TALLINNA TEHNIKAÜLIKOOL
Sotsiaalteaduskond
Õiguse instituut

Kati Mets

TARKVARA AGENDI KASUTAMISE VÕIMALUSTEST ANDMESUBJEKTI OSALUSE PÕHIMÕTTE TAGAMISEL

Magistritöö

Juhendaja: Addi Rull, MA

Tallinn 2016

Deklareerin, et käesolev magistritöö,
mis on minu iseseisva töö tulemus,
on esitatud Tallinna Tehnikaülikooli
magistrikraadi taotlemiseks ja selle alusel
ei ole varem taotletud akadeemilist kraadi.

Kati Mets
„…“…….2016.a.

Töö vastab kehtivatele nõuetele.

Addi Rull, MA
„...“…….2016.a.

Kaitsmisele lubatud „ …“…….2016.a.

Õiguse instituudi magistritööde kaitsmiskomisjoni esimees

Sisukord

Lühendid

AKI – Andmekaitse Inspektsioon.

Andmekaitse määrus – Euroopa Parlamendi ja Nõukogu määrus (ettepanek) üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus).

AvTS – avaliku teabe seadus.

Direktiiv – Euroopa Parlamendi ja Nõukogu 24. oktoober 1995 aasta direktiiv 95/46/EÜ.

DIAT register- isikuandmete töötlejate ja isikuandmete töötlemise eest vastutavate isikute register.

EIK – Euroopa Inimõiguste Kohus.

ELK – Euroopa Kohus.

EL – Euroopa Liit.

EIÕKonv – Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsioon.

ETS 108 – isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon.

Harta – Euroopa Liidu Põhiõiguste Harta.

IKS – isikuandmete kaitse seadus.

ISKE – infosüsteemide kolmeastmeline etalonturbe süsteem.

ISKE määrus- Vabariigi Valitsuse 20.12.2007.a määrus „Infosüsteemide turvameetmete süsteem“.

KOV– kohalik omavalitsus.

Määrus – Vabariigi Valitsuse määruse eelnõu „Teenuste korraldamine ja teabehalduse alused“

PS – Eesti Vabariigi Põhiseadus.

Rakendus – isikuandmete töötlemise kontrolli võimaldav rakendus „Suur vend“.

RIHA – Riigi Infosüsteemi Haldussüsteem.

X-tee – Infosüsteemide andmevahetuskiht.

Sissejuhatus

Euroopa Liidu (edaspidi EL) toimimise lepingu artikli 16 lõikest 1 tulenevalt on igal ühel õigus isikuandmete kaitsele. Euroopa Liidu põhiõiguste harta (edaspidi Harta) artiklis 8[1] on isikuandmete kaitse sätestatud põhiõigusena.

Avalike teenuste pakkumine toimub üha enam IT-teenuste vahendusel. Riigi infosüsteemi haldussüsteemi[2] (edaspidi RIHA) andmetel on Eestis ligikaudu 600 andmekogu. Valdav osa andmekogusid sisaldavad isikuandmeid ning delikaatseid isikuandmeid.

Põhiandmete kontseptsioonist tulenevalt andmeid ei koguta nö topelt. Kui mõnes andmekogus juba kogutakse vajaminevaid andmeid, ei tohi neid andmeid uuesti koguma hakata, vaid tuleb infosüsteemide andmevahetuskihi (edaspidi X-tee) vahendusel kasutada juba teises andmekogus olemasolevaid andmeid. Seega andmekogudel on nii andmeandjad kui andmesaajad ning X-teed kasutatakse laialdaselt.

Avaliku teabe seaduse[3] (edaspidi AvTS-i) andmekogude regulatsioon on aga andmekogudele esitatavate nõuete osas üldsõnaline, näiteks ei kohusta andmekogude regulatsioon määratlema andmesaajaid. Üldistatult võib öelda, et andmesaajate osas sätestatakse kehtivates andmekogusid puudutavates õigusaktides napisõnaliselt, et andmekogudes sisalduvatele andmetele võimaldatakse juurdepääs seadusest tulenevate ülesannete täitmiseks. Ühelt poolt nimetatud asjaolu võimaldab laia tõlgendamisruumi vastutava töötleja jaoks, hindamaks, kellele andmeid anda ja teiselt poolt ei ole andmesubjektil võimalik saada ilma haldusorganit liigselt koormamata infot kellele võib olla tema andmeid edastatud.

Andmesubjekti osaluse põhimõtte, mis on üks õiguspärase andmetöötluse aluspõhimõte, realiseerimise eelduseks on, et isik teab asjaolu, et tema andmeid töödeldakse, millises ulatuses seda tehakse ja milline on andmete töötlemise loogika. Eelnevat informatsiooni omamata ei ole andmesubjektil võimalik hinnata kas andmete töötlemine on õiguspärane või mitte.

Andmesubjekti osaluse põhimõtte realiseerimise võimaldamine on oluline, kuna andmekogude väärkäitlemise juhtumeid on arvukalt, need on leidnud käsitlemist meedias, eriala kirjanduses ja Andmekaitse Inspektsiooni (edaspidi AKI) ülevaadetes. Nii on probleeme lisaks eelnevalt

[1] Euroopa Liidu Põhiõiguste Harta, C 326/391, 26.10.2012, art. 8.
[2] Riigi infosüsteemi haldussüsteemi kodulehekülg https://riha.eesti.ee/riha/main, (17.01.2016).
[3] AvTS, RT I 06.01.2016, 7, 10.

märgitud andmesaajate määratlemisele volitusnormide sõnastamise ja andmete eesmärgipärase töötlemisega, samuti andmetele säilitustähtaja kehtestamise ja muude õiguspärase töötlemise nõuete täitmisega. Eelnevad nõuded on andmekogusid reguleerivates õigusaktides määratletud üldsõnaliselt või puuduvad sootuks. Kui muudel juhtudel isikul on võimalik oma nõusolekust isikuandmete töötlemisel taganeda, siis seaduse alusel[4] töötlemisel on isik, kelle andmeid töödeldakse, täielikult isikuandmete töötleja meelevallas. Eelnevale lisandub laia kõlapinda leidnud avaandmete kontseptsiooni realiseerumine, mis tähendab, et üha enam hakatakse avaliku sektori poolt kogutavaid andmeid kasutama viisil, mis loob isikuandmete töötlemisel täiendavaid ohte. Seetõttu on äärmiselt oluline, et seaduse alusel töötlemisel oleks õiguspärane töötlemine tagatud.

Käesoleval ajal pakub avalik sektor sadu e-teenuseid ja vaid üksikutes andmekogudes, mis on projektiga „Suur Vend“ liitunud[5] on olemas funktsionaalsus, mis võimaldab andmesubjektil ennast autentides:

- Saada enda kohta käivaid andmeid.
- Saada informatsiooni millisele asutusele või institutsioonile on andmesubjekti andmeid edastatud või neile juurdepääs võimaldatud (v.a seadusest tulenevad välistavad juhtumid).

Infotehnoloogia abil pakutavate teenuste lisandumisel ei ole eluliselt usutav, et isikuandmete kaitse seadusest[6] (edaspidi IKS) tulenevat nõuet anda isikule teavet tema andmete töötlemise kohta viie tööpäeva jooksul on võimalik täita ilma olulisel määral andmekogudele esitatavaid nõudeid täiendamata. Samuti ei ole usutav, et andmesubjektil oleks oma õiguste kaitsmise eesmärgil võimalik teha lakkamatult päringuid sadadele volitatud töötlejatele informatsiooni saamiseks.

Suur Vend võimaldab saada informatsiooni üksnes selle kohta kellele on andmeid edastatud. Kui andmesubjekt soovib informatsiooni näiteks andmete edastamise eesmärgi või muude õiguspärase töötlemise nõuete kohta, peab ta pöörduma eraldi vastutava töötleja poole informatsiooni saamiseks, Suur Vend selle kohta informatsiooni ei anna.

[4] Käesolevas töös käsitletakse andmekogusid AvTs mõistes, mis tähendab, et isikuandmeid võib töödelda isiku nõusolekuta. Nõusolekuta töötlemise aluseks võib olla seadus, välisleping või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduv õigusakt.
[5] Näiteks: e-Tervis, karistusregister, kus iga andmesubjekt ennast autentides saab infot endaga seotud andmete kohta ja samuti selle kohta, kellele tema andmeid edastatud on (kuid selle kohta, millistel eesmärkidel andmeid edastatud on, infot ei saa).
[6] IKS, RT I 06.01.2016, 10, 51.

Samas üha enam erinevates eluvaldkondades leiavad kasutust Agendid. Agentide kasutamise eesmärk on abistada kasutajat erinevates valdkondades peamiselt tehnilist laadi töö, näiteks andmete analüüsimine, vähendamise arvelt.[7] Agentide kasutusvõimalust on uuritud ka andmekaitse valdkonnas [8].

Seega andmesubjekti osaluse põhimõtte realiseerimise tagamiseks e-lahenduste abil on mitmeid erinevaid võimalusi.

Eeltoodust tulenevalt töö autor püstitab hüpoteesi, et kehtiv AvTs regulatsioon, mis sätestab nõuded andmekogudele, ei taga andmesubjektile võimalust realiseerida oma õigusi, mis tulenevad andmesubjekti osaluse põhimõttest.

