS § 9 lg 4.
[118] AvTS § 43^9 lg 1 p 6. Riigi infosüsteemi haldussüsteemi vastav määrus võeti vastu 28.02.2008.
[119] RIHA § 3.
[120] Vt nt AvTS § 35 lõige 1 punkt 12-16 või lõige 2 punkt 3.

Ülesande täitmisel aga ei pöörata enam sellele tähelepanu kas see koopia, mis sai selleks otstarbeks tehtud, saab peale töötlemist ja eesmärgi täitmist ka kustutatud. Seega võib juhtuda, et asutuse failiserverites või ametnike arvutite kõvaketastel hoitakse andmeid, mida tegelikult enam ei vajata ja nendega tehtav töötlus, nii algne kui ka hilisem (unustatud) hoidmine on oma olemuselt reguleerimata ja seetõttu ka kontrollimatu. Ka autori tööalases kogemuses on selliseid leide ette tulnud ja seega on väga oluline kehtestada ka asutuse sisesed reeglid andmekogusest andmete välja võtmiseks ja edasiseks töötlemiseks. Lisaks on tarvis koolitada ja teavitada asutuse töötajaid nende õigustest ja kohustustest isikuandmete töötlemisel, sealhulgas ka andmetest tehtavate koopiatega töötlemise osas.

Üldjuhul on asutusel teada kui andmekogudest väljastatakse infot teistele asutustele, sest sellised kokkulepped lisatakse tavaliselt vastava andmekogu põhimäärusesse ning asutustel on kohustus andmete vahtemisel täiendavalt teha vastavad andmevahetuslepingud. Samuti tohib asutute vahel andmete vahetus toimuda sellisel juhul üle x-tee[121] või muu sarnast turvalisust tagava kanali kaudu ja selle kohta tuleb pidada ka arvestust, kellele ja kuidas andmeid edastatakse. Ka tuleb andmekogudes pidada arvestust nii asutustele edastavate andmekoosseisude üle kui ka infosüsteemis andmete töötlemise tehnilise logi osas. Selliste logimiste kohustus ja logiandmete säilitamine on kehtestatud üldjuhul andmekogu põhimääruses. Aga asutuses sees töötajate enda poolne andmete kasutus ja andmetest väljavõtete tegemine ja selle kaardistus on üldjuhul kehv. Selle tulemusel ongi tekkinud olukord, kus isikuandmetega seotud informatsioonile asutuse sees piirangud puuduvad aga isikutele on sellisele teabele juurdepääs piiratud.[122]

1.8. Andmelaod

Lisaks andmekogudele on kasutusel andmete hoidmiseks ka andmeaidad ehk andmelaod milles hoitakse sekundaarseid andmeid ning mille jaoks siseriiklikus õiguses puudub erinorm. Sekundaarsed andmed saadakse primaarsetest andmekogudest ehk seaduse alusel loodud avaliku teabega andmete kogumitest saab teha koopiaid, millest tekib omamoodi andmekogu aga selle erinevusega, et andmeladu võimaldab tõsta kokku ja analüüsida erinevate andmekogude koopiaid. AKI on oma andmekogude juhendis maininud, et andmeladusid ei tohi kasutata operatiivbaasina,

[121] X-tee on AVTS § 43^9 lõige 5 mõistes riigi infosüsteemi kindlustav infosüsteemide andmevahetuskiht; RT I, 06.08.2019, 17, Infosüsteemide andmevahetuskiht §2 punkt 1.
[122] Angelopoulos *et al.*, *supra nota* 111, 1.

see tähendab igapäevaste ülesannete täitmiseks vaid ainult statistika või poliitikakujundamise eesmärgil[123]. Autor on aga seisukohal, et ka selline töötlus on samuti asutuse mingi eesmärgi ja ülesande täitmine. Kuigi AKI on oma juhendis välja toonud, et selliste andmeladude pidamisel tuleb lähtuda AvTS-is toodud andmekogude reeglitest[124], siis autori praktilise kogemusi põhjal seda ei tehta, sest üheski andmekaitsetingimuses millega autor on kokku puutunud, ei ole eraldi välja toodud andmelaoga seonduvat töötlust kirjeldatud.

Probleem on sedavõrd olulisem, et andmeladudes tohib töödelda ka isikustatud andmeid ja sellega tekib oht, et asutused, kellel on seaduse alusel vajalik täita erinevaid ülesandeid ja seega õiguslik alus luua rohkem kui üks andmekogu oma eesmärkide täitmiseks, võivad nendest andmekogude koopiatest andmeladusid moodustades isikute kohta kokku panna hoopis täpsema info ja seejuures tekitada oluliselt suurema eraelu puutumatuse ja privaatsuse riive.[125] Kuigi sellisele andmetöötlusele tuleb kohaldada üldmääruse põhimõtteid siis sellist varjatud andmeladude loomist võimaldab täna näiteks ka RIHA määruse § 7 lõige 2 punkt 1 mis ei kohusta andmekogu asutamisel või andmekogus kogutavate andmete muutmisel kooskõlastamist tegema juhul, kui andmekogu asutatakse ainult organisatsiooni sisemise töökorralduse vajaduseks. Kuna kooskõlastus eeldab andmekogu dokumentatsiooni edastamist muu hulgas ka AKI-le, siis ei saa ka AKI veenduda, kas selles loodavas andmekogus mida tegelikult kasutatakse andmelaona, toimub seal ka isikuandmete töötlemine vastavalt kehtestatud nõuetele[126].

Ühe erandina andmeladude osas toob aga autor välja selle, et näiteks Sotsiaalministeerium on oma vastutusalas kasutatava tervise infosüsteemi põhimääruses lisanud alles hiljuti § 14 andmelao kasutamise[127], kus on kirjas, et andmelaos töödeldakse pseudonüümitud isikuandmeid äriprotsesside toetamiseks, poliitika kujundamiseks, mõjude hindamiseks ja teabenõuetele vastamiseks.[128]

Esimene peatükk käsitleb üldmääruse ja läbipaistva isikuandmete töötlemise põhimõtte kujunemist. Käesolevas töös analüüsitav mõiste läbipaistvus on e*xpressis verbis* põhimõte liidu

[123] Andmekaitse inspektsioon (2016). *Andmekogude juhend.* Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf 20. veebruar 2020, 5.
[124] *Ibid.*
[125] *Ibid.*
[126] RIHA § 7 lõige 6.
[127] Vastav muudatus jõustus 15.03.2019.
[128] Tervise infosüsteemi põhimäärus. RT I, 26.02.2020, 2, §14 lõige 1.

tasandil ning ELTL artikkel 15 kohustab kõiki asutusi seda ka järgima. Autor tuvastas, et läbipaistvuse põhimõte andmete töötlemisel ei ole uus mõiste ning on olnud erinevas sõnastus ka varasemalt kehtinud isikuandmete töötlemisega seostud õigusaktides. 2016 aastal vastuvõetud üldmääruses koondati need erinevused, täiendati ja pandi ühise termini alla kokku.

Läbipaistvus tähendab seda, et isikuandmeid töötlevad asutused peavad tegema isikutele lihtsas ja selges keeles kergesti leitavaks sellise info, mis puudutab isikuandmete erinevat laadi töötlemist ning sellega kaasnevaid ohtusid, kohustusi ja võimalikke muid tagajärgi. Lisaks peavad asutused suutma igal ajahetkel tõendama, et isikuandmete töötlemine on tehtud seaduse või selle alusel välja antud õigusaktiga kooskõlas, minimaalne ja õiglane. Selle tagamiseks tuleb asutustel luua isikuandmete töötlemise register kõikidest andmetest sealhulgas ka nendest, mis olid kogutud enne üldmääruse rakendumist.

Alates 2013 aastast on riigis koostatud erinevaid strateegia dokumente ja juhendeid, mis pidid aitama asutusi enda jaoks läbi mõelda, millest koosnevad nende teenused ehk kuidas nad tagavad isikute õiguste ja kohustuste täitmise vastavalt asutusele pandud ülesannete teostamisel. Sellise teenuse pakkumine, milles on kasutatud IKT komponenti isikutega suhtlemisel nimetatakse avalikuks e-teenuseks. Läbi aegade asutuse poolt hõivatud isikuteandmete elektrooniline struktureeritud töötlemine on võimaldanud asutustel moodustada erinevaid andmekogusid ja nende põhjal ka andmeladusid täiendavaks andmete analüüsiks. Selles osas aga tuvastati, et kui asutusel on õigus andmeid töödelda õigusaktist tuleneva ülesande täitmiseks ja andmetest moodustavate andmekogude loomiseks on riigis erinormid, siis andmete täiendavaks töötlemiseks moodustatud andmelaod on jäänud ilma õigusliku regulatsioonita. See võib aga luua olukorra, kus asutustes toimub isikuandmete töötlemine aga isiku eest on see varjatud vastavalt asutuse poolse õigusega kehtestada andmetele juurdepääsu piiranguid.

2. PROAKTIIVNE TEENUS KUI TULEVIK

Arenenud majandused kes soovivad säilitada isikute usaldust riigi vastu, peavad ka väärtustama oma kodanikke privaatsust andmete töötlemisel ja hoidma isikute andmeid õiglaselt ja turvaliselt. Andmetöötluses kasutatavad ausa töötluse põhimõtteid nagu eesmärgipärane ja minimaalne andmehõive, avatus töötlemisel ning andmete kvaliteedi tagamine garanteerivad ka selle, et e-riigi teenuste kasutamine oleks ka päriselt turvaline ja seda ka kodaniku vaatest.[129] Avalike e-teenuste pakkumisel peab tagama ja järgima isikuandmete töötlemisele kehtestatud nõudeid. Vastavad isikuandmete töötlemise õigused, nõuded ja kohustused peavad olema kirjeldatud kehtivas siseriiklikus õiguses ja asutused peavad neist kinni pidama. Kuna e-teenuseid saab pakkuda ainult üle interneti, siis peab olema ka teenusega seotud andmekaitsetingimused leitavad samas keskkonnas. Nõuded selliste andmekaitsetingimuste kohta on toodud üldmääruse artikkel 12 kus on kirjas selged juhised millele asutused peavad tähelepanu pöörama andmekaitsetingimuste ettevalmistamisel ja esitamisel ning milline info tuleb kindlasti välja tuua. Selline teave peab olema ettevõtte internetilehelt kergesti leitav ja loetav[130] ning baseeruma põhimõtetel, mida ettevõtte sees ka tegelikult hinnatakse ja täidetakse. Kui see on nii, siis saab olla kindel, et vastav ettevõte on teadlik isikuandmete töötlemise nõuetest ja peab lugu ka üldmääruse põhimõtetest. Ka avaliku sektori asutused peavad kodanikelt kogutud andmete igasugusel töötlemisel kohaldama privaatsuspõhimõtteid ja need peavad olema kooskõlas kehtivate seadustega ja tagama, et neid ka järgitakse.[131]

2.1. Proaktiivne teenus sisult ja näitelt

Proaktiivne teenus on üks kahest riigi poolt pakutavast otsesest teenusest. Lisaks otsestele teenustele on kasutusel ka tugiteenus aga see on asutuse enda sisene teenus ja isikutele väljaspool asutust seda ei pakuta. Kui teenusete üldisel käsitlemisel käesoleva töö peatükkides 1.4 ja 1.5 jõuti järeldusele, et see on isikutele pakutav asutuse avalik ülesanne läbi mingi kindla või erinevate kanalite ja isiku tahteavalduse alusel, siis proaktiivne teenus on avaliku teenuse selline osa, mida

[129] Angelopoulos *et al.*, *supra nota* 111, 2.
[130] Dode, A. (2018, 21-22. September). *The challenges of implementing General Data Protection Law (GDPR)*. Article, 14th International Conference in "STANDARDIZATION, PROTYPES AND QUALITY: A MEANS OF BALKAN COUNTRIES' COLLABORATION", Tirana, Albania, 4.; Ustaran, E., Lovells, H. (Eds.) (2018). European Data Protection: Law and Practise. Portsmouth, USA: International Association of Privacy Professionals, 141.
[131] Angelopoulos *et al.*, *supra nota* 111, 2.

saab osutada juba teostatud ülesande käigus varasemalt hõivatud ja salvestatud andmete põhjal isikule personaalselt. See on teenus, mis on kavandatud ja täiustatud selliselt, et infosüsteemi on lisatud algoritmid ehk tehisintellekt, mis on võimeline analüüsima juba olemasolevat infot erinevates andmekogudes ja tuvastama olukordi, millal isikul tekib teatud õigus hüvele või siis mõni kohustus. Proaktiivse teenuse kontekstis kirjeldatakse ka sündmusteenust mida saab kasutada teatud juhtudel koos.[132]