Eelneva hüpoteesi uurimisküsimused on järgnevad:

1. Millised on andmesubjekti osaluse põhimõtte sisunõuded?

2. Kas AvTS andmekogude regulatsioon tagab andmesubjekti osaluse põhimõtte realiseerimise?

3. Millised peavad olema nõuded e-lahendustele andmesubjekti osaluse põhimõttest lähtuvalt?

4. Kas ja millisel määral rakendus „Suur Vend“ tagab andmesubjekti osaluse põhimõtte realiseerimise võimaluse andmesubjekti jaoks.

5. Teise, alternatiivse ja teoreetilise lahendusena uuritakse kas ja millisel määral Agent aitaks andmesubjektil realiseerida andmesubjekti osaluse põhimõtet.

Esimese uurimisküsimuse lahendamise käigus sisustatakse andmesubjekti osaluse põhimõte, selleks käsitletakse andmesubjekti osaluse põhimõtte kujunemist nii läbi EL privaatsusõigust käsitlevate olulisemate õigusaktide, Euroopa Inimõiguste Kohtu (edaspidi EIK) ja Euroopa Kohtu (edaspidi ELK) kohtupraktika, kui ka Eesti isikuandmete kaitse ja andmekogude regulatsiooni. Lisaks kasutatakse andmesubjekti osaluse põhimõtte sisustamisel töös AKI ülevaateid ja erialakirjandust.

Teise uurimisküsimuse lahendamise käigus hinnatakse andmekogude regulatsiooni vastavust andmesubjekti osaluse põhimõttele, ning tehakse ettepanekud andmekogude regulatsiooni muutmiseks ja täiendamiseks.

[7] Serenko, A.; Detlor, Ę. B. Intelligent agents as innovations. Springer, 2004, lk. 364-381.
[8] Rull *et al.* Towards Software-Agent Enhanced Privacy Protection. Springer, lk. 73-94.

Kolmanda uurimisküsimuse lahendamise käigus käsitletakse nõudeid e-lahendustele andmesubjekti osaluse põhimõtte realiseerimisel. Nõuete sisustamisel võetakse aluseks Vabariigi Valitsuse määruse eelnõu „Teenuste korraldamine ja teabehalduse alused“ (Lisa 1) (edaspidi Määrus), Infoühiskonna arengukava 2020[9], Valitsuserakondade koalitsioonilepe[10], Avalike teenuste korraldamise roheline raamat[11] ja E-riigi harta[12].

Neljanda ja viienda küsimuse uurimiseks käsitletakse töös tehnoloogilisi võimalusi andmesubjekti osaluse põhimõtte realiseerimisel. Selleks võrreldakse rakendust Suur Vend ja Agenti eelnevalt sisustatud andmesubjekti osaluse põhimõttega ja nõuetega e-lahendustele. Agenditeooria uurimiseks kasutatakse teadusartikleid.

Töö eesmärgiks on seega pakkuda välja lahendused avaliku teabe seaduse ja vajadusel muude õigusaktide muutmiseks mis puudutab andmekogude regulatsiooni, et tagada andmesubjektile andmesubjekti osaluse põhimõtte realiseerimise võimalus ning uurida tehnoloogia kasutamise võimalusi andmesubjekti osaluse põhimõtte realiseerimisel.

Töö on aktuaalne, kuna mitmete autorite, nt. Solove hinnangul tehnoloogia kasutamine avaliku sektori andmekogudes kasvab kiiresti, sealjuures on võimalik kogutavaid andmeid lihtsasti edastada, otsida ja kopeerida, mis ohustab andmesubjektide privaatsust[13].

Töö metoodika on kvalitatiivne, analüüsitakse asjakohaseid õigusakte, eriala kirjandust, AKI aasta aruandeid ja muid andmesubjekti osaluse põhimõtet käsitlevaid dokumente.

Töö autor tänab juhendajat põhjaliku tagasiside ja nõuannete eest, mis oli töö koostamisel suureks abiks.

[9] Infoühiskonna arengukava 2020 https://www.mkm.ee/et/arengukavad (20.01.2016).
[10] Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta, p. 4.20, http://www.sotsdem.ee/wp-content/uploads/2015/04/RE-SDE-ja-IRLi-valitsusliidu-lepe.pdf (20.01.2016).
[11] Avalike teenuste roheline raamat, lk 17-18, https://www.mkm.ee/sites/default/files/avalike_teenuste_korraldamise_roheline_raamat.pdf, (20.01.2016).
[12] E-riigi harta, http://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Muudpublikatsioonid/tabid/113/language/et-EE/Default.aspx (20.01.2016).
[13] Solove, D. J. Access and Aggregation: Public Records, Privacy and the Constitutions. Minnesota Law Review 2002, lk. 1138-1176.

1. Andmesubjekti osaluse põhimõte ja andmekogude regulatsioon

1.1. Andmesubjekti osaluse põhimõte Euroopa Liidu õiguses

Privaatsust on kaitstud juba sajandeid, mõningaid näiteid privaatsuse kaitsest võib leida isegi Vana-Kreeka õigusest[14]. Tänapäevane andmekaitse ja privaatsusõiguse kiire areng on seotud infotehnoloogia laialdasema kasutuselevõtuga 1960 ja 1970 aastatel[15].

Andmesubjekti osaluse põhimõtte ja isikuandmete kaitse põhimõtete sisu kujunemisele on mõju avaldanud arvukad dokumendid. Üheks olulisemaks neist peetakse Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsiooni[16] (edaspidi EIÕKonv), mis võeti vastu 4. novembril 1950 aastal Roomas ning millega on ühinenud samuti Eesti. Ühinemisega on Eesti võtnud kohustuse siseriiklik õigus EIÕKonv sisalduvate põhimõtetega vastavusse viia.

EIÕKonv privaatsuse kaitse lisamist seostatakse peamiselt Teise maailmasõja ajal Saksamaal toimunud isikuandmete väärkasutusega. Konventsiooni nimest võib ekslikult jääda mulje, et selle osalised on üksnes Euroopa riigid – tegelikkuses on selle mõju laiem. Tänaseks võib öelda, et sellel on olnud märkimisväärne mõju kõikide EL liikmesriikide privaatsusõiguse normide tõlgendamisele.[17] Andmekaitse kui õigusharu ongi välja arenenud EIÕKonv toel[18]. Selle artikkel 8 on privaatsusõiguse kõige olulisem allikas[19]. Artikli 8 sõnastusest ei tulene selgesõnalist õigust isikuandmete kaitsele, selle kohaselt „Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust“[20] ning et võimu sekkumine selle õiguse realiseerimisse peab alati olema kooskõlas seadusega ning see peab olema demokraatlikus ühiskonnas riigi julgeoleku või muudes ühiskondlikku hüve teenivates asjaoludes vajalik[21].

EIÕKonv artiklit 8 on nimetatud ka „vihmavarju sätteks“[22], see tähendab, et kui algselt käsitleti sätet peamiselt seonduvalt kodu kaitsega, on selle kaitseala ajapikku laienenud, hõlmates tänaseks nii isiku vaba eneseteostuse kui ka turvalisuse küsimused[23]. Privaatsuse kaitse on otseselt seotud

[14] Kemp, R.; Moore, A. D. Privacy. Library Hi Tech, 2007, Vol.25(1), lk 59-61.
[15] Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. Juridica VII/2002, lk 435.
[16] EIÕKonv, RT II 1996, 11, 34.
[17] Tikk, E.; Nõmper, A. Informatsioon ja õigus. Tallinn, Juura 2007, lk 29.
[18] Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn, Juura 2011, lk 57.
[19] Ovey, C.; White R. C. A. European Convention on Human Rights. 3rd ed. Oxford University Press 2002, lk 1.
[20] EIÕKonv, *supra* note 16, art 8.
[21] Ibid.
[22] T. Ilus. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. Juridica VIII/2005, lk 521.
[23] Ibid, lk 521.

inimese vaba eneseteostuse, valikute ja otsuste tegemisega[24], ning artikli 8 privaatsuse mõiste sisu täieneb vastavalt ühiskonna arengule[25].

Kontrollimaks konventsiooniga liitunud riikide osas konventsiooni täitmist, kutsuti 1959 aastal ellu EIK. Susi hinnangul Riigikohtu praktika toetab EIÕKonv otsekohaldamist ning EIK lahendite siduvust[26]. Seega avaldab EIÕKonv otsest mõju Eesti õigusruumile.

Teiseks oluliseks dokumendiks isikuandmete kaitse valdkonnas võib pidada isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni[27] (edaspidi ETS 108).

ETS 108 hakati välja töötama 1970 aastatel ning see valmis 1981 aastaks [28]. Selle eesmärgiks oli vähendada ohtusid üksikisiku privaatsusele mis tulenesid info- ja kommunikatsioonitehnoloogia järjest laialdasemast kasutuselevõtust. Konventsiooni alusel ei teki subjektiivseid õigusi, küll aga tekib liitunud riikidel kohustus konventsioonis sisalduvad põhimõtted oma õigusesse üle võtta.[29]

Privaatsusõiguse seos automatiseeritud töötlemisega on väljendatud konventsiooni preambulas märkimisväärselt täpsemalt kui EIÕKonv-is. Selles viidatakse otsesõnu isikuandmete automatiseeritud töötlemisele ning asjaolule, et automatiseeritud töötlemise sagenemine vajab tõhusamaid meetmeid isikute õiguste ja põhivabaduste kaitseks[30].

ETS 108 artiklis 2 sätestatakse ka andmetöötluse kesksed mõisted nagu isikuandmed, andmesubjekt, artiklis 8 käsitletakse lisaks andmesubjekti osaluse põhimõtet, artiklis 6 andmekvaliteedi põhimõtted[31].

ETS 108 artikli 2 punkti a kohaselt isikuandmed on mis tahes informatsioon tuvastatud või tuvastatava isiku ehk andmesubjekti kohta[32]. Võib öelda, et andmesubjekti osaluse põhimõte, mille selgesõnaline käsitlus eelnevalt käsitletud dokumendis puudus, on jäänud ka hilisemates dokumentides suuresti samaks. ETS 108 artikli 8 kohaselt peab isikule võimaldama automatiseeritud töötlemisel:

[24] Solove, D. J. Conceptualizing Privacy California Law Review Vol. 90:1087, 2002, lk. 1143.
[25] Ovey *et al. supra* note 19, lk 217; Bygrave, L., A. Data Protection Law: Approaching Its Rationale, Logic and Limits. Kluwer Law International 2002, lk 34.
[26] Susi, M. Euroopa Inimõiguste Kohtu 2010. aasta kohtulahendite ülevaade, Tartumaa, OÜ Greif, 2011, lk 5.
[27] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon, RT II 2001, 1, 3.
[28] Tikk, Nõmper, *supra* note 17, lk 31.
[29] Bygrave, L. A. Data Privacy Law An International Perspective, Oxford University Press, 2014, lk 52.
[30] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon, *supra* note 27.
[31] Ibid, art 2 ja 3.
[32] Ibid, art 2 p.a.

- teha kindlaks isikuandmete kogu olemasolu;
- töötlemise eesmärgid;
- töötleja andmed;
- saada ilma liigse viivituseta ja kuluta teavet kas isikuandmeid säilitatakse andmekogus ja saada neid andmeid mõistetavas vormis;
- nõuda oma andmete parandamist, töötlemise lõpetamist, mille töötlemine on vastuolus siseriikliku õigusega;
- kasutada õiguskaitse vahendeid kui parandamise ja töötlemise lõpetamise taotlust ei rahuldata. [33]

Kuid ETS 108 suurim puudus oli, et see kaitses isikut vaid tema isikuandmete automatiseeritud töötlemisel[34].

Järgmine andmesubjekti õigusi reguleeriv ja Eesti õiguskorra arengut privaatsusõiguse aspektist mõjutanud dokument on Euroopa Parlamendi ja Nõukogu 24. oktoober 1995 aasta Direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[35] (edaspidi Direktiiv). Võrreldes eelnevalt käsitletud dokumentidega on Direktiiv detailisem[36].

Direktiivi tähtsus andmesubjekti jaoks seisneb eelkõige selles, et võrrelduna andmekaitse konventsiooniga laiendati sellega tunduvalt andmete töötlemise mõistet. Kui konventsioonis keskenduti peamiselt andmete automatiseeritud töötlemisele, siis Direktiivi kohaselt ei oma tähtsust, kas andmeid töödeldakse automatiseeritult või mitte: igal juhul on tegemist isikuandmete töötlemisega. Samuti pannakse liikmesriikidele kohustus sätestada isikuandmete töötlemine siseriiklikes seadustes.[37] Direktiivi artiklis 7 on esmakordselt sätestatud nõuded mis peavad olema enne isikuandmete töötlemisele asumist tagatud[38]. Andmesubjektile nähti samuti ette senisest

[33] Ibid, art 8.
[34] Ibid.
[35] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, 24.10.1995, ELT L 281/31.
[36] Bygrave (2014), *supra* note 29, lk 53-54.
[37] Männiko, *supra* note 18, lk 72.
[38] Gundermann, L. Euroopa Liidu andmekaitseõigus – andmekaitse ja andmetele avaliku juurdepääsu suhtest ning andmekaitse järelevalve olukorrast Juridica VIII/2005, lk. 512.

laialdasem kontroll oma andmete töötlemisel[39]. Lisaks kohustati liikmesriike ellu kutsuma järelevalveasutusi[40].

Direktiivis defineeritakse isikuandmeid sisuliselt samas sõnastuses eelnevalt käsitletud dokumendiga: isikuandmeteks võib pidada igasugust teavet füüsilise isiku ehk andmesubjekti kohta. Sealjuures ei ole oluline, kas tegemist on tuvastatud või tuvastatava isikuga. Oluline on märkida, et Direktiivi preambula punkt 24 kohaselt ei käsitleta andmesubjektina juriidilist isikut.[41]

Teine oluline ja käesolevas töös läbiv mõiste on töötlemine. Direktiiv käsitleb töötlemist kui iga isikuandmetega tehtavat toimingut või toimingute kogumit, „/…/ olenemata sellest, kas see on automatiseeritud või mitte, näiteks kogumine, salvestamine, korrastamine, säilitamine, kohandamine või muutmine, väljavõtete tegemine, päringu teostamine, kasutamine, üleandmine, levitamine või muul moel avaldamine, ühitamine või ühendamine, sulgemine, kustutamine või hävitamine;[42].

Andmesubjekti osaluse põhimõte väljendub selgesti Direktiivi preambula punktides 38 – 43 ja nagu eelnevalt öeldud, kattub see suuresti ETS 108 artiklis 8 käsitletud andmesubjekti osaluse põhimõtte käsitlusega: õigluse huvides tuleb andmesubjekti tema andmete kogumisest teavitada, andmesubjektil on õigus teada andmetöötluse asjaoludest sh kellele on tema andmeid edastatud. Oluline on märkida, et preambula punktis 40 tuuakse erisusena välja töötlemine seaduse alusel: seaduse alusel töötlemisel võib andmesubjekti teavitamiskohustust mitte täita kui andmete töötlemine on õigusaktides otsesõnu ette nähtud. [43] Preambula punkt 41 käsitleb andmesubjekti juurdepääsõigust, et andmesubjektil oleks võimalik kontrollida oma andmete õigsust ja õiguspärast töötlemist. Preambula punktis 43 sätestatakse juurdepääsuõiguste piirangutena muuhulgas riigi julgeolek, avalik kord jne. Õigust tutvuda oma andmete töötlemisega käsitletakse täpsemalt Direktiivi artiklis 12. Andmesubjektil on õigus saada liigse viivituse ja kulutusteta infot töödeldavate andmete kohta, kellele neid andmeid on avaldatud, millised on töötlemise eesmärgid, kuidas ja millistel tingimustel andmeid töödeldakse. Lisaks peab andmesubjektil olema õigus oma andmed töötlemiseks sulgeda, kustutada, parandada. Selline õigus on andmesubjektil juhul, kui Direktiivi nõudeid ei täideta. Märkimisväärne on, et Direktiivi artikli 12 punkti b alusel ei tehta

[39] Bainbridge, D. I. Processing Personal Data and the Data Protection Directive. Information & Communications Technology Law, vol. 6, No. 1, 1997, lk. 17.
[40] Eestis on järelevalveorganiks Andmekaitse Inspektsioon.
[41] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, *supra* note 35, preambula p 24 ja art.2 p. a.
[42] Ibid, art.2 p.b.
[43] Ibid, preambula punktid 38-43.

töötlemise lõpetamise õigusel vahet, kas andmeid töötleb avalik sektor seaduse alusel või toimub töötlemine andmesubjekti nõusoleku alusel.[44]

Lisaks sätestatakse õiguspärase töötlemise aluspõhimõtetena seadusliku töötlemise, eesmärgikohasuse, andmete kvaliteedi, minimaalsuse, kasutuse piiramise ja turvalisuse põhimõtted. Nimetatud põhimõtted on otseselt seotud õigusega saada informatsiooni oma andmete töötlemise asjaolude kohta, mis on osa andmesubjekti osaluse põhimõttest. Kui isikuandmete töötlemine ei ole kooskõlas nimetatud põhimõtetega, ei ole tegemist õiguspärase töötlemisega. Seega andmesubjekti osaluse põhimõtte täielikuks realiseerimiseks peab andmesubjektil olema võimalik kontrollida eeltoodud põhimõtete järgimist endaga seotud andmete töötlemisel. Nende põhimõtete kontekstis on tal võimalik hinnata andmetöötluse õiguspärasust ning esitada vastuväiteid oma andmete töötlemise kohta. Käesolevas töös käsitletakse eeltoodud põhimõtteid kui andmesubjekti osaluse põhimõtte olulisi osi.

Seaduslikkuse põhimõtet väljendab Direktiivi preambula punkt 28 ning artikkel 6 lõike 1 punkt a, mille kohaselt andmete töötlemine peab olema andmesubjekti jaoks õiglane ja seaduslik. Andmete töötlemise alusel peab olema selge seos kogutavate andmetega.[45]

Eesmärgi kohasuse, kasutuse piiramise ja andmete kvaliteedi põhimõtet väljendab juba eelnevalt käsitletud preambula punkt 28 ja artikkel 6, mille kohaselt töötlemine ei pea olema üksnes seaduslik vaid ka vajalik avalikes huvides või avalike ülesannete täitmiseks vajalik, andmeid kogutakse vaid selleks ettenähtud eesmärkidel, andmed peavad olema adekvaatsed[46].

Minimaalsuse põhimõtet käsitletakse Direktiivi artikli 6 lõike 1 punktis c, mille kohaselt andmed peavad olema piisavad ja asjakohased ja ei ületa selle otstarbe piire, mille tarvis neid kogutakse[47].