Et sellisest kombineeritud teenusest paremat ülevaadet saada on Kõrge *et al.* selle väga hästi lahti seletanud, et kuidas sellised teenused tekivad ja miks neid vaja on. Ta on öelnud, et isikutele oluliste elusündmuste nagu sünni registreerimine, lasteaia ja kooli koha taotlemine, elukoha registreerimine või muud erinevad perekonnaga seotud toimingud on kõik riigi poolt pakutavad otsesed teenused läbi erinevate asutuste. Enamus selliseid teenuseid on ka digitaliseeritud ehk siis neid on võimalik läbi avalike e-kanalite või asutuste elektrooniliste vormide täitmisega kasutada. Osade teenuste puhul saab kõik vajalikud toimingud tehtud digitaalses keskkonnas, osasid saab vähemalt seal alustada aga tulem saadakse teisest kanalist. Eesmärk on see, et isikul puuduks vajadus asutusi füüsiliselt külastada. Samas võib aga olla ka selliseid toiminguid, mille tegemiseks peab isik suhtlema mitme erineva asutusega ja seega on leitud, et riigi poolt pakutavaid teenuseid tuleks hakata moodustama lähtudes isikukesksest lähenemisest.[133] Just sellise lähenemise saavutamiseks on hakanud riigid uurima ennetavate teenuste pakkumist, mis põhineks justnimelt elujuhtumiga seotud teenustest. Seega peaks selline teenus koondama sarnaste teenuste ühised osad ja kasutajale kuvatakse see justkui ühe teenusena aga taustal toimub siis automaatne andmete töötlemine vastavalt teenuse iseloomule. Sellega tagatakse isiku ja riigi vaheline minimaalne interaktsioon ja välistatakse korduv andmete küsimine.[134] Näiteks Maanteeameti e-teenus juhiloa vahetamisel on kehtiva tervisetõendi olemasolul täielikult digitaalne kui ei arvesta seda, et uuele juhiloale peab järele minema elukohana märgitud aadressi postkasti. Kui aga kehtivat tervisetõendit ei ole, siis tuleb külastada oma perearsti ja vastav tõend väljastatakse digitaalselt.

Just tehnoloogia areng on avanud väga palju uusi võimalusi sarnaste elusündmustega seotud isikustatud avalike teenuste arendamiseks mille keskmeks on isik, mitte asutus. Sirendi ja Taveter on tulevikku vaadates pakkunud välja ka proaktiivsete teenuste pakkumise niinimetatud push-

[132] Kõrge H., Erlenheim R., Draheim D. (2019). Designing Proactive Business Event Services. In: P. Panagiotopoulos, N. Edelmann, O. Glassey, G. Misuraca, P. Parycek, T. Lampoltshammer, B. Re (Eds), *Electronic Participation*, (73-84), 2.
[133] *Ibid.*
[134] *Ibid.*

meetodiga. Selle meetodi eripäraks ongi see, et riigid osutavad ise juba ennetavalt oma kodanikele õigeaegseid, kohandatud ja asjakohaseid teenuseid mitte nagu täna, kus kodanikud peavad ise otsima õiget asutust ja teenust mida ta peab kasutama vastavalt olukorrale.[135] Nende arvates tulekski avalikud teenused kohandada kodanike vajadustest lähtuvalt, mitte asutuste vajadusest lähtuvalt.[136]

Proaktiivsete teenuste teadvustatus ja kasutatavus tänaste teenuste hulgas on aga pea olematu kuigi selliste teenuste vajadusest räägitakse pidevalt[137]. Iseenesest tundub ju mugav, kui näiteks lapse sünni järgselt temale omistatud isikukoodiga saab uus ilmakodanik ka automaatselt ravikindlustuse, tehakse registreerimine perearsti nimistusse ja sissekirjutus vanema aadressile koos lasteaeda koha broneeringuga. Põhimõtteliselt puuduks vanemal igasugune vajadus suhelda erinevate asutustega ja piisaks ainult mõnest klikist näiteks eesti.ee-s.

Lisaks eelnevalt kirjeldatud Maanteeameti e-teenusele on kõige tuntumaks ja hästi töötavaks proaktiivse teenuse näiteks e-maksuameti tuludeklaratsiooni esitamine. Selle teenuse puhul on oluline see, et kodaniku eest on kõik vajalikud andmehõived juba eelnevalt automaatika poolt ära tehtud ja kodanikul piisab ainult MTA e-keskkonda sisse logida ja mõne klikiga on tal teada otsus[138], kas eelmise kalendriaasta jooksul on tulud-kulud deklareeritud korrektselt. Oma olemuselt toimub maksude- ja tulude deklareerimise automaatne teenus nii, et kindlaks määratud kuupäevaks on MTA-l olemas kõik eelneva kalendriaastaga seonduvad isiku ametlikud tulud, laenutagasimaksete intressi summad, kulutused koolitustele ja lastele ning põhimõtteliselt mõne klikiga on isikul olemas kinnitus tuludeklaratsiooni täitmise osas. See on teenus, mida reklaamitakse üle terve maailma ja tuuakse näiteks kui ühte suurimat viimase aja digitaalset edulugu Eestis. Samas sellise proaktiivse teenuse puhul, kus toimub automaatne andmehõive ei saa rääkida ainult tulemusele ja kiirusele orienteeritusest vaid tuleb ka veenduda, et üldmääruses toodud läbipaistvuse põhimõtted oleks täidetud. Kontrollides MTA ametlikku veebilehte on seal olemas isikuandmete töötlemise tingimused, kus on lihtsalt ja kergesti loetavalt üldsõnaliselt kirjas kuidas ja miks MTA isikuandmeid kasutab ja kaua neid hoiab. Samuti on kirjas info automaatsest isikuandmete töötlusest ning selgitatud mis otsuseid tehakse automaatselt ning kuidas saab isik esitada vajadusel vaiet ehk siis üldmääruse mõistes on läbipaistvus tagatud.

---

[135] Sirendi, Taveter, *supra nota* 97, 226-228.
[136] *Ibid.*
[137] *Ibid.*
[138] *Ibid.*

Samas puudub isikul aga igasugune info selle kohta milliseid IKT lahendusi ja andmekogusid kasutatakse ning mis andmeid nendes hoitakse. Lisaks jääb selgusetuks, mis ajahetkel on isiku andmeid kogutud ja töödeldud. Selliste asjade teada saamiseks on kaks võimalust: isikul tuleks eraldi pöörduda MTA poole vastava taotlusega ja seda informatsiooni küsida; või hakata ise edasi uurima, mille alusel on MTA-le ülesanded püstitatud ja milliseid andmekogusid nad kasutavad. Seega on tegu väga mugava proaktiivse teenusega ja justkui ka läbipaistvus oleks tagatud, aga kas ikka on?

2.2. Olemasolevate andmete (taas)kasutus

Proaktiivset teenust võib osutada riigi infosüsteemi kuuluvate andmekogudes olevate andmete alusel[139] mis ilmselgelt vähendab isikute kaasamist andmete töötlemise protsessi ja seeläbi suurendab läbipaistmatust üldmääruse mõistes. Kuna riikidel on lubatud siseriiklikult anda välja täiendavaid juhiseid ja õigusakte andmete seaduslikuks töötlemiseks, siis on lisatud hetkel kehtivasse AvTS redaktsiooni punkt, mis kohustab andmete andmekogusse kandmisel lähtuda ühekordse andmete küsimise põhimõttest[140]. Kahjuks puudub seaduse eelnõu seletuskirjas konkreetse punkti lisamise osas selgitus milleks sellist punkti oli tarvis ja mis eesmärki see täidab. Seletuskirjast võib lugeda vaid seda, et kui vältida andmete korduvküsimist, saab seeläbi parandada riigis olevate andmete kvaliteeti ja see tagaks paremad teenused isikutele.[141] Kuna selline üldsõnaline selgitus ei toeta antud punkti lisamise vajadust, siis tuleb leida täiendavaid toetavaid allikaid, et aru saada, mida tähendab ühekordne andmete küsimise põhimõte ja kas ning kuidas mõjutab see proaktiivsete teenuste pakkumist.

2015 aastal avaldati Euroopa Komisjoni poolt Euroopa digitaalse ühtse turu strateegia milles defineeritakse seda kui „isikute, kaupade, kapitali ja teenuste vaba liikumisega tagatud turgu, kus isikutel olenemata elukohast on võimalus pääseda ligi internetis toimuvale nii, et on tagatud ka

---

[139] TKHA §2 lõige 3.
[140] AvTS §43[1] lõige 3.
[141] Vabariigi Valitsus (2019). *Riikliku statistika seaduse ja avaliku teabe seaduse muutmise seadus 794 SE*. *Seletuskiri* Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6932ebe8-2dfa-4613-b627-f9c967a3d12f/Riikliku%20statistika%20seaduse%20ja%20avaliku%20teabe%20seaduse%20muutmise%20seadus 25. aprill 2020, 14.

isikuandmete kaitse kõrge tase.“[142] Selles dokumendis tuuakse välja, et avaliku sektori veebipõhised teenused on isikutele pakutavate teenuste kulutõhususe ja kvaliteedi seisukohalt otsustava tähtsusega. Tõhususe all peetakse silmas siis andmete kogumise ühekordsuse põhimõtet mis seisneb selles, et kasutatakse juba olemasolevaid andmeid selle asemel, et neid uuesti küsida isikutelt. Samuti mainitakse, et asutuste ja isikute vahelised kontaktpunktid on killustunud ja ebatäielikud ning ainult 48%-l asutustest on võimekust isikute kohta juba olemasolevat teavet uuesti kasutada. Seepärast peetakse strateegia dokumendis oluliseks andmete taaskasutamist ja andmekogude vahelist andmete ristkasutust, et suurendada teenuste pakkumise võimalusi ja oleks tagatud isikuandmete kaitse vastavalt õigusaktidele.[143]

Ühekordsuse põhimõte tähendab sellist kohustust asutustele, millega nad peavad tagama isikutele teenused selliselt, et väheneks isikutelt pidevalt ühtede ja samade andmete küsimine. Lisaks veel seda, et riigisisene õigus peab võimaldama pakkuda oma teenuseid selliselt, et ei tekitaks isikutele lisakohustusi. Pakutavad teenused peavad vastama erinevatele huvigruppidele ja asutused peavad jagama juba olemasolevat teavet omavahel selliselt, et isikutele jääks nendele üldmääruses sätestatud õiguseid.[144]

Aga kas ühe punkti lisamine siseriiklikusse õigusesse, mille kohta on vastavas seletuskirjas väga üldsõnaline kommentaar, tagab juba ühekorduse põhimõtte. Pigem mitte, kuid sellise punkti lisamine täiendab juba varasemalt AvTS-is toodud punke selliselt, et tekib terviklik arusaam andmekogude asutamise ja nendes andmete töötlemise osas. Nimelt AvTS § 43^1 lõige 2 ja lõige 3 ning AvTS §43^3 lõige 2 koosmõjus on tekkinud väga selge tingimuste kogum andmekogude asutamisele, kus lähtudes õigusele töödelda ka teistes andmekogudes olevaid andmeid ja pidades kinni andmete ühekordse küsimise põhimõttest ning keelust asutada eraldi andmekogusid samade andmete kogumiseks, toetab aga igati proaktiivse teenuse osutamist vastavalt TKHA-s toodud tingimusele.

[142] Euroopa Komisjon (2015). *Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele Euroopa digitaalse ühtse turu strateegia.* Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52015DC0192 26. aprill 2020, 3.
[143] *Ibid.*, 17.
[144] Euroopa Komisjon (2016), *supra nota* 102, 4.

2.3. Andmejälgija ja RIHA

Asutuste teenuste pakkumise läbipaistvuse suurendamiseks on Eestis alates 2003 aastast kasutusel riigiportaal eesti.ee mis peaks olema praktiliseks kontaktpunktiks isikutele, et leida infot asutuste poolt pakutavate teenuste kohta. Samuti peaks see võimaldama asutustel isikutega turvaliselt suhelda.[145] Seda portaali haldab Riigi Infosüsteemide Amet[146] (RIA) ja selles on olemas tehniline lahendus „andmejälgija", mille kaudu peaks saama „tutvuda enda isikuandmete töötlemisega riiklikes andmekogudes. Andmejälgija kajastab nii andmekogusiseseid toiminguid kui olukordi, kus isikuandmeid pärib mõni kolmas osapool. Ülevaate nägemiseks valige rippmenüüst teid huvitav andmekogu."[147]

Tulles tagasi nii Maanteeameti kui ka MTA proaktiivsete teenuste näidete juurde[148] ja lähtudes andmejälgija eesmärgist, tuleb kontrollida kas selles on kajastatud info, millal ja mis infot nii Maanteeamet kui ka MTA isiku kohta on kasutatud. Paraku on aga andmejälgija andmekogude vastavas valikus ainult neli infosüsteemi, millede seas kummagi asutusega seotud andmekogusid ei ole. See tähendab, et antud näidete puhul ei saa andmejälgijast teada milliseid andmeid ja millal on asutus isiku kohta kogunud ja töödelnud.