Turvalisuse põhimõtet käsitlevad Direktiivi preambula punkt 46 ja artikli 17 lõige 1. Andmete töötleja peab rakendama infotehnoloogilisi ja organisatoorseid meetmeid isikuandmete kaotsi mineku ja hävimise vältimiseks, ebaseadusliku avalikustamise ning ebaseadusliku juurdepääsu võimaldamise eest.[48]

[44] Ibid, preambula p 38-40 ja art. 10-14.
[45] Ibid, preambula p 28 ja art. 6 lg. 1 p. a.
[46] Ibid, preambula p 28 ja art. 6 lg. 1 p. e.
[47] Ibid, art. 6 lg. 1 p. c.
[48] Ibid, preambula p. 46 ja art. 17 lg. 1.

Isikuandmete kaitset kui põhiõigust EL õiguses märgiti esmakordselt Harta artiklis 8[49], hartat on käsitletud kui märkimisväärset arengut privaatsusõiguse valdkonnas[50]. Harta artiklis 8 sätestatakse, et „Igaühel on õigus oma isikuandmete kaitsele“[51], sama artikli punktis 2 sätestatakse, et õiguspärase töötlemise eelduseks on seadusliku aluse olemasolu ning, et andmesubjektil peab olema võimalus oma andmetele juurdepääsuks ja võimalus neid andmeid parandada[52]. Harta loomise aluseks oli Euroopa Ülemkogu otsus konsolideerida EL põhiõigused[53]. Seega harta koostamisel on arvesse võetud kõiki käesolevas töös eelpool käsitletud konventsioone ja direktiive[54].

Käesoleval ajal on käimas EL andmekaitse reform, mille raames valmistatakse muuhulgas ette isikuandmete kaitse üldmäärust (edaspidi Andmekaitse määrus)[55].

Andmekaitse määruse andja on selgitanud, et tehnoloogia areng võimaldab isikuandmeid kasutada enneolematult suures ulatuses, mis on põhjustanud uusi ohtusid isikuandmete kaitsel. Üksikisikul peab olema kontroll oma andmete töötlemise üle, mis suurendab andmesubjektide usaldust tagades digitaalse majanduse arengu. Eelneva tõttu on vajalik Direktiiv üle vaadata ja täiendada.[56]

Käeoleva töö seisukohtalt on kindlasti oluline preambula punkt 51, milles sätestatakse, et andmesubjektil peab olema võimalik oma andmete töötlemisest teada ja kontrollida töötlemise seaduslikkust. Andmesubjektil on õigus saada teavet andmete töötlemise eesmärkide, andmete saajate, töödeldavate andmete loogika ja ajavahemiku, mil andmeid töödeldakse, kohta. Väärib märkimist, et määruse eelnõus rõhutatakse, et eelnev peab olema andmesubjekti jaoks lihtsasti kasutatav. [57]

Andmekaitse määruse preambula punkti 53 kohaselt on õigus isikuandmete töötlemise lõpetamist nõuda muuhulgas juhul, kui isikuandmete töötlemine ei vasta määruse põhimõtetele. Sarnaselt Direktiivis sätestatule ei tehta töötlemise lõpetamise nõude õigusel vahet, kas töötlemine toimub seaduse alusel või mitte. Preambula punkti 61 kohaselt peab vastutav töötleja tagama sise-eeskirjade kehtestamise isikuandmete töötlemisel infotehnoloogilisi vahendeid kasutades.

[49] Euroopa Liidu Põhiõiguste Harta, *supra* note 1, art. 8.
[50] Bybrave (2014), *supra* note 29, lk 58-59.
[51] Euroopa Liidu Põhiõiguste Harta, *supra* note 1, art 8.
[52] Ibid.
[53] Laurand, A. Euroopa Liidu liitumine Euroopa põhivabaduse kaitse konventsiooniga. Juridica IX 2013, lk 677.
[54] Bygrave (2014), *supra* note 29, lk 58-59.
[55] Euroopa Parlamendi ja Nõukogu määrus (ettepanek) üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (isikuandmete kaitse üldmäärus), COM(2012) 11 final, 2012/0011 (COD).
[56] Ibid, lk 1 ja 18.
[57] Ibid, preambula p 51.

Tehnilisi meetmeid isikuandmete õiguspäraseks töötlemiseks tuleb rakendada nii andmekogu kavandamise kui töötlemise käigus. [58] Ka mitmete autorite hinnangul isikuandmete kaitse ei saa tänapäevases ühiskonnas olla üksnes õigusnormidele rajatud, see peab olema toetatud tehnoloogiliste vahendite poolt, vaid tehnoloogiliste vahendite rakendamine saab olla eduka isikuandmete kaitse tagamise aluseks [59].

Väärib märkimist, et preambula punkti 67 kohaselt tuleb andmesubjektile tagada isikuandmete rikkumisega seotud juhtumitest teada andmine 24 tunni jooksul, rikkumisest teada saamisest arvates. Andmekaitse määruse andja põhjendab seda asjaoluga, et rikkumisega võib kaasneda isikule oluline sotsiaalne ja majanduslik kahju. Rikkumise hindamist käsitletakse punktis 68, mille kohaselt tuleb rikkumise puhul hinnata kas töötlemine on kooskõlas turvalisuse põhimõttega.[60]

Lisaks eeltoodule tähtsustatakse Andmekaitse määruses andmete säilitamise tähtaegu, mis on seotud õigusega saada unustatud ning rõhutatakse andmekogude koosvõimelisuse tähtsust. Üldised õiguspärase töötlemise mõisted on suuresti jäänud samaks ning sarnaselt Direktiivis sätestatuga peab nõuolekuta töötlemisel olema töötlemise asjaolud selgesti õigusaktides sätestatud.

Seega EL tasandil on isikuandmete kaitsele antud põhiõiguse staatus. Samas andmete töötlemisel seaduse alusel andmesubjekt peab arvesse võtma, et andmete töötleja võib andmesubjekti osaluse põhimõttega seotud õiguseid nagu teavitamisekohustus andmesubjekti andmete töötlemisel, andmesubjekti nõusolek andmete töötlemisel ja juurdepääsuõigus, piirata. Kuid eeltoodust lähtuvalt ei tähenda töötlemine seaduse alusel siiski seda, et õiguspärase töötlemise põhimõtteid ei pea üldse arvesse võtma, vastupidi - seaduse alusel töötlemine tähendab, et see on lubatud, kui seadus seda selgesõnaliselt sätestab ning kasutusele on võetud asjakohased tagatised eelpool toodud põhimõtete tagamiseks. Andmekogu vastutav töötleja peab arvesse võtma, et andmesubjekti andmete töötlemisel oleks tagatud minimaalsuse, kasutuse piiramise, eesmärgikohasuse, andmesubjekti osaluse, seaduslikkuse, turvalisuse ja andmesubjekti osaluse põhimõtetest tulenevad nõuded. Samuti peab andmesubjektile olema tagatud kiire ja mõistlikult arusaadavalt esitatud teave tema andmete töötlemise kohta. Andmekaitse määruses sätestatud andmekogude koosvõimelisuse nõue on eelneva eelduseks.

[58] Ibid, preambula p 53 ja 61.
[59] Hornung, G. Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework. Innovation: The European Journal of Social Science Research, Vol. 26, Nos. 1-2, 2013, lk 182-183.
[60] Ibid, preambula p 68, 67.

1.2. Andmesubjekti osaluse põhimõte siseriiklikus õiguses

1.2.1. Eesti Vabariigi põhiseadus

Siseriiklikus õiguses on esmaseks allikaks andmesubjekti õiguste määratlemisel nimetatud Eesti Vabariigi Põhiseaduse (edaspidi PS) paragrahve 19; 26 ja 44 lõiget 3[61].

Andmesubjekti osaluse põhimõtte üheks tunnuseks on, et andmeid tohib töödelda vaid andmesubjekti nõusolekul ja teadmisel ning isikuandmete töötlemise protsess peab olema andmesubjekti poolt kontrollitav[62]. Seda väljendab PS paragrahv 19, mille kohaselt vaba eneseteostus on igaühe õigus[63]. Õigust otsustada, kui palju andmesubjekti kohta andmeid töödeldakse, peetakse samuti vaba eneseteostuse üheks oluliseks osaks[64]. Kahtlemata ei ole vaba eneseteostus võimalik, kui andmesubjekt ei ole teadlik tema kohta kogutavatest andmetest: isegi üksikute andmekoosseisude pinnalt on koostoimes mõne teise infokilluga võimalik teha ulatuslikke järeldusi andmesubjekti kohta, mistõttu on tõhusad õiguslikud tagatised äärmiselt olulised[65]. Alexy soovitabki tuletada § 19 lg 1-s sisalduvast enesemääramisõigusest õigus informatsioonilisele enesemääramisele. Ta lisab, et elektroonilised töötlussüsteemid on ohuks vaba eneseteostuse idee realiseerimisele, sest võimaldavad kergesti saada hulgaliselt teavet, mis koostoimes võivad anda märkimisväärselt palju informatsiooni isikute eraelu kohta.[66] Oluline on märkida, et põhiõiguste riivena on käsitletav iga isikuandmetega tehtava toiming[67].