Aga nimekirjas on olemas Rahvastikuregister (RR) ja vastavalt AvTS § 43^6 lõige 2 kohaselt tuleb andmekogus nende andmete töötlemisel, mida kogub põhiandmetena teine riigi infosüsteemi kuuluv andmekogu, aluseks võtta vastava teise andmekogu põhiandmed. Isiku nimi, isikukood, aadress on RR põhiandmed, seega juhul, kui mõlemad asutused täidavad vastavat AvTS nõuet ja on võtnud isikuga seotud põhiandmed RR-ist, siis peab vastav töötluse kirje olema ka RR andmekogu all kajastatud. Autor kontrollis enda kohta vastavat infot ja sai kaks erinevat tulemust. Maanteeameti puhul oli olemas kirje „kuupäev, kellaaeg: MAANTEEAMET: ISIKUANDMETE JA SÜNNIKOHA PÄRING ISIKUKOODIDE JÄRGI", see näitab, et autori andmed võeti korrektselt RR-ist mis on andmete algallikaks. MTA puhul aga puudusid märkmed selle kohta, et asutus oleks RR-ist andmeid küsinud. Põhimõtteliselt võib see tähendada vähemalt kahte asja,

[145] Riigi infosüsteemised amet (2020). Riigi Infosüsteemi Ameti aastaraamat 2020. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_48lk_est_veeb_0.pdf 25. aprill 2020, 16.
[146] Vastav kohustus on sätestatud RT I, 25.03.2020, 10,Riigi Infosüsteemi Ameti põhimäärus§ 8 lõige 3 punkt 1).
[147] https://www.eesti.ee Kättesaadav peale isikutuvastamist antud keskkonnas https://www.eesti.ee/et/minuasjad/andmejalgija 04. mai 2020.
[148] Vt käesolev töö, 29-30.

esmalt seda, et MTA hoiab isikuga seotud põhiandmeid ka dubleerivalt enda andmekogudes ning seda, et võib toimuda erinevatest andmekogudest saadavate andmete pidev ja isikutele varjatud andmete töötlemine mis ei vasta üldmääruse põhimõtetele ja ei taga isikuandmete kaitset võimaliku riigi omavolilise andmete töötlemise eest.

Mis puudutab eesti.ee-s andmejälgija mitte kasutamist MTA poolt, siis otsest seaduse rikkumist antud juhul ei tuvastata, sest üheski seaduses või selle alusel välja antud muus õigusaktis ei ole kohustust asutustel andmejälgijat kasutada. RIA asutuse kodulehel on küll selline soovitus ja juhend ning muud vajalikud materjalid asutustele selle kasutamiseks aga e*xpressis verbis* kohustus siseriiklikus õiguses seda teenust kasutada puudub. Samas on sellise lahenduse kasutamine asutusele tasuta ja see tagaks ka täiendavalt isikuandmete töötlemise läbipaistvuse vähemalt andmete ristkasutamise osas.

Kuigi vastav MTA teenus on kodaniku jaoks tehtud hästi lihtsaks kaasneb sellega ka isikuandmete töötlemine ja üldmääruse valguses peab olema väga selgelt välja toodud millist avalikku ülesannet täidetakse ja kui suurel määral isikuandmeid töödeldakse. Selleks, et riik saaks pakkuda sarnaseid proaktiivseid teenuseid võetigi 2017 aastal vastu TKTA, mis justkui nagu lubaks proaktiivseid teenuseid pakkuda asutuse omal initsiatiivil, isikute eeldaval tahtel ja riigi riigiinfosüsteemi kuuluvate andmete alusel. Seda teenust võib pakkuda nii automaatselt kui ka isiku nõusolekul.[149]

2.4. Töötlemine nõusoleku alusel

Interneti teel teenuste tarbijatel palutakse regulaarselt anda luba või nõusolek oma isikuandmete kogumiseks ja kasutamiseks, millele vastutasuks nad saavad siis juurdepääsu teatud teenustele ja neid ka kasutada.[150] Kui erasektori puhul on oluline saada esmalt andmesubjektilt nõusolek andmete kasutamiseks[151] enne lepingulise suhte loomist mis seejärel annab hilisema õiguse isikuandmeid töödelda, siis avaliku sektori puhul ei ole nõusolek andmete töötlemiseks valikus. Avaliku sektori asutused saavad koguda ja töödelda isiku andmeid ainult kas mõne lepingulise ülesande nagu näiteks töölepingu seaduse või avaliku teenistuse seaduse alusel oma asutuse

[149] TKTA §2 lg 3.
[150] Efroni, Z., Metzger, J., Mischau, L., Schirmbeck, M. (2019). Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. *European Data Protection Law Review*, 5 (3), 352-366, 352.
[151] Üldmäärus art 6 lg 1 p a - juhul kui andmeid ei koguta juba lepingu loomise jaoks.

töötajate ja teenistujatega sõlmitud lepingu täitmiseks[152] või siis on töötlemine vajalik avalikes huvides oleva ülesande täitmiseks ning avaliku võimu teostamiseks[153] mis peab olema selgelt sätestatud liidu või liikmesriigi õigusaktis[154]. Ka TKTA-s on toodud ühe töötlemise alusena „isiku nõusolek" ja see on sätestatud liikmesriigi õigusaktis. Aga kas see on piisav, et tagada asutusel oma teenuste pakkumine isikutele?

Üldiselt on isiku nõusolek üldmääruse mõistes üks mitmest võimalusest isikuandmeid seaduslikult töödelda aga see ei kehti avalikes huvides oleva ülesande ja vastutava töötleja avaliku võimu teostamisel. Seda sellepärast, et üldmääruse artikkel 6 lõige 3 kehtestab nõude, et asutused tohivad isikuandmeid töödelda ainult kas liidu õigusega või vastutava töötleja suhtes kohaldatava liikmesriigi õigusega. Siin võib aga olla õiguste kollisioon, sest siseriiklikult kehtiv TKTA nagu annaks õiguse isiku nõusoleku alusel isikuandmeid töödelda.

Tegelikkuses on nõusolek aga oma olemuselt vabatahtlik ja teadlikult antav alus andmete töötlemiseks. Seega asutusega suheldes jätaks nõusoleku küsimine ja saamine eksliku mulje, nagu isikul oleks ka tegelikult otsustusõigus olukorras, kus asutus täidab temale pandud ülesannet ja õigus andmete töötlemiseks on asutusel õiguslikult juba olemas.[155] Sarnaselt on ka AKI rõhutanud, et nõusoleku mõiste kasutamisest tuleb hoiduda ka juhul, kui soovitakse isikut lihtsalt informeerida avaliku võimu teostamisest või oma ülesande täitmise käigus toimuvast andmetöötlusest.[156] Ka üldmääruses on selgelt märgitud, et nõusolekut ei tohi küsida olukorras, kus andmesubjekt ja vastutav töötleja on selgelt ebavõrdses olukorras ja seda eriti juhul, kui vastutav töötleja on avaliku sektori asutus.[157]

Nagu eelpool viidatud, peab nõusolek olema antud vabatahtlikult. Vabatahtlik tähendab seda, et isikul on tõeliselt vaba voli otsustada andmete töötlemise üle. Kui riik aga oma teenuste pakkumisel peaks igal juhul isiku andmeid töötlema, siis ei saa rääkida vabatahtlikult antud nõusolekust vaid seadusest tuleva ülesande täitmisest. Samuti ei ole nõusolek vabatahtlik, kui selle andmata jätmise tooks isikule kaasa kahjulikke või negatiivseid tagajärgi.[158] Kui nüüd uurida

[152] Üldmäärus art 6 lg 1 p b ja põhjenduspunk 44.
[153] Üldmäärus art 6 lg 1 p e.
[154] Üldmäärus põhjenduspunk 45.
[155] AKI (2019), *supra nota* 37, 39.
[156] *Ibid.*
[157] Üldmääruse põhjenduspunkt 43.
[158] Üldmääruse põhjenduspunkt 42.; Artikli 29 töörühm (2018). *Suunised määruse (EL) 2016/679 kohase nõusoleku kohta.* Kättesaadav:

proaktiivse teenuse olemust, siis on tegu teenusega, mille pakkumiseks on analüüsitud andmekogudesse kogutud fakte ja andmeid ning on tuvastatud, et isikul on tekkinud juba mingi õigus hüvele ja soodustusele või mõnele kohustusele. Seejärel osutab infosüsteem selle teenuse automaatselt või siis küsib nõusolekut antud soodustuse või kohustuse täitmise kohta.[159] Jääb aga selgusetuks, mille kohta sellisel juhul nõusolekut küsitakse, kas *ex post* juba tehtud töötluse kohta või *ex ante* tulevase töötluse osas, sest proaktiivne teenus võib endas hõlmata täiendavalt mitut edasist töötlemistoimingut ja kas need erinevad toimingud on ka selgelt välja toodud.

Maanteeameti näite puhul, lisades taotlusesse oma elukoha aadress ja nõustudes, et uus dokument saadetakse postiga on eeldatav, et isikuandmed töödeldakse edasi. Aga mis ulatuses? Kas juhilubade printimist ja koju toomist teeb asutus ise või volitab mõne teise asutuse seda tegema? Selle kohta igasugune info puudub. Samuti ka MTA näite puhul, kui selgub, et isikul tekib õigus riigilt teatav osa enammakstud tulust tagasi saada ja ta annab nõusoleku selle summa kandmiseks enda pangaarvele, siis kas on piisavalt üksikasjalikult sellise nõusoleku andmisel isikule selgitatud mida tegelikult see tähendab isikuandmete töötlemise mõistes. Autor peab siin silmas seda, et riigis teostab makseid isikutele ainult Rahandusministeerium, seega kas sellise nõusoleku andmisega on ka olemas tutvustav info selle kohta, et MTA peale enda poolset andmete töötlemist edastab need järgmisele asutusele, kes siis omakorda töötleb saadud andmeid. Mõlema näite puhul selgub, et isikule ei ole teada millised tema andmed ja kelle edastatakse. Seega võib üldmääruse põhjenduspunkti 43 tõlgendada nii, et kuna nõusoleku andmisel ei ole võimalik erinevate andmetöötluste osas eraldi nõusolekuid anda siis ei saa seda nõusolekut ka vabatahtlikult antuks pidada. Erinevate andmetöötluste all peetakse siis silmas täiendavaid töötluseid andmetega mida on veel tarvis teha ja mille kohta peab olema selgelt ja lihtsalt leitav vastav info. Sarnaseid olukordi võib tekkida ka teiste riigi poolt pakutavate soodustuste ja hüvede pakkumisel.

Autor leiab, et kui proaktiivset teenust pakutakse isiku nõusolekul, siis sellisel juhul toimub mitme üldmääruse põhimõtte rikkumine. Arvestades, et isikul on tekkinud õigus kas siis soodustusele või mõnele kohustusele, on ilmselgelt tegu asutuse avaliku ülesandega. Seega on nõusoleku küsimine ebavajalik ja vastav alus peaks olema kirjas seaduses või selle alusel välja antud õigusaktis mis annab ka aluse andmete töötlemiseks. Teiseks on kirjeldatud, et otsus tehakse juba olemasolevate

---

https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_nousoleku_kohta_wp259_rev_0.1_et.pdf 20. veebruar 2020, 5.

[159] Majandus- ja Kommunikatsiooniministeerium (2019). *Juhised määruse "Teenuste korraldamise ja teabehalduse alused" rakendajatele.* Kättesaadav: https://mkm.ee/sites/default/files/content-editors/lyhijuhised_tkta_rakendajatele_vers_1_1.pdf 23. märts 2020, 5.

andmete põhjal mis on asutusel olemas. Seega peaks olema isikule juba andmete kogumise momendil selge, mis tema andmetega tehakse ning kuidas ja kas neid edaspidi töödeldakse[160] või kui andmed on saadud mujalt kui isikult endalt, siis tuleb teda ka vastavalt teavitada[161], et andmed on saadud ja mida nendega edasi tehakse. Samuti ei ole autor peale kõnealuse MTA teenuse kasutamist saanud ühtegi täiendavat teavitust asutustelt, kes võisid selle protsessi käigus isikuandmeid kasutada. Vastava teavituse kohustus tuleneb üldmäärusest artikkel 14 teave, mis tuleb esitada juhul, kui isikuandmeid ei ole saadud andmesubjektilt.