PS paragrahv 26 on oluline eelkõige seetõttu, et see annab piirangud, millistel juhtudel andmesubjekti osaluse põhimõtte realiseerimist piirata tohib. PS paragrahvi 26 kohaselt perekonna ja eraelu puutumatus peab olema tagatud igaühele. [68] Kuid sama paragrahvi järgnev lause sätestab juhud, millal on selline sekkumine õigustatud. Andmesubjekti osaluse põhimõtte realiseerimist on võimalik piirata „seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks“.[69]

PS paragrahvi 44 lõikest 3 tuleneb õigus tutvuda võimuorganite poolt isiku kohta kogutavate andmetega. See on otseselt seotud andmesubjekti õigusega tutvuda oma andmetega, mis on

[61] PS, RT I 15.05.2015, §-id 19; 26; ja 44 lg 3.
[62] Ilus (2005), *supra* note 22, lk 523-524.
[63] PS, *supra* note 61, § 19.
[64] Truuväli, E. J. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. Tallinn: Juura 2002, kommentaar nr 4.1.
[65] Alexy, R. Põhiõigused Eesti põhiseaduses Juridica eriväljanne , Tallinn 2001, põhiõigused Eesti põhiseaduses, p. 6.1.2.2.
[66] Ibid, p. 6.1.2.2.
[67] Pilving, I. Õigus isikuandmete kaitsele. Juridica VIII/2005, lk. 533.
[68] PS, *supra* note 61, § 26.
[69] Ibid.

andmesubjekti osaluse põhimõtte üks alustalasid[70]. Mõistagi peab ka siin andmesubjekt arvesse võtma PS paragrahvist 26 tulenevaid piiranguid.

Kokkuvõtvalt võib öelda, et PS käsitluses andmesubjekti osaluse põhimõtte realiseerumise võimaldamine on andmesubjektile oluline eelkõige põhjusel, et see võimaldab tal oma käitumist vastavalt sellele juhtida ja ennast ühiskonnas vabalt teostada[71].

1.1.1. Isikuandmete kaitse seadus

Eestis reguleerivad isikuandmete töötlemist veel (antud töö kontekstis käsitletavate andmekogude puhul) IKS[72] ja AvTs[73]. Isikuandmete kaitse reguleerimise alguseks võib pidada 1996 aastat, hilisemalt on regulatsiooni korduvalt muudetud[74].

Seadusandja on IKS-is sisalduvaid põhimõtteid selgitades märkinud, et kõik eelpool nimetatud aktid, eelkõige Direktiivi põhimõtted on mõjutanud IKS arengut[75].

Isikuandmeteks peetakse sarnaselt Direktiivile andmeid tuvastatud või tuvastatava isiku kohta[76]. Seadusandja on selgitanud, et isikuandmeid ei saa olla juriidilisel isikul, kuna neil puudub eraelu[77]. Andmesubjektina käsitletakse isikut kelle isikuandmeid töödeldakse[78].

Isikuandmete töötlemise mõiste sisustamisel on samuti lähtutud Direktiivis sätestatust[79]. Seega ei omista IKS sarnaselt Direktiivis sätestatule tähtsust kas töötlemine toimub elektrooniliselt või mitte.

Andmesubjekti osaluse põhimõtet käsitletakse paragrahvis 6. Sarnaselt Direktiivis sätestatule tuleb andmesubjektile võimaldada juurdepääs temaga seotud andmetele, ning tal on õigus nõuda eksitavate ja valede andmete parandamist. Oluline on märkida, et andmesubjekt peab oma andmete töötlemiseks nõusoleku andma ja teda tuleb tema andmete töötlemisest teavitada, kuid samas on

[70] Ilus (2005), *supra* note 22, lk 528.
[71] Ibid, lk 524-525.
[72] IKS, *supra* note 6, §-d 4; 5 ja 8.
[73] AvTS, *supra* note 3, §-d 43 ja 43^2.
[74] Lillemaa, P. F. Märkusi isikuandmete kaitse seaduse eelnõu kohta. Juridica VII, 2002 lk. 447.
[75] Isikuandmete kaitse seaduse seletuskiri (17.01.2015).
[76] IKS, *supra* note 6, § 4.
[77] Isikuandmete kaitse seaduse seletuskiri, *supra* note 75, § 4.
[78] IKS, *supra* note 6, § 8.
[79] Ibid § 5: „Isikuandmete töötlemine on iga isikuandmetega tehtav toiming, sealhulgas isikuandmete kogumine, salvestamine, korrastamine, säilitamine, muutmine ja avalikustamine, juurdepääsu võimaldamine isikuandmetele, päringute teostamine ja väljavõtete tegemine, isikuandmete kasutamine, edastamine, ristkasutamine, ühendamine, sulgemine, kustutamine või hävitamine, või mitu eelnimetatud toimingut, sõltumata toimingute teostamise viisist ja kasutatavatest vahenditest“.

võimalik eelnevast kõrvale kalduda, kui andmeid töötleb haldusorgan avaliku ülesande täitmise käigus seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud kohustuse täitmiseks.[80]

Teavitamise põhimõttest on võimalik IKS paragrahvi 10 ja 14 alusel kõrvale kalduda, kui see on seaduses sätestatud. Kui isikuandmete töötlemine on ette nähtud seaduses, välislepingus või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduvas õigusaktis[81].

Lisaks väärib märkimist, et IKS paragrahvi 21 alusel ei ole andmesubjektil võimalik nõuda andmete töötlemise lõpetamist kui andmete töötlemine toimub seaduse alusel. Eelnevalt käsitletud Direktiiv ja Andmekaitse määrus võimaldavad töötlemise lõpetamist nõuda muuhulgas siis, kui töötlemine ei ole kooskõlas nimetatud dokumentides käsitletud õiguspärase töötlemise põhimõtetega.[82]

Sarnaselt Direktiiviga käsitletakse IKS-is ka teisi andmesubjekti osaluse põhimõtte realiseerimiseks vajalikke põhimõtteid[83].

Eeltoodust nähtub, et IKS-i mõistekasutus kattub suuresti Direktiivis käsitletuga (vt. p. 1.1.). Erisusena võib välja tuua, et isikuandmeid ja delikaatseid isikuandmeid ei eristata töötlemisele esitatavate nõuete mõistes, see tähendab, et isikuandmed on muuhulgas delikaatsed isikuandmed, kuid delikaatsete isikuandmete töötlemisele on seatud andmesubjekti jaoks täiendavad tagatised, näiteks peab asutuses olema isik, kes vastutab delikaatsete isikuandmete töötlemise õiguspärasuse eest, kui seda pole määratud, peab delikaatsete isikuandmete töötlemine olema AKI-s registreeritud.[84] Kuna töötlemisena käsitletakse ka infotehnoloogilist töötlemist, tulenevad sisulised nõuded andmekogule, mis töötleb isikuandmeid, siseriiklikus õiguses eelkõige IKS-ist. See tähendab, et lähtuma peab muuhulgas eelpool käsitletud õiguspärase töötlemise nõuetest, mis on üle võetud Direktiivist.

[80] Ibid, § 6.
[81] Ibid, §-d 10 ja 14.
[82] Ibid, § 21.
[83] Ibid, § 6: 1) Seaduslikkuse põhimõte – eraelu puutumatuse piiramine seadusliku aluseta on keelatud. 2) Eesmärgikohasuse põhimõte - andmete töötlemine ja töötlemise viis peavad olema kooskõlas andmete kogumiseks määratud eesmärgiga. 3) Minimaalsuse põhimõte – andmete kogumisel peab hindama, kas nende kogumine on vältimatult vajalik seatud eesmärgi saavutamiseks. 4) Kasutuse piiramise põhimõte – töödeldavate andmete kasutamine muudel eesmärkidel on võimalik üksnes andmesubjekti nõusolekul või õigustatud haldusorgani loal. 5) Andmete kvaliteedi põhimõte – isikuandmed peavad olema ajakohased ja täielikud, vastasel korral kaotab isikuandmete töötlemine mõtte. 6) Turvalisuse põhimõte – isikuandmete kaitseks peab rakendama asjakohaseid turvameetmeid, et tagada andmete säilimine ning kaitse volitamata töötlemise ja hävimise eest.
[84] Ibid, §-d 4; 5 ja 8.

Seega käesoleva töö tähenduses andmesubjekti osaluse põhimõtte kohaselt:

- andmesubjekti andmeid võib töödelda seaduse alusel juhul, kui see on õigusaktides selgesti ette nähtud;
- andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet milliseid andmeid tema kohta töödeldakse (v.a eelnevalt käsitletud piirangud);
- andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet millistele kolmandatele isikutele on tema andmeid edastatud (v.a eelnevalt käsitletud piirangud);
- andmesubjektil on õigus saada teavet oma andmete töötlemise eesmärkide kohta (v.a eelnevalt käsitletud piirangud);
- andmesubjektil on õigus saada teavet oma andmete töötleja kohta;
- andmesubjektil on õigus oma andmed töötlemiseks sulgeda, neid kustutada ja parandada kui andmeid ei töödelda õiguspärase töötlemise põhimõtetega kooskõlas;
- andmesubjektil on õigus saada teavet oma andmete töötlemise protsessi ja loogika kohta st eelnevalt käsitletud minimaalsuse, andmekvaliteedi, eesmärgikohasuse, seaduslikkuse, turvalisuse ja kasutuse piiramise kohta oma andmete töötlemisel.

1.1.2. Avaliku teabe seadus

AvTs defineerib andmekogu mõiste ja lisanõuded töötlemisele. Seega kui tegemist on isikuandmete töötlemisega, mis vastab andmekogu tunnustele AvTs mõistes, peab rakendama lisaks IKS-ile kõiki teisi nõudeid, mis tulenevad AvTs-ist. Tegemist on sisuliselt lisatagatistega andmesubjekti jaoks isikuandmete nõuetekohasel töötlemisel.

Andmekogu AvTs käsitluse kohaselt on „Riigi, kohaliku omavalitsuse või muu avalik-õigusliku isiku või avalikke ülesandeid täitva eraõigusliku isiku infosüsteemis töödeldavate korrastatud andmete kogum, mis asutatakse ja mida kasutatakse seaduses, selle alusel antud õigusaktis või rahvusvahelises lepingus sätestatud ülesannete täitmiseks“[85]. Käesolevas töös käsitletakse andmekogu mõistet vastavuses AvTs-is defineerituga. Käesoleva töö parema loetavuse huvides kasutatakse töös edaspidi eelnevalt defineeritud sõnastuse asemel sõnastust „seaduse alusel“.

Andmekogu asutamisel peab AvTs regulatsiooni kohaselt arvesse võtma järgnevat: andmekogu asutamine peab olema kooskõlastatud Riigi Infosüsteemi Ametiga, Andmekaitse Inspektsiooniga ja Statistikaametiga. Seejuures sätestatakse andmekogu kooskõlastamise mitme astmelisus: esiteks

[85] AvTS, *supra* note 3, § 43^1.

kooskõlastatakse andmekogu asutamine, seejärel andmekogu kasutuselevõtt. Kui mõlemad etapid on läbitud, toimub andmekogu registreerimine. Seega on lubatud kasutusele võtta registreeritud andmekogu.[86]

Kehtestatud on samuti nõuded andmekogude põhimäärustele. Andmekogu põhimääruses sätestatakse andmekogu pidamise kord, sealhulgas andmekogu vastutav töötleja (haldaja), andmekogusse kogutavate andmete koosseis, andmeandjad ja vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused. [87] Andmekogu õiguslikud küsimused seonduvad juurdepääsuõigusega, kolmandate isikutega, kellele andmeid on edastatud jne ning eesmärgikohasuse, seaduslikkuse ja kasutuse piiramise põhimõtetega.

Lisaks ei ole lubatud luua ühtede ja samade andmete kogumiseks eraldi andmekogusid[88]. See on otseselt seotud eelnevalt käsitletud minimaalsuse ja andmete kvaliteedi põhimõttega. Lähtuma peab põhiandmete kontseptsioonist, mille kohaselt ei tohi asuda koguma isikuandmeid, mida juba mõnes teises andmekogus selle andmekogu vastutava töötleja avalike ülesannete käigus kogutakse. Põhiandmete kontseptsiooni ja eelpool käsitletud õiguspärase töötlemise realiseerumine on aga otseses seoses riigi infosüsteemi kindlustavate süsteemidega. Olulisemad neist käesoleva töö kontekstis on riigi infosüsteemi haldussüsteem, infosüsteemide andmevahetuskiht ja infosüsteemide turvameetmete süsteem.

1.1.2.1. Riigi Infosüsteemi haldussüsteem

RIHA loodi 2008 aastal ja RIHA põhimääruse kohaselt on selle eesmärk riigi infosüsteemi haldamise läbipaistvuse tagamine[89].

AvTs alusel on kohustus andmekogu enne asutamisest ja enne kasutulevõttu kooskõlastada, millele järgneb registreerimine RIHA-s. RIHA põhimääruse paragrahvi 13 lõike 3 kohaselt RIHAs registreerimata andmekogu kasutusele võtmine on keelatud[90]. Andmekogu asutamise ehk esimene kooskõlastusring tuleb läbida vähemalt enne riigihanke väljakuulutamist. Ilmselgelt ei ole andmekogu kohta selleks ajaks veel võimalik esitada lõplikku dokumentatsiooni, sest arendustööde käigus, mis võivad kesta mitmeid aastaid, võib muutuda projekti skoop jne, mistõttu näiteks andmekogu põhimääruse lõplik versioon ja tehniline dokumentatsioon ei saa veel olla

[86] Ibid, § 43^2 lg 1; § 43^3 lg 3; 4 ja 5; § 43^7.
[87] Ibid, § 43^5.
[88] Ibid, § 43^3 lg 2.
[89] Riigi Infosüsteemi haldussüsteem, RT I, 04.07.2014, 7, § 13 lg 3.
[90] Ibid, § 13 lg 3.

riigihanke väljakuulutamise eelsel ajal valmis. Mõistagi ei pruugi hange ka õnnestuda, näiteks osutub arendustöö liialt kulukaks, mistõttu vajamineva dokumentatsiooni täies mahus koostamine selles etapis ei pruugi olla mõttekas. Eeltoodu tõttu on vajalik enne andmekogu kasutusele registreerimist läbida teine, kasutuselevõtu kooskõlastusring. Selleks ajaks peab olema võimalik esitada lõplik, täielik, andmekogu dokumentatsioon vastavalt RIHA põhimäärusele.

RIHA põhimääruses on mahukas kataloog RIHA-sse kantavatest andmekogu puudutavatest andmetest ja menetluskord. Nii hindavad andmekogu kasutuselevõtu valmidust AKI, Statistikaamet, Riigi Infosüsteemi Amet jt. Andmekogu peab enne kasutuselevõttu olema RIHA-s nähtav staatuses „kasutusel".[91] Selles menetluses annavad eelpool nimetatud asutused vastutava töötleja poolt esitatud dokumentatsiooni alusel hinnangu, kas andmekogus on rakendatud kõik õiguspärase töötlemise põhimõtted[92].

AKI peadirektor on kinnitanud lisaks täpsustava juhise andmekogude registreerimiseks RIHA-s ning selle kohaselt toimubki avaliku sektori andmekogude kooskõlastamine AKI poolt RIHA menetluse raames, kes kontrollib andmete õiguspärast töötlemist[93]. RIHA-s registreerimata andmekogu on keelatud kasutusele võtta[94].

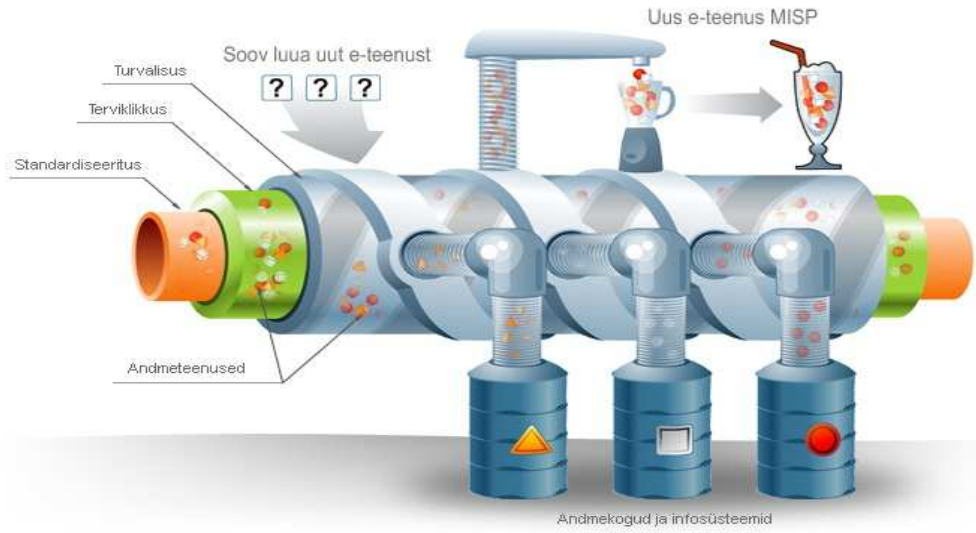
Kui andmekogu on registreeritud, tähendab see, et asjaolud, nagu põhimääruses sisalduvad sätted andmete juurdepääsude, kustutamise, töötlemise aluste ja muude isikuandmete nõuetekohaste töötlemise tingimuste kohta on heaks kiidetud. Samuti on Majandus- ja Kommunikatsiooniministeeriumi poolt hinnatud andmekogu arhitektuuri ja muude RIHA põhimääruses sätestatud asjaolude nõuetele vastavust. Lisaks on kasutuselevõtu kooskõlastanud Statistikaamet, Maa-amet, Riigi Infosüsteemide Amet ja Rahvusarhiiv.

Eeltoodut arvesse võttes on andmesubjekti jaoks kahtlemata oluline, et vastavad menetlused on tema andmeid töötleva andmekogu puhul läbitud, kuna selle menetluse raames antakse hinnang kõikidele eelpool käsitletud õiguspärase andmetöötluse põhimõtetele.

1.1.2.2. Infosüsteemide andmevahetuskiht

[91] Ibid, § 3; 7 ja 18.
[92] Ibid, § 7 lg 4; 5 ja 6.
[93] Andmekaitse Inspektsiooni menetluskord Riigi infosüsteemi haldussüsteemis, kinnitatud AKI peadirektori 14.08.2013.a käskkirjaga.
[94] Riigi Infosüsteemi Haldussüsteem, *supra* note 89, § 13 lg 3.

X-teega seonduvat reguleeritakse määrusega[95]. Riigi Infosüsteemide Ameti kodulehel avaldatakse, et X-tee võimaldab selle liikmete vahel turvalist liiklemist. X-teega liitujal on võimalik ise otsustada, kellele ta annab juurdepääsuõiguse teenustele ja milliseid teenuseid ta X-tee vahendusel osutab. X-tee tagab, et teave liigub vaid nende osapoolte vahel kes on õigustatud seda saama. Tõestusväärtuse tagamiseks on kasutusel digitaalallkirjastamine ning liikmete koosvõimelisus ei ole sõltuvuses liikmete poolt kasutatavast tehnoloogiast.[96] (vt. Joonis 1 „X-tee arhitektuur“).



Joonis 1. „X-tee arhitektuur“. Allikas: Riigi Infosüsteemide Ameti koduleheküg[97].