Lisaks ei pea autor mõistlikuks asutustel töödelda isikuandmeid nõusoleku alusel vaid leida selleks mõni seaduslik alus, sest nõusolek on antud vabatahtlikult ja see tähendab, et selle võib ka igal ajahetkel tagasi võtta. Nõusoleku tagasivõtmine tähendaks asutusele täiendavaid üldmäärusest tulenevaid kohustusi, sealhulgas keeldu edaspidi neid andmeid töödelda, sest vastava nõusolekuga saadud andmete kasutamist saab piirata ja isik saab nõuda andmete ülekandmist.[162] Praktikas sellist asja aga ei juhtu ja isik neid õigusi tegelikult teostada ei saa, sest kui asutus täidab oma avalikku ülesannet siis jääb asutusele kohustus neid andmeid endiselt edasi hoida. Sellega rikutakse jällegi üldmääruse tingimusi kuigi seaduse alusel toimuva töötlemise puhul jääks andmete edasine töötlemine võimalikuks. Asutus ei saa ka kombineerida erinevaid töötlemise aluseid omavahel. Ehk teisisõnu, kui asutus täidab seadusest tulenevat ülesannet, siis ei saa poole töötlemise peal edasi tugineda nõusolekule. Vastav otsus, mille alusel andmeid töödeldakse tuleb ikkagi teha enne andmete töölust.[163]

2.5. Töötlemine automatiseeritud üksikotsuse tegemiseks

Proaktiivse teenuse pakkumisel tuleb tähelepanu pöörata sellele, et toimub automaatne andmete töötlemine ja kui leitakse alus soodustusele või kohustusele, siis osutatakse teenus automaatselt. Üldmääruses on kehtestatud väga selged reeglid automatiseeritud töötlusel põhineva üksikotsuse tegemise kohta ja selle üldise põhimõttena on kirjas, et otsust, mis toob isikule kaasa õiguslikke

[160] Üldmäärus artikkel 13.
[161] Üldmäärus artikkel 14.
[162] Üldmääruse artikkel 16-20 nõusoleku põhjal töötlemisega kaasnevad õigused.
[163] Artikli 29 töörühm (2018). *Suunised määruse (EL) 2016/679 kohase nõusoleku kohta.* Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_nousoleku_kohta_wp259_rev_0.1_et.pdf 20. veebruar 2020, 24.

tagajärgi ja põhineb üksnes automatiseeritud töötlemisel, teha ei tohi.[164] Erandina on lubatud sellist töötlemist kas lepingu täitmiseks või isiku nõusolekul aga nagu eelnevalt analüüsitud siis ei anna need asutusele alust oma teenuse osutamisel andmete töötlemiseks. Asutus tohib automatiseeritud otsust teha vaid juhul kui see on lubatud vastutava töötleja suhtes liidu või liikmesriigi õigusega ja kui on tagatud asjakohased meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitseks.[165] Lisaks on üldmääruse põhjenduspunktis 71 selgitatud, et vastutav töötleja peab rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et välistada valepositiivsed otsused mis mõjutaks märkimisväärselt asjaomaste isikute olukorda, käitumist või valikuid.[166] Kuigi märkimisväärset mõju on keeruline hinnata on töörühm oma juhendis väljatoonud, et seda on ka otsused, mis mõjutavad kellegi rahalist olukorda, näiteks nende laenukõlblikkust[167], leiab autor, et ka riigi poolt pakutav finantsiline soodustus ja hüve või kohustus, peaks kuuluma samasse kategooriasse. Seega on oluline, et otsuste tegemine oleks isikutele selge ja läbipaistev ning tagaks nende õigused. Proaktiivse teenuse puhul ongi esmaseks kriteeriumiks tagada automatiseeritud töötlemise õiguslikkus ja läbipaistvus.

Ka töörühm toob välja, et automatiseeritud töötlemise kõige tõenäolisem negatiivne tagajärg automatiseeritud otsuste tegemisel on märkimisväärne oht üksikisikute õigustele ja vabadustele, sest need protsessid võivad olla läbipaistmatud.[168] See aga võib omakorda tekitada täiendavat umbusaldust nii riigi kui tema teenuste vastu kuna puudub selgus, millisel määral ikkagi andmeid kasutatakse. Autori arvates ilmestab seda hetkel eelnõude infosüsteemis olev Siseministeeriumi algatatud eelnõu „Siseministri määruste muutmine ja kehtetuks tunnistamine“ nr 20-0461[169] kus eelnõu § 6 lõige 8 kohaselt täiendatakse Hädaabiteadete menetlemise andmekogu asutamine ja andmekogu pidamise põhimäärust järgnevalt „(10) tervise infosüsteemi vastutav töötleja või volitatud töötleja esitab andmekogusse arvatava kriisiolukorras kannatanu andmed.“ Jättes seejuures selgitamata ja lisamata, mis on need andmed mida siis kannatanu kohta edastatakse. Arvestades asjaolu, et info edastatakse tervise infosüsteemist automaatselt ja kuna tegu on

[164] Üldmäärus artikkel 22 lõige 1; Roig, A. (2017). Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology*. 8 (3), 1-17, 3.
[165] Üldmäärus artikkel 22 lõige 2.
[166] Artikli 29 töörühm (2018). *Suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta.* Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_automatiseeritud_tootlusel_pohinevate_uksikotsuste_tegemise_ja_profiilianaluusi_kohta_maaruse_2016679_kohaldamisel.pdf 20.veebruar 2020, 22.
[167] *Ibid.*
[168] Töörühm (2018), *supra nota* 166, 5.
[169] Siseministeerium (2020). *Siseministri määruste muutmine ja kehtetuks tunnistamine. EN_PäästeS rakendusaktide muutmine seoses PäästeS muutmisega.* Kättesaadav: https://eelnoud.valitsus.ee/main/mount/docList/40937f02-d3c2-40a3-bfc3-356fe2688ec6 28. aprill 2020.

kannatanu andmetega siis on üldmääruse mõistes tegemist terviseandmetega ehk eriliigiliste isikuandmete töötlemisega millele samuti kehtib üldine töötlemise keeld.[170] Vastava eelnõu seletuskirjas on selgitatud, et kannatanu andmeteks on isiku ees- ja perekonnanimi, isikukood või sünniaeg, seotus kriisiolukorraga ning kus ja millal on talle osutatud kriisiolukorra tõttu tervishoiuteenust. Autor leiab, et antud juhul ja lähtudes üldmäärus põhimõtetest peab selline info olema esitatud andmekogu põhimääruses, mitte seletuskirjas millel tegelik juriidiline võime puudub.

Eelnev näide ei täida täielikult automatiseeritud üksikotsuse tingimust vaid automatiseeritud töötlemist andmete edastamisel aga on heaks näiteks sellest, et ka praegu, kui üldmäärus on kaks aastat olnud aluseks isikuandmete töötlemisel, antakse ikka veel asutuse tasandil välja umbmääraseid korraldusi isikuandmete töötlemiseks. Ja kui selline üldsõnaline norm on kehtestatud automatiseeritud töötlustele, siis jääbki töötluse eesmärk ja sisu isikule läbipaistmatuks.

Antud juhul aga proaktiivse teenuse pakkumise kontekstis saab üldmäärust automaatotsuse tegemisel osaliselt ka pooldavalt tõlgendada. Kuigi artikkel 22 lõige 1 kehtestab üldise keelu automatiseeritud töötlemisele juhul, kui sellega kaasneb isikule õiguslik tagajärg, lubab seda siiski lõige 2 kui selline õigus on kehtestatud liidu või liikmesriigi õiguses ja sealjuures on välja toodud meetmed isiku õiguste ja vabaduste ning õigustatud huvide kaitseks. See tähendab, et tuleb järgida üldmääruse artikkel 5 lõige 1 toodud üldised põhimõtteid nagu seaduslikkus, õiglus, läbipaistvus ja isikutele informeeritus teenuse osutamisel. Isikutel peab olema selge, et kui asutus teeb automatiseeritud andmete töötlust ja sellega kaasneb õiguslik tagajärg, siis millistest andmetest lähtudes vastav otsus tehti ning kas ja kes on otsuse järgselt edasised andmete töötlejad ning mis ulatuses. Kui asutus täidab oma avalikku ülesannet teenuse pakkumisel[171] siis on tal õigus isikuandmeid töödelda, jääb vaid tagada üldmääruse artikkel 12 toodud kohustus edastada isikule töötlemisega seonduv info selgelt, lihtsalt ja arusaadavalt ja teave vastavalt artikkel 13 ja 14 toodud korrale.

[170] Üldmäärus artikkel 9 lõige 1; Quintel, T. (2018). Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals. *European Data Protection Law Review*, 4 (4), 470 – 482, 481.
[171] On täidetud üldmääruse artikkel 6 lõige 1 punkt e – avalikes huvides oleva ülesande täitmine.

Automatiseeritud töötlemisel tuleb asutusel jälgida ka nõuet, et kui võetakse kasutusele isikuandmete töötlemisel uusi tehnoloogilisi lahendusi[172] näiteks tehisintellekt ja kui toimub isikute süstemaatiline ja ulatuslik hindamine mis põhineb automaatsel isikuandmete töötlemisel[173], siis on vajalik teha ka andmekaitsealane mõjuhinnang. Proaktiivse teenuse eelduseks ongi automaatse analüüsi teostamine andmekogudes oleva info põhjal, seega on täidetud mõjuhinnangu tegemist toetavad tingimused. Nendeks toetavateks tingimusteks on süstemaatiline[174] ja ulatuslik[175] andmete töötlemine mis tähendab, et proaktiivseid teenuseid pakkuvad asutused peavad tegema ka vastava mõjuhinnangu. AKI soovitab, et kui asutuse tegevus põhineb õigusaktil ja mõjuhinnangu tegemine on vajalik, siis võiks mõjuhinnangu ära teha juba õigusakti eelnõu väljatöötamise raames ja lisada tulemus eelnõu seletuskirja.[176] Selline lähenemine toetab ka läbipaistvuse põhimõtet ja näitab, et asutus on teenuste planeerimisel juba läbi mõelnud ja kaarditanud võimalikud ohud mis võib isikuid vastava töötluse tulemusel ohustada.

2.6. Veelkord andmekogudest ja teenustest aga isiku vaatest

Angelopoulos *et al.* on kirjutanud, et „e-riikide usaldus on võrdelises seoses tema kodanike usaldusega süsteemide vastu. Seda siis seetõttu, et kodanike peamine mure on selles, et kuidas, mis eesmärkidel ja ulatuses riik kogub, kasutab, säilitab ja töötleb nende andmeid.“[177] Nagu juba tuvastatud[178] siis on üsna tõenäoline, et asutused ise andmete täpse töötlemise kohta infot jagades ei ole arvestanud sellega, et lisaks nende poolsele töötlusele tuleb ka välja tuua kaasatud osapooled, kellega kavatsetakse andmeid jagada. Ka riigi poolt pakutud andmejälgija ei taga isikutele infot nende kohta asutusel olemasolevatest andmetest ja töötlemisest. Samas on ka argumenteeritud, et asutuste andmetöötlus ongi erinev tavapärasest andmetöötlusest ja seepärast on ka privaatsuse tagamine keeruline. Andmeid kogutakse vastavalt oma ülesannetele selleks spetsiaalselt loodud andmekogusse. See aga tähendab, et asutustel on kogunud erinevate ülesannete täitmise sarnaseid andmeid.[179] Selline lähenemine on paraku just soodustanud ka andmeladude teket.

---

[172] Üldmäärus artikkel 35 lõige 1.
[173] Üldmäärus artikkel 35 lõige 3 punk a.
[174] AKI (2019), *supra nota* 37, töötlemine on süstemaatiline, kui see on planeeritud ja metoodiline.
[175] AKI (2019), *supra nota* 37, töötlemine on ulatuslik, kui valimis on üle 50 000 isiku.
[176] AKI (2019), *supra nota* 37, 27.
[177] Angelopoulos *et al.*, *supra nota* 111, 3.
[178] Vt käesolev töö peatükk 2.1 ja 2.3.
[179] Tsulukidze *et al.*, *supra nota* 14, 479.

Tsulukidze *et al.* toob ka välja selle, et asutused lähtuvad oma seaduslikust ülesandest ja õigusaktides toodud õigustest mis võib aga jätta tahaplaanile andmete kogumise tegeliku vajaduse ja analüüsi, milliseid andmeid tegelikult võiks vaja minna. Selline käitumine aga soodustab seda, et info on isikule juurdepääsu piiranguga ja tal puudub võimalus piirata ja veel vähem kontrollida, mida tema andmetega tehakse.[180]

Selle tõenduseks kontrollis autor ka RIHA-s olevate MTA infosüsteemide registreerimist ja tuvastas, et neid on kokku 64. Kui nüüd soovida leida mis andmeid isiku kohta MTA hoiab seoses tuludeklaratsiooni põhjal tagastava summa töötlemisega siis jääb see tegemata, sest RIHA-st info kättesaamine vastava teenuse ja avaliku ülesande täitmise osas on kõike muud kui lihtne, läbipaistev ja kergesti leitav. Sarnane olukord on kahjuks ka Maanteeametiga, millel on registreeritud 23 erinevat infosüsteemi ja juhilubadega ei seostu otseselt ükski. Aga samas on see ka arusaadav, sest RIHA eesmärk ei olegi isikuandmetega tehtavate toimingute läbipaistvamaks tegemine vaid riigi infosüsteemi haldamise läbipaistvuse tagamine, riigi infohalduse planeerimine ning riigi, KOV ja avalikke ülesandeid täitvate eraõiguslike isikute andmekogude koosvõime toetamine.[181] Seega ei peagi isikud sealt infot otsima vaid see on mõeldud asutustele.