X-tee võimaldab otseselt realiseerida eelpool käsitletud andmete kvaliteedi ja minimaalsuse põhimõtteid, näiteks oleks keeruline teostada ilma X-tee olemasoluta põhiandmete kontseptsiooni realiseerumist.

Vastavalt X-tee määrusele X-teega liidestuja peab muuhulgas hoidma oma andmed RIHAs ajakohasena ning määrama andmekogule infosüsteemide kolmeastmeline etalonturbe süsteemi (edaspidi ISKE) kohase turbeastme ning ISKE-t ka rakendama[98]. See on vajalik, et üldse oleks võimalik tagada turvaline liiklus X-teel.

1.1.2.3. Infosüsteemide kolmeastmeline etalonturbe süsteem

[95] Infosüsteemide andmevahetuskiht RT I, 15.09.2015, 11.
[96] RIA koduleheküg https://www.ria.ee/ee/x-tee-tutvustus.html#mis (13.03.2016).
[97] Ibid.
[98] Infosüsteemide andmevahetuskiht, *supra* note 95, § 15 ja § 19.

AvTs näeb andmesubjektile ette lisatagatised vastavalt infosüsteemide turvameetmete süsteemi määrusele[99] (edaspidi ISKE määrus). Riigiasutused ja kohalikud omavalitsused (edaspidi KOV) peavad oma vastutaval töötlemisel olevate infosüsteemide kaitseks rakendama infosüsteemide kolmeastmelist etalonturbe süsteemi.

ISKE rakendamine seondub otseselt turvalisuse põhimõttega, mida käesoleva töö tähenduses andmekogud rakendavadki läbi ISKE. ISKE on samuti eeltoodud RIHA menetluse objektiks, ning peab olema andmekogu kasutuselevõtu hetkeks rakendatud.

Turvalisuse põhimõtte tagamiseks pannakse andmete töötlejale kohustus rakendada meetmeid käideldavuse, konfidentsiaalsuse ja turvalisuse tagamiseks. Käideldavus puudutab andmekogu kättesaadavust, terviklus andmete volitamatut töötlemist ja konfidentsiaalsus andmete volitamatut kasutamist. [100]

Eeltoodud käideldavuse, tervikluse ja konfidentsiaalsuse kaitseks peab vastutav töötleja korraldama ISKE osaklasside ja turbeastme määramise vastavalt määruse paragrahvile 7. ISKE määruse paragrahvis 9^1 on sätestatud, et ISKE rakendamist tuleb auditeerida perioodiliselt vastavalt andmekogule määratud turbeastmele. Samuti on määruses sätestatud auditeerimisele kuuluvad tööd ja kehtestatud nõuded audiitorile, kes on õigustatud auditit läbi viima.[101] ISKE rakendamise eest valitsusasutuses vastutab infoturbe juht, kelle määramine on kohustuslik[102]. Mis puudutab KOV andmekogusid, siis neile on kehtestatud erandid paragrahvis 9^2: KOV peab oma andmekogude puhul küll ISKE-t rakendama, kuid konkreetne auditeerimise intervall puudub – määruses on sätestatud, et KOV-ide puhul auditeerimist korraldab vajadusel Majandus – ja Kommunikatsiooniministeerium. Oluline on märkida, et määruse kohaldamisalast jäävad välja AvTs paragrahvis 43^1 nimetatud muud avalik-õiguslikud isikud või avalikke ülesandeid täitvad eraõiguslikud isikud, kes töötlevad samuti andmeid seaduse alusel ehk valdavalt ilma andmesubjekti nõusolekuta.

ISKE määruse paragrahvis 9 sätestatakse, et turbemeetmete rakendamine peab toimuma ISKE rakendusjuhendi ja ISKE kataloogi alusel, mis avaldatakse Riigi Infosüsteemide Ameti kodulehel[103]. ISKE määruses on sätestatud, et andmekogu turva osaklassid ja turbeastme ja seega rakendamisele kuuluvad meetmed määrab vastutav töötleja, kuid ISKE klassi määramine ei ole

[99] Infosüsteemide turvameetmete süsteem RT I, 15.09.2015, 11.
[100] IKS, *supra* note 6, § 25.
[101] Infosüsteemide turvameetmete süsteem, *supra* note 99, § 7 ja 9^1.
[102] Infoturbe juhtimise süsteem RT I, 19.03.2012, 4.
[103] ISKE rakendamise juhendid ja kataloogid. RIA kodulehekülg: https://www.ria.ee/ee/iske.html (13.03.2016).

vastutava töötleja suva: ISKE rakendamise juhend annab ette selged suunised, nii näiteks delikaatseid isikuandmeid sisaldava andmekogu konfidentsiaalsuse osaklass peab olema vähemalt S2. ISKE kataloogid koosnevad tuhandetest meetmetest alatest füüsilistest (nt hoonete, kus andmetöötlus toimub, füüsilised turvanõuded jne) ja organisatoorsetest meetmetest (nt tööprotsesside juhised töötajatele jne) lõpetades tehniliste nõuetega infosüsteemidele. Seega andmesubjekti seisukohast on äärmiselt oluline, et ISKE oleks rakendatud. Oluline on märkida, et ISKE rakendamine peab olema pidev, seetõttu on määratud ka ISKE auditeerimise intervallid. Näiteks kõrge turbeastmega andmekogu puhul on sätestatud kahe aastane auditeerimise intervall.[104] Andmesubjektil ongi võimalik tugineda auditeerimise kohta informatsiooni saamiseks andmekogu vastutava töötleja poolt antud selgitustele või tugineda RIHA-s avaldatud informatsioonile. Mõistagi ei ole võimalik andmesubjektil (tõenäoliselt) tutvuda auditi tulemustega sisuliselt, kuid tal on võimalik saada kinnitus kas andmekogu on auditeerimise läbinud edukalt. Võttes arvesse, et andmekogu vastutav töötleja on kohustatud hoidma RIHAs andmeid ajakohasena, on võimalik andmesubjektil huvi korral vastavat informatsiooni saada RIHA kodulehelt.[105]

1.2. Probleemid andmekogude regulatsioonis seoses andmesubjekti osaluse põhimõttega

1.2.1. Andmesubjekti teavitamiskohustus ja tema andmete töötlemine seaduse alusel

Andmesubjekti teavitamise põhimõte on oluline eelkõige seetõttu, et andmesubjektil on võimalik andmesubjekti osaluse põhimõtet täiel määral rakendada üksnes juhul, kui ta on teadlik, et tema andmeid töödeldakse[106]. IKS näeb andmesubjekti teavitamise kohustuse ette paragrahvis 15, kuid selle lõikes 2 on sätestatud, et teavitamiskohustust ei ole muuhulgas vaja täita kui isikuandmete töötlemine on ette nähtud seaduses, välislepingus või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduvas õigusaktis[107]. Seda põhimõtet väljendatakse samuti Direktiivis, kuid rõhutades, et teavitamiskohustusest kõrvalekaldumine peab siiski olema õigusaktides selgesõnaliselt sätestatud[108].

Teiselt poolt kaitseb andmesubjekti esmase andmeallika põhimõte, mille üldreegliks on, et andmetöötlus on lubatud vaid juhul, kui need on saadud andmesubjektilt eneselt. Selline

[104] Infosüsteemide turvameetmete süsteem, *supra* note 99, 9^1.
[105] RIHA kodulehekülg, *supra* note 2.
[106] Männiko, *supra* note 18, lk 45.
[107] IKS, *supra* note 6, § 15.
[108] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, *supra* note 35, art. 1 lg 2.

lähenemine tagab, et isikuandmete levimine on täielikult andmesubjekti kontrolli all. See võimaldab välistada vananenud või valede andmete levimise.[109]

Esmase andmeallika põhimõtet oleks aga keeruline järgida, kuna sadades infosüsteemides töödeldakse tuhandeid andmekoosseise. Sellises olukorras esmase andmeallika põhimõtte rakendamine oleks koormav nii andmete töötlejatele kui andmesubjektidele, kuna see eeldaks lakkamatut tegutsemist mõlemalt poolelt. Selline lähenemine, olles küll riigi jaoks efektiivne, ei ole aga läbipaistev andmesubjekti jaoks. Seetõttu on läbipaistvuse tagamiseks väga oluline, et andmete ristkasutus toimuks otsesel seaduslikul alusel, „/…/, et andmesubjektile oleks õigusaktidest üheselt selge, millised asutused milliseid andmeid töötlevad“[110].

Eelpool toodud seisukohad realiseeruvad IKS-is, mille kohaselt on andmete töötlemine võimalik üksnes andmesubjekti nõusolekul, kuid näeb samas ette, et haldusorgan võib avalike ülesannete täitmiseks töödelda andmeid ka ilma andmesubjekti nõusolekuta, seades eelduseks, et töötlemine toimub seaduse alusel[111].

Põhiõiguste riivet avalike ülesannete täitmisel on aktsepteerinud ka ELK asjas *Huber vs. Saksamaa:*[112] kaebaja soovis endaga seotud andmete kustutamist välismaalaste registrist. Registrile omasid juurdepääsu ka teised haldusorganid. ELK sedastas, et niisugune töötlemine on Direktiivi artikli 7 punkti e alusel õiguspärane, sest on seotud haldusorgani poolt avalike ülesannete täitmisega.