Olles kontrollinud ühe Eesti enim kiidetud proaktiivse teenuse andmete töötlemise läbipaistvust kolmes erinevas keskkonnas, asutuse kodulehel, andmejälgijas ja RIHA-s on selgunud, et vaatamata info küllusele, mida võib leida, jääb siiski täielik läbipaistvus, vähemalt MTA puhul, saavutamata. Küllalti sarnane olukord asutuse kodulehel ja RIHA-s on ka Maanteeameti teenusega. Erinevalt MTA-st, Maanteeamet võtab põhiandmed RR-ist ja vastav info on ka kajastatud andmejälgijas vähemalt juhiloa vahetamise teenuses osas.

Olukord on seda kriitilisem, et juba 2015 aastal, kui Eesti Vabariigi Valitsus oma kabinetinõupidamisel kiitis heaks avalike teenuste omanike määratlemise analüüsi ja ettepanekud, oli juba toona välja toodud sarnaseid puuduseid riigi teenuste pakkumisel. Analüüsis on kirjas, et riigis puudub täpne ja õige ülevaade sellest milliseid teenuseid kasutatakse, kelle pakutakse ja milliseid kanaleid pidi. Samuti leiti, et AvTS § 28 lg 1 p 27 ja § 29 lg 1 sätted, mis kohustavad teabevaldajat avalikustama oma veebilehel andmeid üldkasutatavate teenuste osutamise tingimuste kohta, täidetakse väga erinevalt. Ka heideti ette seda, et andmekogude asutamisel ei ole

[180] *Ibid*; vt ka käesolev töö peatükk 1.7, teine lõik.
[181] RIHA § 3.

põhjalikult analüüsitud andmekogu loomise vajalikkust ja milliseid andmeid on võimalik juba teistest andmekogudest saada, et vähendada isikutelt juba olemasolevate andmete küsimist ning puudub analüüs andmete ja alusdokumentide säilitustähtaegadest.[182]

Ettepanekute osas on aga välja toodud, et on tarvis keskset töövahendit, millega saaks asutused kirjeldada oma teenuste üldised põhimõtted. Vastav keskkond peab olema veebipõhine, et aidata kaasa asutuse poolt pakutud teenuste osutamise selgitamise osas ning sisaldab asutuste e-kanalis pakutavate teenuste kirjeldusi.[183] Veebilehekülg riigiteenuste jaoks on loodud www.riigiteenused.ee ja sealt allasutusi otsides on kirjeldatud ka MTA, mis pakub 25-te teenust.[184] Lehel on kirjeldatud teenus „Füüsilise isiku tulud, maksustamine ja huvid“ aga igasugune muu info, kaasa arvatud millise õigusliku alusega seda teenust pakutakse sellelt lehelt ei leia. Seega see leht ei aita ka isikuid, et leida täpsemat infot teenuse sisu või andmete kasutamise kohta. Maanteeametil on sellel lehel välja toodud 43 teenust, nende seas ka „Juhtimisõigust tõendava dokumendi vahetamine, asendamine, juhtimisõiguse peatamine, äravõtmine ning kehtetuks tunnistamine ja peatamine“, kus on näha teenuse osutamise arvu, teenuse rahulolu protsenti ja teenusele kuuluvat ajakulu aga isikuandmete töötlemise osas seal samuti info puudub ja leht on suunatud pigem asutusele.

Teises peatükis analüüsiti reaalsete näidete põhjal kas ja mis ulatuses on tänases seisus proaktiivsete teenuste pakkumisel esitatav info kodanikule ehk kontrolliti üldmääruse mõistes andmetöötluse läbipaistvust. Näideteks oli e-maksuameti tuludeklaratsioon ja Maanteeameti juhilubade vahetus. Mõlemad teenused on vajalikud ja põhimõtteliselt mõne minutiga arvuti ekraanil teostatavad. Analüüs tuvastas, et mõlemad teenused kasutavad juba riigil olemasolevaid andmeid isiku kohta ehk siis toimub andmete ühekordne küsimine ja isikul täiendavalt info sisestamise vajadust ei olnud. Seega toimus andmete automaatne töötlemine, mis on ka üldmääruse artikkel 22 lõige 2 alusel lubatud, kui seda tehakse avaliku ülesande täitmisel. Proaktiivse teenuse vaatest on olemasolevate andmekogude andmete riskkasutus juba teenuse pakkumise eelduseks.

---

[182] Vabariigi Valitsus (2015), *supra nota* 75, 2.
[183] *Ibid.*, 8.
[184] Vahemärkusena, et lehel www.riigteenused.ee on „otsi“ inglise keelsena ja kui kasutada funktsiooni otsi, siis kuvatakse tulemus osaliselt inglise keelsena. Samuti on keeled lehe peal segamini kui valida põhikeeleks vene keel või inglise keel.

Proaktiivse teenuse pakkumise peamisteks puudusteks tuvastati aga TKTA-s sätestatud sõnastus ja avaliku sektori poolt ülesannete täitmisel toimuva andmetöötluse puudulik läbipaistvus.

TKTA sõnastuse kohapealt on sätestatud, et proaktiivset teenust võib osutada isiku nõusolekul. Selline punkt määruses on ebatäpne ja vajab ümbersõnastamist. Põhjuseid leiti neli, esimene on see, et asutused oma ülesannet täites peavad lähtuma ainult kehtivast õigusest ja nendele pandud ülesannetest ehk siis täidavad kindlat avalikku ülesannet. Seega on nõusoleku küsimine üleliigne tegevus ja isikut eksitav, sest jäetakse mulje nagu isikul oleks võimalus ka päriselt ise otsustada, kas ta soovib vastavat teenust riigilt või mitte. Teine põhjus on asjaolu, et nõusolekut ei tohi küsida olukorras, kus üks osapool on selgelt ebavõrdses olukorras ehk siis riigi ja isiku vahel on tegu sellise ebavõrdse olukorraga. Kolmandaks on asjaolu, et kui isikul puudub läbipaistvus tehtud ja plaanitud tegevuste osas ja kui ta ei saa anda iga erineva andmetöötluse osas eraldi nõusolekut, siis see nõusolek ei ole vabatahtlik. Ja neljandaks põhjuseks on see, et kui asutus on juba andmeid töödelnud mingi oma ülesande täitmise raames, siis ei ole lubatud poole töötluse pealt muuta töötlemise alust. See tähendab seda, et kui asutusel on õigusest tulenev alus andmete töötlemiseks, siis ei pea ka selleks nõusolekut täiendavalt küsima.

Samas võib olla olukord, kus riik on tuvastanud, et isikul on tekkinud õigus mingile soodustusele aga isik ka päriselt ei soovi seda teenust. Sellisel juhul on juba andmeid töödeldud ja isikule ei ole sellest teada antud. Mis tähendab, et ei ole tagatud läbipaistvuse põhimõtteid esitada isikule tema andmete kasutamise kohta selget teavet. Siin uuriti praktilisest vaatest, millised on võimalused isikul endal tuvastada tema andmetega tehtud või tehtavaid toimingud. Kasutatud näidete puhul selgus, et asutuste kodulehtedel on küll palju infot aga konkreetse teenuse andmetöötluse kohta infot napib. Samuti ei aidanud ka riigi poolt pakutav lahendus läbipaistvuse suurendamiseks mõeldud andmejälgija, sest sealt ei olnud asutuste kohta registreeritud mitte ühtegi infosüsteemi ja seega ei ole võimalik tuvastada, millal ja mis isikuandmeid kasutati. Analüüsiti veel ka RIHA ja www.riigiteenused.ee keskkondasid aga need on suunatud pigem asutustele endile ja pole mõeldud isikutele isikuandmetega tehtava toimingute otsimiseks.

TKTA-s toodud sõnastuses on veel mainitud töötlemise aluseks isiku eeldatav tahe ja asutuse oma initsiatiivi aga neid detailsemalt ei analüüsitud, sest kui asutus peab teenuseid pakkuma õiguslikul alusel, siis need kaks mainitud alust on juba eos välistatud ning sellised töötlemist lubavad alused puuduvad ka üldmääruses.

3. MILLISED LAHENDUSED ON JÄÄNUD KASUTAMATA

Kuigi üldmääruse rakendumisega jõustusid üle euroopalised ühtsed andmetöötlusreeglid, jäeti siiski „mitu (sh olulist) andmekaitseõiguslikku nüanssi liimesriikide reguleerida. See tähendab, et uus reaalsus andmekaitses ei saa olema algselt välja reklaamistud ühtne harmoniseeritud reeglistik, vaid jätkuvalt killustunud tervikpilt.“[185] Portmeister ja Nisu toovad veel välja, et seetõttu on ka tekkinud olukord, kus kohalduvate nõuete mitmekesisus ja variaablus eri liikmesriikide lõikes on praktiliseks probleemiks lisaks andmetöötlejatele ja järelevalveasutustele ka andmesubjektidele, kes peavad aru saama, millised õigused neil igal andmetöötluse üksikjuhtumil tegelikult on.[186] Lisaks liidu õigusele on isikuandmete kaitse tagamiseks avaldatud erinevaid juhiseid, soovitusi ja arvamusi ka liikmesriikide endi andmekaitse järelevalveasutuste, sealhulgas AKI ja töörühma poolt. Viimati mainitud dokumendid ei ole aga siduvad õiguse mõistes vaid pakuvad täiendavaid selgitusi mis aitavad asutustel kergemini aru saada üldmääruse nõuetest.[187]

Samas annab selline teatav volitus liikmesriigile võimaluse täiendada siseriikliku õigust ka selliselt[188], mis teeks läbipaistvuse tagamise ka isikutele arusaadavamalt selgemaks ja kätte saadavamaks.

3.1. Privaatsusikoonid

Privaatsustingimuste kajastamise kohta on Custers *et al.* kirjutanud tuginedes Hollandi näitele, et keskeltläbi 11% veebiteenuste kasutajatest loevad ainult kogu andmetöötlust ja privaatsust kirjeldavaid dokumente.[189] Ta toob välja, et nende dokumentidega tutvumine on väga ajamahukas ning uuringud on tuvastanud, et aastas kulub ühel inimesel keskmiselt 244 tundi, et tutvuda kõikide vastavate dokumentidega.[190] Asutuste puhul on lisaks veel tarvis tutvuda vastavate asutuste

[185] Portmeister, K., Nisu, N. (2018). Liidusisese kohalduva õiguse dilemma isikuandmete kaitse üldmääruses. *Juridica*, 2, 125-136, 125.
[186] *Ibid.*
[187] Fabiano, N. (2019). Ethics and the Protection of Data. *The Journal on Systemics, Cybernetics and Informatics*, 17 (2), 58-64, 60.
[188] Kamara, I. (2017). Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology*, 8 (1), 1-24, 2.
[189] Custers, B., Dechesne, F., Sears, A. M., Tani, T., van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 34 (2), 7.
[190] *Ibid.*

seaduste ja avaliku teenuse pakkumise aluseks olevate õigusaktidega. Kui neid erinevaid dokumente lugeda võib sattuda keeluliste juriidiliste ja vahel ka tehniliste terminite otsa mis tekitavad pigem rohkem segadust kui arusaamist. Seega oleks õigustatud küsimus, kui palju tuleks informatsiooni pakkuda, et oleks piisavalt arusaadav kodanikule.

Kuna üldmääruse kontekstis on läbipaistvuse tagamine üks olulisemaid tingimusi ning seda teostades peab edastav info olema isikule kergesti arusaadav siis ei tohi lugejat liigselt koormata ning sellest peab aru saama ka sihtrühma keskpärane liige[191]. Seepärast on ühe võimalusena üldmääruse artikkel 12 lõige 7 näinud ette ka võimaluse esitada vastav info ikoonide kujul. On eeldus, et kui isikud loevad tingimusi ja nendes tehtud muudatusi üksnes põgusalt siis visuaalsed efektid ja ikoonid teeksid informatsiooni edastamise oluliselt selgemaks.[192] Seda muidugi eeldusel, et on olemas kokkulepe milliseid ikoone läbivalt kasutatakse. Sarnaselt toimib ka liiklusseaduses kehtestatud nõuete teostamine liikluses läbi liiklusmärkide, mis on oma olemuselt ka infot edastavad ikoonid.

Tulenevalt sellest, et nii privaatsustingimused kui ka õigusaktides olev tekst ja info võib olla keeruline ja raskesti arusaadav, peakski olema täiendavalt kasutusel ka näiteks privaatsusikoonid. Ikoonidega peaks olema lihtsam anda infot edasi kui tekstidega ja sellega saaks kasutajad kiiremini ja selgema ülevaate milleks ja kuidas nende andmeid kasutatakse või kavatsetakse kasutada.[193] Efroni *et al.* on oma uurimuses tuvastanud, et piltidel on eelis teksti ees, sest neid on lihtsam meelde jätta ja seostada mingi tegevusega. Nad leidsid veel selliseid seoseid, et inimesed reageerisid paremini ja kiiremini hoiatuspiltidele kui sama sisu edastatavatele hoiatustekstide. Ja eriti suureks eeliseks peavad nad seda, et piltidel on universaalsuse mõõde see tähendab, et nendel puudub keeleline piirang ja neid ei pea tõlkima[194] seega saaks need kasutusele võtta kogu liidu piires kui Euroopa Komisjon need näiteks kehtestaks.

Kuigi üldmääruse artikkel 12 ei anna täpsemaid juhiseid kohustuslike ikoonidega edastatava info kohta, viitab see siiski üldmääruse artiklitele 13 ja 14[195] ning täpsustab, et ikoonid võivad täiendada nendes artiklites sätestatud teabekohustust. Samas ei piira ega ka kohusta artikkel 12 kogu info markeerimist ikoonidega vaid annab suunise, et neid tuleks kohaldada artiklites 13 ja 14

[191] Töörühm (2018), *supra nota* 46, 7.
[192] Töörühm (2018), *supra nota* 46, 16.
[193] Efroni *et al.*, *supra nota* 150, 358.
[194] *Ibid.*
[195] Üldmäärus artikkel 12 lõige 7.

toodud nõutava teabe näitamise osas mis erineb näiteks artiklist 15 esitatud teabest.[196] Efroni *et al.* on veel leidnud, et ikoonide võimaliku sisu osas tuleks artikli 12 lõikeid 7 ja 8 tõlgendada laiemalt, sest üldmääruse eesmärk on isikut igakülgselt teavitada. Ta toetub üldmääruse põhjenduspunktile 60, et "vastutav töötleja peaks esitama andmesubjektile igasuguse täiendava teave, mis on vajalik õiglase ja läbipaistva töötlemise tagamiseks, võttes arvesse konkreetseid asjaolusid ja konteksti", ja et seda teavet võib esitada koos standardsete ikoonidega.[197] Järelikult ei piirata ikoonide kasutamist ainult artiklites 13 ja 14 toodud info esitamisega.[198]

Info esitamisel ikoonidega tuleks aga eelnevalt kokku leppida, et mida me tahame ikoonidega näidata ning mis alustel ja tingimustel tuleb ikoone kasutada. Võib valida kas ettevõtteid iseloomustavad ikoonid mis annavad isikule turvalisuse tema andmete töötlemisel või siis konkreetselt teatavat töötlemise liiki toetvad ikoonid. Neid ikoone võib kasutada nii era- kui ka avalik sektor, samas kui hakata asutusi üldiselt hindama ühe konkreetse iseloomustava ikooniga, siis oleks vastuvõetamatu, kui mõni asutus ei saa seda ikooni, mis näitaks, et see asutus justkui nagu ei hooliks isikute andmete kaitsmisest. Kõiki töötlemisel kasutusel olevaid aspekte ja pikki privaatsustingimusi ei ole mõistlik ega ka tulemuslik viia üle ikoonidele sest ka ikoonide paljusus viib selleni, et inimesed ei hakka nendele enam tähelepanu pöörama ja nendest vaadatakse „läbi".[199] Elfoni *et al.* tuginedes Eurobaromeeter 2015 aasta raportile, toob välja, et EL riikide kodanikud on teadlikud ja oskavad hinnata erinevaid ohte ja riske isikuandmete töötlemisel.[200] Risk on aga üldmääruses hinnatav termin ja jätab asutustele ruumi tõlgendamiseks. Samas kui hinnata riski sarnaselt automatiseeritud töötlusel mõjuhinnangu aspektidega siis võiks igale proaktiivsele teenusele ühtsetel alustel ikoonid ära defineerida.[201] Seega võiks ikoonide kasutamine olla sarnastel tingimustel nagu mõjuhinnangu tegemine ehk siis kohustuslik asutustele. Kui AKI soovitas mõjuhinnangut eelnõu juures välja tuua, siis ikoonid võiks olla leitavad näiteks RIHA-s või www.riigiteenused.ee lehel iga vastava andmekogu või teenuse juures. Ühe variandi võimalikest ikoonidest võib leida aadressilt: http://gdprbydesign.cirsfid.unibo.it/dapis-2/

[196] Efroni *et al.*, *supra nota* 150, 360.
[197] Üldmäärus põhjenduspunk 60.
[198] Efroni *et al.*, *supra nota* 150, 360.
[199] *Ibid.*
[200] Efroni *et al.*, *supra nota* 150, 361.
[201] Vt käesolev töö 40; *supra nota* 174 ja 175.

3.2. Mida saab teha riik

2017 aastal on AKI peadirektor olnud seisukohal, et üldmääruse artikkel 6 lõige 1 punkt e) mis sätestab andmetöötluse avalikes huvides, tuleb tõlgendada nii, et andmete töötlemise õigus ongi kehtestatud liikmesriigi õigusega ja andmete töötlemiseks ei ole vaja eraldi juurde kirjutada millisest õigusest töötlus tuleneb. [202] Lisaks, on ta et öelnud, et avaliku ülesande tuletamine seaduse eesmärgist peaks olema piisav ja täiendavat erinormi töötlemis aluste osas tekitada pole vaja. Küll aga toob ta välja, et eriliiki isikuandmete töötlemis selline lähenemine ei ole õige ja soovitab täiendavaid eeskirju ka seaduse tasandil.[203] Töö autori arvates on tõesti selline lähenemine piisav, kui peetakse silmas ainult asutusi. Samas ongi kogu selle üldmääruse tõlgendamise juures jäänud silma see, et juhendeid ja soovitusi jagatakse ainult asutustele. Samas isikutele, kelle andmeid tegelikult soovitakse kaitsta, puuduvad igasugused juhendid selle kohta, kuidas nad saaks ka päriselt leida infot selle kohta, milline asutus mis infot isiku kohta hoiab.

Töö autor tuvastas ka MTA ja Maanteeameti teenuse näitel, et AKI peadirektori tollane seisukoht täiendava erinormi tekitamise osas on viinud olukorrani, kus sihtrühma keskmise tasemega isikul on pea võimatu tegelikult aru saada kas ja mida tähendab asutuse poolt küsitud nõusolek ja milline andmete töötlus sellega tegelikult kaasneb. Samuti tänaseks loodud vahendid kontrollimaks andmete kasutust ei võimalda tegelikult tuvastada kas ja millal on riik isikuandmeid kasutanud. Riik on eeldanud, et isikud oskavad ise leida informatsiooni nii asutuste kodulehtedelt kui ka erinevatest õigusaktidest. Lisaks on tehtud asutustele töövahendid läbipaistvuse suurendamiseks aga need on kasutamata jäetud või siis kasutusel minimaalselt. Praeguses olukorras ei ole võimalik teostada kontrolli põhiseadusest tuleneva kodaniku eraellu sekkumise keelu kohta mis kehtib riigiasutustele, KOV ja nende ametiisikutele[204] sealhulgas ka isikuandmete omavolilist töötlemist mugavusteenuste arendamisel ja omaalgatuslikul teavitamisel[205].

---

[202] Andmekaitse inspektsioon (2017). *Andmekaitse Inspektsiooni peadirektori seisukohad uue andmekaitseõiguse kontseptsiooni asjus*. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/reform/jum_oigusraamistiku_kontseptsiooni_markused_27.04.2017.pdf 20. veebruar 2020, 7.
[203] *Ibid.*
[204] PS § 26 lõige 2.
[205] AKI (2017), *supra nota* 202, 7.

Põhiseadus peab tagama informatsiooni avatuse põhimõte ja selle, et igaühel on õigus ise otsustada kas ja kui palju tema kohta andmeid kogutakse, säilitatakse ja kasutatakse.[206] Seega on oluline, et õigusaktides, milledes käsitletakse asutuste poolset isikuandmete töötlemist, tuleb selgelt ja detailselt välja tuua sellekohane info mis andmeid ja mille jaoks töödeldakse, mitte aga ühe lauseline üldine tekst sellest, et me kogume andmeid.[207] Samuti tuleb teha kohustuslikuks andmeladude registreerimine RIHA-s ja mitte piirduma ainult sellega, et juhul kui andmekogu kasutatakse asutuse siseste protsesside jaoks. Ka asutuse sisesed protsessid peavad olema läbipaistvad, seda eriti juhul kui nendes kasutatakse isikute andmeid. Autor peab vajalikuks rõhutada, et isikuandmete omanikuks on siiski isik ise, mitte asutus, kellele käes on need andmed. Asutus, kes omab isikute andmeid, nimetatakse vastutavaks töötlejaks. Seega isikul on õigus teada, mida ja mis otsuseid tema andmete põhjal tehakse ja riik peab tagama läbipaistvuse.

Turk ja Pild lähtuvad põhimõttest, et täiendav õiguslik reglementeerimine tuleb kasuks vaid siis kui kehtivad seadused viiksid sobimatule või ebaadekvaatse tulemuseni.[208] Paraku aga tuleb antud juhul üle vaadata nii andmekogude põhimäärused, vajadusel AvTS andmekogude osa kui ka kokku leppida termini andmeladu või andmeait kasutus ja kuidas toimub nende registreerimine ning nendes olevate andmete töötlus. Lisaks on tarvilik kokku leppida keskkonnad, kus kodanikud saaksid võimalikult lihtsa vaevaga kontrollida oma andmete eesmärgipärast kasutamist.

Proaktiivsete teenuste pakkumine on ka üks Euroopa peamini suundi ja kui on eemaldatud piirangud ning tagatud üldmääruse mõistes läbipaistvus võib selliseid teenuseid tehnoloogiliste lahendustega täiustada ja arendada ning Eesti saaks olla siin jälle teerajajaks. AvTS on juba täna vähemalt andmekogude osas selgelt reguleerinud, millal ja mis andmete jaoks tohib luua uusi andmekogusid ja millistel tingimustel. Nagu eelnevalt mainitud, tuleb reguleerida ka andmeladusid.

Sarnaselt 2017 aastal AKI peadirektori seisukohale[209] on täna endiselt oluline, et isikute teavitamise ja osaluse kohustuse täitmiseks on tarvis ka päriselt andmejälgija kasutusele võtta, seda eriti asutuste andmekogude ristkasutuse tuvastamiseks. Lisaks tuleb andmejälgija vastavalt

---

[206] PS § 26 põhjenduspunkt 24; RKHKo 12.07.2012, 3-3-1-3-12, p 19; RT I 1998, 47, 700. Eesti infopoliitika põhialuste heakskiitmine § 25.
[207] Vt käesolev töö, 38.
[208] Turk, K., Pild, M. (2019). Kratiga või kratita – see on küsimus: Robotitest ja tehis-intellektist tsiviilõiguslikult. *Juridica*, 1, 43-55, 4.
[209] AKI (2017), *supra nota* 202, 10.

AvTS §43[9] toodud teiste riigi infosüsteemi kindlustavate süsteemidega teha kohustuslikuks asutustele.

RIHA määruse § 5 lõige 2 sätestab, et lisaks riigi infosüsteemi haldamise põhimõtetele kohaldatakse isikuandmete töötlemisele riigi infosüsteemis IKS § 6 sätestatud isikuandmete töötlemise põhimõtteid. Autori arvates on aga jäänud peale uue IKS vastuvõtmist RIHA määrus uuendamata, sest antudjuhul kehtiva IKS § 6 reguleerib isikuandmete töötlemise erialuseid teadus- ja ajaloouuringu ning riikliku statistika vajadusteks. Küll aga oli kehtetus IKS § 6 välja toodud isikuandmete töötlemise põhimõtted.

Täiendavalt tuleb uuendada RIHA määruse § 6 lõige 4 andmekogu dokumentatsiooni koostamise osas, kui kontrolli tulemusel selgub, et vajalikke andmeid kogutakse juba mõne asutatud andmekogu kooseisus, esitab uue andmekogu asutaja RIHA kaudu selle andmekogu vastutavale töötlejale taotluse andmete kättesaadavaks tegemiseks riigi infosüsteemis. Autor tegi järelepärimise RIA-le, et täpsustada kus RIHA-s selline taotluse vorm asub siis vastati, et selline võimalus oli vanas RIHA versioonis[210]. Uus RIHA versioon on kasutusel alates 2018.

Käesolevas peatükis käitles autor peamiselt neid punkte, kus saaks proaktiivsete teenuste pakkumisele kaasa aidata. Analüüsi tulemusel leiti, et üldmäärus võimaldab kasutusele võtta andmetöötlust visualiseerivad ikoonid. Neid ikoone võib omistada nii üldmääruse põhimõtetest kinni pidavatele asutustele kui ka erinevate andmetöötluste kohta. Selliste ikoonide kasutusele võttu saab reguleerida kas Euroopa Komisjon üle liidu või siseriiklikult AKI. Ikoonid võiksid olla nähtavad RIHA-s ja riigiteenuste portaalis.

Siseriiklikult tuleks täiendavalt TKTA-le muuta ka AvTS, kuhu tuleb selgelt sisse viia andmeladude mõiste. Lisaks tuvastati, et RIHA määrus tuleb kooskõlla viia kehtiva IKS-ga ja RIHA veebikeskkonna võimalustega. Riigiteenuste lehekülg tuleb korda teha, et saaks sinna ka vajadusel töötlemise ikoone lisada. Ning andmejälgija tuleb ka päriselt kasutusele võtta.

[210] Autori kirjavahetus Riigi infosüsteemi ametiga 05. mai 2020.

KOKKUVÕTE

Käesolevas magistritöös otsiti vastust, kas TKTA § 2 lõikes 2 sätestatud otsese avaliku teenuse ja lõikes 3 sätestatud proaktiivse teenuse pakkumine asutuste poolt on kooskõlas üldmäärusega ning jõuti järeldusele, et tänases sõnastuses ei ole korrektne kasutada TKTA-d kui siseriikliku õigusega pandud kohustust asutustele, millega on lubatud pakkuda avalikke teenuseid ja millega saaks tagatud ka isikuandmete töötlemise läbipaistvus.

Magistritöös analüüsiti, kas peale üldmääruse jõustumist on tarvis teha muudatusi TKTA-s sätestatud otsese avaliku teenuse ja proaktiivse teenuse praeguses sõnastuses ning selgitada välja millises osas esineb praktilisi puudujääke proaktiivse teenuse pakkumisel läbipaistvuse tagamisel kahe olemasoleva e-teenuse näitel.

Antud töö hüpoteesiks oli, et TKTA §2 lõige 3 sätestatud proaktiivse teenuse osutamine asutuse omal initsiatiivil, isiku nõusolekul ja eeldataval tahtel ei ole kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 (üldmäärus) artikkel 12 läbipaistvuse põhimõttega, leidis kinnitust.

Käesolevas töös analüüsiti mõistet läbipaistvus isikuandmete töötlemisel ja tuvastati, et lisaks üldmäärusele on see ka e*xpressis verbis* põhimõte ka liidu tasandil ning ELTL artikkel 15 kohustab kõiki asutusi seda ka järgima. See tähendab, et isikuandmeid töötlevad asutused peavad tegema isikutele lihtsas ja selges keeles kergesti leitavaks sellise info, mis puudutab isikuandmete erinevat laadi töötlemist ning sellega kaasnevaid ohtusid, kohustusi ja võimalikke muid tagajärgi.

TKTA määrus mis vastuvõtmisel oli kooskõlas direktiivi ja IKS-ga andis õiguse asutustele pakkuda proaktiivseid teenuseid on täna muutmata kujul ja autori analüüsi põhjal vastuolus üldmääruse läbipaistvuse tagamise põhimõtetega, sest selles toodud teenuse pakkumise alused ei vasta üldmääruses põhimõtetele:

- **Andmete töötlemine asutuse omal initsiatiivil** – üldmääruses puudub selline isikuandmete töötlemise alus. Samas on üldmääruses lubatud isikuandmeid töödelda vastutava töötleja suhtes kohaldatava liikmesriigi õigusega. Praegune sõnastus aga ei anna õiguslikku alust isikuandmete töötlemiseks, sest andmete töötlemise eesmärk määratakse

kindlaks õiguslikust alusest tulevast avalikust huvist ja täidetavast ülesandest. Asutuse initsiatiiv isikuandmete töötlemiseks ei ole seega kooskõlas töötlemise alustega;

- **Isikute nõusolekul** – üldmääruses on selline andmete töötlemise alus olemas kuid seda ei saa kasutada seaduses sätestatud ülesande täitmiseks.
- **Eeldataval tahtel** – paraku ei suutnud autor leida üldmäärusest ega ka siseriiklikust õigust sellist juriidilist mõistet nagu eeldatav tahe. Selline mõiste esines erinevates strateegia dokumentides aga mitte õigusaktides. Seega ei saa ka seda kasutada andmete töötlemiseks.
- **Riigi infosüsteemi kuuluvate andmekogude alusel** – infosüsteemi kuuluvad andmekogudes olevate andmete (taas)kasutamine on juriidiliselt õiguspärane tulenevalt AvTS toodud põhimõtetele andmekogude loomisel. Kuid reaalsed lahendused täna ei paku läbipaistvust andmete töötlemisel.

Analüüsi käigus leiti veel, et kui asutusel on õigus andmeid töödelda õigusaktist tuleneva ülesande täitmiseks ja andmetest moodustavate andmekogude loomiseks on riigis erinormid, siis andmete täiendavaks töötlemiseks moodustatud andmelaod on jäänud ilma õigusliku regulatsioonita. See võib aga luua olukorra, kus asutustes toimub isikuandmete töötlemine aga isiku eest on see varjatud vastavalt asutuse poolse õigusega kehtestada andmetele juurdepääsu piiranguid.

Andmetöötluse läbipaistvuse kontrollimiseks kasutati näitena e-maksuameti tuludeklaratsiooni ja Maanteeameti juhilubade vahetuse e-teenust. Mõlemad vajalikud ja arvutis kiiresti teostatavad teenused kuid analüüsi käigus tuvastati läbipaistvuse osas puudusi; asutuste kodulehtedel on olemas üldised asutuses andmete töötlemise tingimused aga puuduvad täpsed tingimused teenuste pakkumisel toimuva andmetöötluse osas. Lisaks ei paku ka riigi poolt selleks puhuks tehtud andmejälgija täit ülevaadet andmete töötlusest. RIHA ja riigiteenused.ee lehtedelt on leitav mõlema asutuse infosüsteemid ja teenused aga nendes puudub info kasutatavate isikuandmete koosseisude ja töötlemise osas.

Läbipaistvuse suurendamiseks leiti analüüsi tulemusel, et üldmäärus võimaldab kasutusele võtta andmetöötlust visualiseerivad ikoonid. Neid ikoone võib omistada nii üldmääruse põhimõtetest kinni pidavatele asutustele kui ka erinevate andmetöötluste kohta. Selliste ikoone kasutusele võttu saab reguleerida kas Euroopa Komisjon üle liidu või siseriiklikult AKI. Ikoonid võiksid olla nähtavad RIHA-s ja riigiteenuste portaalis.

Siseriiklikult tuleks täiendavalt TKTA-le muuta ka AvTS, kuhu tuleb selgelt sisse viia andmeladude mõiste. Lisaks tuvastati, et RIHA määrus tuleb kooskõlla viia kehtiva IKS-ga ja RIHA veebikeskkonna võimalustega. Riigiteenuste lehekülg tuleb korda teha, et saaks sinna ka vajadusel töötlemise ikoone lisada. Ning RIA poolt loodud andmejälgija tuleb ka päriselt kasutusele võtta ja seda on ka AKI peadirektor juba varasemalt rõhutanud.

SUMMARY

MAKING PROACTIVE SERVICE DATA PROCESSING MORE TRANSPARENT TO CITIZEN

Priit Davel

The purpose of this Master's Thesis is to analyse whether the regulation no. 88 Principles for Managing Services and Governing Information § 2 (2) defined direct public services and § 2 (3) defined proactive services which are provided by an authority are in accordance with the European Parliament and the Council Regulation (EU) 2016/679 (GDPR). More precisely, whether regulation no. 88 *as is* in current wording can provide lawfulness to authority to process personal data in order to provide public services and fulfils the GDPR transparency requirement.

The author of this thesis stated the hypothesis that regulation no. 88 § 2 (3) defined proactive services provided by an authority on its own initiative, in accordance with the consent of a person and with the presumed will of persons are not supported by the GDPR article 12 transparency requirement.

To support the thesis hypothesis, the author focuses on whether after GDPR enforcement there is a need to amend regulation no. 88 wording which allows authority to process personal data and provide direct and proactive services to public and tests the proactive service transparency with two commonly used and known e-service from the Road Administration and Tax and Customs Board (ETCB).

The research method of this paper is qualitative analytical and the author has analysed different international, European Union and local legislation, compares scientific sources and applicable guidances.

In the first chapter, the author examines the GDPR and transparency principle formation and how authority must comply in order to fulfil the transparency requirement. In addition, the legal basis of authorities, its tasks to carry out the public interest and lawful personal data processing was analysed. Public Information Act was examined as it sets rules to state how to handle public data and sets the overall rules how and when state can create and use databases.

Second chapter introduces the aim and need for proactive services and two such services were analysed in order to understand whether they are in accordance with GDPR article 12 stated transparency requirement. The proactive service transparency test included applicable authority websites, data tracker provided by state portal www.eesti.ee, state information system management system (RIHA) and portal for public services www.riigiteenused.ee.

In the third chapter, the author concluded possible solutions to make proactive service provided by authorities more transparent with privacy icons and gave some suggestions in order to change local regulation. Mainly RIHA regulation as it seems to be outdated and Public Information Act as it regulates the state databases but does mention anything about data warehouses.

As a conclusion, the author found that transparency within public authority is not only stated in GDPR but is also *expressis verbis* stated in Lisbon Treaty which means authorities must comply with it and provide information about any transaction done with personal data. As a result regulation no. 88 *as is* in current wording and should provide lawfulness to authority to process personal data in order to provide public services does not fulfil the GDPR transparency requirements on data processing:

- **by an authority on its own initiative** – GDPR states that processing in order to carry out public interest or exercise official authority must me clearly states in Union law or in Member State law to which the controller is subject. Therefore authority own interest does not provide lawfulness to process personal data;
- **in accordance with the consent of a person** – the author identified at least four occasions why authorities can not use consent as legal basis to provide services;
- **with the presumed will of persons** – GDPR does not recognise such possibility neither could the author find such possibility in any legislation or scientific source;
- **based on the data in the databases belonging to the state information system** – as in general such processing can be lawful and is supported in Public Information Act. However there are strict limitation if data is processed automatically and the processing transparency is the key issue which is not currently filled.

Additional findings were that data warehouses are not regulated in law which makes transparency basically non existent. Authorities automated data processes are not clearly defined in their webpages nor they are seen in data tracer. RIHA and public service websites contain

some information but mainly focused to authorities itself and not for public use to identify personal data processing.

In order to provide more transparency there is a possibility to start using applicable data protection icons. GDPR allows such method and encourages also local supervisory authorities to find possible certification method for it. Such icons can be used in RIHA or in state service webpage.

KASUTATUD KIRJANDUS

Teadusraamatud:

1. Kuner, C. (2012). *European Data Protection Law: Corporate Compliance and Regulation* (2nd ed.). Oxford, UK: Oxford University Press.

2. Männiko, M. (2011). *Õigus privaatsusele ja andmekaitse.* Tallinn: Juura.

Teadusartiklid:

3. Agbozo E., Alhassan D., Spassov K. (2019). Personal Data and Privacy Barriers to E-Government Adoption, Implementation and Development in Sub-Saharan Africa. In: A. Chugunov, Y. Misnikov, E. Roshchin, D. (Eds.), *Electronic Governance and Open Society: Challenges in Eurasia* (1-10). Cham: Springer.

4. Alan, N., Hasan, M. (2015). . A Review of E-Government Services. *Advances in Social Sciences Research Journal*, 2 (8), 48-65.

5. Custers, B., Dechesne, F., Sears, A. M., Tani, T., van der Hof, S. (2018). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 34 (2), 234-243.

6. Dąbrowska, A., Janoś-Kresło, M., Lubowiecki-Vikuk, A. (2019). The Elderly as Participants of the Market of Selected E-services. *Studia Periegetica*, 2 (26), 13-23.

7. Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation. *Computer Law & Security Review*, 35 (6), 1-14.

8. Drogkaris P., Gritzalis A. (2015). A Privacy Preserving Framework for Big Data in e-Government Environments. In: S. Fischer-Hübner, C. Lambrinoudakis, J. López (Eds.), *Trust, Privacy and Security in Digital Business* (210-218). Cham: Springer.

9. Efroni, Z., Metzger, J., Mischau, L., Schirmbeck, M. (2019). Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. *European Data Protection Law Review*, 5 (3), 352-366.

10. Eliantonio, M., Galli, F., Schaper, M. (2016). A Balanced Data Protection in the EU: Conflicts and Possible Solutions. *Maastricht Journal of European and Comparative Law*, 23 (3), 391-403.

11. Engin, Z., Treleaven, P. (2018). Algoritmic Government: Automating Public Services and Supporting Civil Servants in using Data Science Technologies. *The Computer Journal*, 62 (3), 448–460.

12. Fabiano, N. (2019). Ethics and the Protection of Data. *The Journal on Systemics, Cybernetics and Informatics*, 17 (2), 58-64.

13. Ikkonen, M. (2005). Avalik huvi kui määratlemata õigusmõiste. *Juridica*, 3, 187-199.

14. Kamara, I. (2017). Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology*, 8 (1), 1-24.

15. Kvasnicova, T., Kremenova, I., Fabus, J. (2016) From an analysis of e-services definitions and classifications to the proposal of new e-service classification. *Procedia Economics and Finance*, 36, 192-196.

16. Kõrge H., Erlenheim R., Draheim D. (2019). Designing Proactive Business Event Services. In: P. Panagiotopoulos, N. Edelmann, O. Glassey, G. Misuraca, P. Parycek, T. Lampoltshammer, B. Re (Eds), *Electronic Participation* (73-84). Cham: Springer.

17. Larsson, A., Lilja, P. (2019). GDPR: What are the risks and benefits? In: A. Larsson, R. Teigland (Eds.), *The Digital Transformation of Labor: Automation, the Gig Economy and Welfare* (187-199). Cham: Springer.

18. Mahieu, R., van Hoboken, J., Asghari, H. (2019). Responsibility for Data protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10 (3), 85-105.

19. Merusk, K. (1994). Avalikõiguslik juriidiline isik kehtivas õiguskorras. *Juridica,*4, 85-87.

20. Peep, V. (2018). Andmekaitseõigusest andmekaitseasutuse pilguga. *Juridica,* 2, 116-124.

21. Portmeister, K., Nisu, N. (2018). Liidusisese kohalduva õiguse dilemma isikuandmete kaitse üldmääruses. *Juridica*, 2, 125-136.

22. Quintel, T. (2018). Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals. *European Data Protection Law Review*, 4 (4), 470 – 482.

23. Roig, A. (2017). Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR). *European Journal of Law and Technology*. 8 (3), 1-17.

24. Salumaa, K. (2018). Andmesubjekti õigused uue isikuandmete kaitse üldmääruse foonil. *Juridica*, 2, 83-93.

25. Sein, K., Mikiver, M., Paloma K. T. (2018). Pilguheit andmesubjekti õiguskaitsevanditele uues isikuandmete kaitse üldmääruses. *Juridica,* 2, 94-114.

26. Sirendi, R., Taveter, K. (2016). Bringing Service Design Thinking into the Public Sector to Create Proactive and User-Friendly Public Services. In: F.F.-H. Nah, C.-H. Tan (Eds.), *HCI in Business, Government, and Organizations: Information Systems* (221–230). Cham: Springer.

27. Thompson, N., Ravindran, R., Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government information quarterly*, 32 (3), 316-322.

28. Tsulukidze M., Nyman-Metcalf K., Tsap V., Pappel I., Draheim D. (2019) Aspects of Personal Data Protection from State and Citizen Perspectives – Case of Georgia. In: I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie (Eds.), *Digital Transformation for a Sustainable Society in the 21st Century* (476-488). Cham: Springer.

29. Turk, K., Pild, M. (2019). Kratiga või kratita – see on küsimus: Robotitest ja tehis-intellektist tsiviilõiguslikult. *Juridica,* 1, 43-55.

30. Veale, M., Edwards, L. (2017). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision- making and profiling. *Computer Law & Security Review: The International Journal of Technology Law and Practice*,34 (2), 398-404.

31. Wachter, S., Mittelstadt, B., Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 7 (2), 76-99.

Eesti õigusaktid:

32. Andmekogude seadus. RT I 1997, 28, 423, 01.05.2007.

33. Avaliku teabe seadus. RT I, 15.03.2019, 11.

34. Eesti infopoliitika põhialuste heakskiitmine. RT I 1998, 47, 700.

35. Eesti Vabariigi põhiseadus. RT I, 15.05.2015, 2.

36. Haldusmenetluse seadus. RT I, 13.03.2019, 55.

37. Infosüsteemide andmevahetuskiht. RT I, 06.08.2019, 17.

38. Isikuandmete kaitse seadus. RT I, 12.07.2014, 51.

39. Isikuandmete kaitse seadus, RT I, 04.01.2019, 11.

40. Riigi Infosüsteemi Ameti põhimäärus. RT I, 25.03.2020, 10.

41. Riigi infosüsteemi haldussüsteem. RT I, 29.03.2016, 6.

42. Teenuste korraldamise ja teabehalduse alused. RT I, 31.05.2017, 7.

43. Tervise infosüsteemi põhimäärus. RT I, 26.02.2020, 2.

44. Vabariigi Valitsuse seadus. RT I, 12.12.2018, 8

ELi õigusaktid ja rahvusvahelised õigusaktid

45. Council of Europe. Convention for the Protection of Human Rights and Fundamental Freedoms. ETS No. 5, Rome, 04/11/1950.

46. Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. ETS No.108, Strasbourg 28/01/1981 (Convention 108).

47. EL (2012), Euroopa Liidu põhiõiguste harta (ELT C 326, 26.10.2012).

48. Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid. (ELT C 202, 07.06.2016).

49. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EU, 24.10.1995, kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. (EÜT L 281, 23.11.1995).

50. Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46EÜ kehtetuks tunnistamise kohta (ELT L 119, 04.05.2016).

51. Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut. (ELT C 306, 17.12.2007).

Eesti kohtulahendid

52. RKHKo 12.07.2012, 3-3-1-3-12, p 19.

Muud allikad

53. Andmekaitse inspektsioon (2017). *Andmekaitse Inspektsiooni peadirektori seisukohad uue andmekaitseõiguse kontseptsiooni asjus*. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/reform/jum_oigusraamistiku_kontseptsiooni_markused_27.04.2017.pdf 20. veebruar 2020.

54. Andmekaitse inspektsioon (2016). *Andmekogude juhend.* Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf 20. veebruar 2020.

55. Andmekaitse inspektsioon (2019). *Isikuandmete töötleja üldjuhend*. Kättesaadav: https://www.aki.ee/sites/default/files/dokumendid/isikuandmete_tootleja_uldjuhend.pdf 20. veebruar 2020.

56. Angelopoulos, K., Diamantopoulou, V., Mouratidis, H., Pavlidis, M., Salnitri, M., Giorgini, P., Ruiz, J. F. (2017). A Holistic Approach for Privacy Protection in E-Government. *ARES '17: Proceedings of the 12th International Conference on Availability, Reliability and Security*. 7, 1-10.

57. Artikli 29 töörühm (2018). *Suunised automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta.* Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_automatiseeritud_tootlusel_pohinevate_uksikotsuste_tegemise_ja_profiilianaluusi_kohta_maaruse_2016679_kohaldamisel.pdf 20. veebruar 2020.

58. Artikli 29 töörühm (2018). *Suunised määruse 2016/679 kohase läbipaistvuse kohta*. Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_maaruse_2016679_kohase_labipaistvuse_kohta.pdf 20. veebruar 2020.

59. Artikli 29 töörühm (2018). *Suunised määruse (EL) 2016/679 kohase nõusoleku kohta.* Kättesaadav: https://www.aki.ee/sites/default/files/inspektsioon/rahvusvaheline/juhised/suunised_nousoleku_kohta_wp259_rev_0.1_et.pdf 20. veebruar 2020.

60. Dode, A. (2018, 21-22. September). *The challenges of implementing General Data Protection Law (GDPR)*. Article, 14th International Conference in "STANDARDIZATION, PROTYPES AND QUALITY: A MEANS OF BALKAN COUNTRIES' COLLABORATION", Tirana, Albania.

61. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne 2017. Kättesaadav: https://pohiseadus.ee/ 08. veebruar 2020.

62. Ernst & Young Baltic AS (2012). *Avaliku sektori äriprotsessid. Protsessianalüüsi käsiraamat.* Kättesaadav: http://dspace.ut.ee/bitstream/handle/10062/45124/protsessianaluusi_kasiraamat.pdf?sequence=1&isAllowed=y 23. märts 2020.

63. Euroopa Komisjon (2012). *Kirjuta selgelt*. Kättesaadav: https://op.europa.eu/en/publication-detail/-/publication/bb87884e-4cb6-4985-b796-70784ee181ce/language-et 11. aprill 2020.

64. Euroopa Komisjon (2016). *Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele ELi e-valitsuse tegevuskava 2016-2020, Valitsussektori digitaalse arengu kiirendamine.* Kättesaadav: https://eur-lex.europa.eu/legal-content/et/TXT/?uri=CELEX:52016DC0179 26. aprill 2020.

65. Euroopa Komisjon (2015). *Komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa majandus- ja sotsiaalkomiteele ning regioonide komiteele Euroopa digitaalse ühtse turu strateegia.* Kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52015DC0192 26. aprill 2020.

66. Majandus- ja Kommunikatsiooniministeerium (2013). *Avalike teenuste korraldamise roheline raamat*. Kättesaadav: https://mkm.ee/sites/default/files/avalike_teenuste_korraldamise_roheline_raamat.pdf 23. märts 2020.

67. Majandus- ja Kommunikatsiooniministeerium (2018). E*esti infoühiskonna arengukava 2020.* Kättesaadav: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava_2020.pdf 23. märts 2020.

68. Majandus- ja Kommunikatsiooniministeerium (2019). *Juhised määruse "Teenuste korraldamise ja teabehalduse alused" rakendajatele*. Kättesaadav: https://mkm.ee/sites/default/files/content-editors/lyhijuhised_tkta_rakendajatele_vers_1_1.pdf 23. märts 2020.

69. Riigi infosüsteemised amet (2020). Riigi Infosüsteemi Ameti aastaraamat 2020. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/RIA/ria_aastaraamat_2020_48lk_est_veeb_0.pdf 25. aprill 2020.

70. Riigikantselei (2014). *Avalike teenuste ühtse portfellijuhtimise kokkuvõte.* Kättesaadav: https://mkm.ee/sites/default/files/avalike_teenuste_uhtne_portfellijuhtimine_-_kokkuvote.pdf 23. märts 2020.

71. Statistikamet. N03: Sidus ühiskond (2004-2017), interneti kasutamise määr % [e-andmebaas]. Kättesaadav: http://andmebaas.stat.ee/ 07. mai 2020.

72. Siseministeerium (2020). *Siseministri määruste muutmine ja kehtetuks tunnistamine. EN_PäästeS rakendusaktide muutmine seoses PäästeS muutmisega.* Kättesaadav: https://eelnoud.valitsus.ee/main/mount/docList/40937f02-d3c2-40a3-bfc3-356fe2688ec6 28. aprill 2020.

73. Ustaran, E., Lovells, H. (Eds.) (2018). *European Data Protection: Law and Practise.* Portsmouth, USA: International Association of Privacy Professionals.

74. Vabariigi Valitsus (2015). *Avalike teenuste omanike määratlemise analüüs ja ettepanekud.* Kättesaadav: https://www.mkm.ee/sites/default/files/avalike_teenuste_omanike_maaratlemise_analyys_ja_ettepanekud.pdf 23. märts 2020.

75. Vabariigi Valitsus (2012). *Avaliku teabe seaduse muutmise seadus 263 SE*. Kättesaadav https://www.riigikogu.ee/tegevus/eelnoud/eelnou/bd9d9bac-52dc-4549-a23c-ee4816e0a2af 25. aprill 2020.

76. Vabariigi Valitsus (2019). *Riikliku statistika seaduse ja avaliku teabe seaduse muutmise seadus 794 SE*. Kättesaadav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6932ebe8-2dfa-4613-b627-f9c967a3d12f/Riikliku%20statistika%20seaduse%20ja%20avaliku%20teabe%20seaduse%20muutmise%20seadus 25. aprill 2020.

Lisa 1. Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina Priit Davel

1. annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Proaktiivsete teenuste andmetöötluse kodanikule nähtavamaks muutmine“ mille juhendaja on Kristi Joamets,

1.1 reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh TalTechi raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2 üldsusele kättesaadavaks tegemiseks TalTechi veebikeskkonna kaudu, sealhulgas TalTechi raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

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

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

---

[1] *Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil.*