Kuid seaduse alusel töötlemine ei tähenda pelgalt üldsõnalist volitusnormi. Seaduse alusel töötlemisele hinnangut andes peab seda vaatlema läbi seadusliku töötlemise põhimõtte. Männiko peab oluliseks märkida, et andmetöötlus peab olema korraldatud viisil, mis võimaldab andmesubjektil andmetöötluse eesmärke mõista ning andmesubjektil oleks võimalik olla oma andmete töötlemisest teadlik [113]. Vastutav töötleja peab arvesse võtma andmesubjekti huvisid ja ootusi ausale andmetöötlusele. Andmete töötlemine peab olema korraldatud viisil, mis ei ole vastuolus andmesubjekti huvidega ning vastaks andmesubjekti ootusele ausa andmetöötluse osas.

[109] Ilus (2005), *supra* note 22, lk 522-523.
[110] Ibid, lk 523.
[111] IKS, *supra* note 6, §-d 10; 14 lg 1 p 1.
[112] ELK, 16.12.2008, C-524/06, *Huber vs. Saksamaa*, p 49.
[113] Männiko, *supra* note 18, lk 45.

Lisaks tähendab seaduslik töötlemine, et andmetöötlus peab olema läbipaistev andmesubjekti jaoks.[114]

Eeltoodud seisukohti ilmestavad mitmed lahendid: näiteks võib tuua *Rotaru vs Rumeenia*[115]. Menetluse käigus tuvastati seaduslikkuse põhimõtte rikkumine, kuna õigusaktides oli küll antud volitusnorm jälitusandmete kogumiseks, kuid ei olnud määratletud selgesti andmetöötluseesmärke, mis võimaldas samu andmeid töödelda ka erinevatel teistel eesmärkidel, hindas EIK selle EIÕKonv artikli 8 põhimõtetega vastuolus olevaks.

Asjas *Taylor-Sabory vs Ühendkuningriik*[116] leidis EIK samuti EIÕKonv artikli 8 rikkumise: kaebaja riigi õiguses ei olnud reguleeritud jälitustegevus infotehnoloogiliste vahendite (antud juhul piipari kloon) abil, mistõttu ei olnud õiguspärane selliste andmete kasutamine prokuröri poolt.

Mikiver *et al.* toovad seadusliku töötlemise põhimõtte eiramise näitlikustamiseks Eestis näite Piirivalve infosüsteemist. 2003. aastast alates koguti sellesse andmekogusse andmeid mitmetest teistest andmekogudest nagu näiteks sissesõidukeeldude riiklik register, infosüsteem POLIS jne. Õiguskantsleri poolt läbiviidud menetluse käigus selgus, et juurdepääsusillad loodi siseministri ja politsei peadirektori käskkirjadega, isikuandmed anti üle aktidega. Õiguskantsler jõudis oma menetluses järeldusele, et tulenevalt PS paragrahvi 3 lõike 1 halduse seaduslikkuse põhimõttest ei ole võimalik eelpool nimetatud aktidega luua õigust andmete edastamiseks.[117]

Kurioosse näitena on käsitletud samuti nakkushaiguste ennetamise ja tõrje seaduse (NETS) alusel loodud registrit, mille volitusnormi ei saa pidada selgesõnaliseks. Probleemsena toodi NETSi puudutavas ja AKI poolt läbi viidud menetluses esile, et andmekogu andmekoosseisus käsitleti eriti ohtlike ja epideemilisel teel levivate haigustena ka näiteks sügelisi, loomahammustusi jne. Nende andmete säilitamise tähtaeg (isikustatud kujul) oli 75 aastat. AKI, selgitanud välja, et näiteks sügelisi ja looma hammustusi ei saa pidada eriti ohtlikeks, mistõttu ka nende andmete isikustatud kujul pikaajaline säilitamine ei saa olla õiguspärane, pöördus vastutava töötleja poole (sotsiaalministeerium) selgituste saamiseks. Sotsiaalministeerium põhjendas isikustatud kujul

[114] Bygrave (2014), *supra* note 29, lk 147.
[115] EIKo 04.05.2000, 28341/95, *Rotaru vs Rumeenia*, p 57.
[116] EIKo 47114/99, 22. oktoober 2002, *Taylor-Sabory vs Ühendkuningriik.*
[117] Tupay, P. K.; Mikiver M. E-riik ja põhiõigused. Juridica III/2015, lk 165.

andmete töötlemist (sh sügeliste ja loomahammustuste kohta) muuhulgas „/…/ terrorismivastase võitluse argumendiga“.[118] Kahtlemata jääb säärane seos andmesubjektile arusaamatuks.

AKI on lisaks oma 2013 aasta aastaaruandes esile toonud probleemi, et andmekoosseise kirjeldatakse üldsõnaliselt, mis ei võimalda järeldusi teha millises ulatuses andmeid tegelikult töödeldakse, mistõttu AKI-il on keeruline hinnata riive ulatust ja põhjendatust.[119]

1.2.1.1. Andmesubjekti teavitamiskohustus ja tema andmete seaduse alusel töötlemine andmekogude regulatsioonis

IKS kohaselt on isikuandmete töötlemine lubatud kui see toimub seaduse alusel. Kuid kui isikuandmete töötlemine toimub andmekogus AvTs mõttes, tuleb lähtuda lisaks andmekogude regulatsioonist. Seega kui tegemist on isikuandmete töötlemisega, mis vastab andmekogu tunnustele AvTs mõistes, peab rakendama lisaks IKS-ile kõiki teisi nõudeid, mis tulenevad AvTs-ist. Tegemist on sisuliselt lisatagatistega andmesubjekti jaoks isikuandmete nõuetekohasel töötlemisel. Näiteks peavad olema läbitud RIHA menetlused, rakendama peab ISKE-t.

Esmasel vaatlusel võib tunduda, et Eestis on andmesubjekti õigused tagatud piisavalt: AvTs on sisustanud põhimääruse nõuded, IKS andmetöötluse üldised põhimõtted, ISKE annab lisatagatised andmete turvalisel töötlemisel, ning õiguspärase töötlemise kontroll viiakse läbi RIHA menetluste raames. Eelmises alapunktis jõuti järeldusele, et andmesubjekti osaluse põhimõtte ühte olulisemat tahku, teavitamiskohustust, seaduse alusel andmetöötluse puhul sisuliselt järgima ei pea. See tähendab, et seaduse alusel andmete töötlemisel oleneb andmesubjekti teadlikkus tema andmete töötlemisest ja seega ka andmesubjekti põhimõtte rakendamine paljuski sellest, kui arusaadavad on tema jaoks andmete töötlemist käsitlevad õigusaktid, millised on võimalused andmetöötluse lõpetamiseks ja kui läbipaistev on tema jaoks töötlusprotsess. Samuti, nagu eelnevalt käsitletud, ei ole andmesubjektil IKS alusel õigust nõuda oma andmete töötlemise lõpetamist, kui töötlemine toimub seaduse alusel. Mõistagi on andmesubjektil õigus pöörduda nii kohtusse kui AKI poole, kuid kuna põhimäärustele esitatud nõuded on minimaalsed, volitusnormid üldised, mis ei võimalda volitusnormi konkreetse eesmärgiga seostada, on andmesubjektil keeruline põhistada rikkumist oma andmete töötlemisel. Samuti, kui andmesubjekt tuvastab, et tema andmeid kogutakse andmekogus, mille osas AvTs alusel nõutavad menetlused on läbimata st, andmetöötluse

[118] Ibid, lk 169.
[119] Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2013, soovitused aastaks 2014, lk 60 http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202013%20l%C3%B5plik%20PDF.pdf (17.01.2016).

turvalisus ja muud õiguspärase andmetöötluse sisulised küsimuse on läbi vaatamata, võib see kaasa tuua raskeid tagajärgi andmesubjekti eraelus (näiteks HIV positiivsete registrist andmete lekkimise oht). Ka eelnevalt käsitletud Andmekaitse määruses viidati võimalikele sotsiaalsetele ja majanduslikele tagajärgedele seoses andmetöötlusega, selle riski maandamiseks Andmekaitse määruse kohaselt peab hindama juba andmekogu kavandamisel milliseid infotehnoloogilisi abinõusid rakendada ning mitteõiguspärasest andmetöötlusest peab andmesubjekti teavitama 24 tunni jooksul.

Kui vaadata näiteks RIHA kodulehel[120] olevaid andmeid, mis on avalikud ja peaksid andma adekvaatset informatsiooni riigi infosüsteemide kohta, tekib mitmeid küsitavusi.

Võtame näiteks tuntumad infosüsteemid, mis töötlevad isikuandmeid ja vastavad andmekogu mõistele AvTs mõistes: karistusregister, DNA register, sõrmejälje register ja POLIS[121]. On üldteada, et need infosüsteemid töötlevad isikuandmeid juba aastaid. Nagu eelpool öeldud, kasutusel olev andmekogu peab olema RIHA-s registreeritud ehk RIHA-s kuvatud staatuses „kasutusel". Eelpool toodud registrite puhul on staatuseks „asutamine kooskõlastamisel" või „asutamine kooskõlastatud".[122] See tähendab, et kasutuselevõtmise menetlusetapp, mis on andmekogu õiguspärase kasutamise eeltingimus, on täielikult läbimata[123]. Andmesubjekt saab selle informatsiooni pinnalt järeldada, et tema andmete töötlemist nendes infosüsteemides (veel) ei toimu. Selline olukord andmesubjekti jaoks on kindlasti kõike muud kui läbipaistev. Veelgi enam, kuna AvTS alusel on infosüsteemi kasutuselevõtu ja seega ka selles andmete töötlemise eelduseks seadusest tulenev alus ja teiseks nõuetekohane registreering RIHAs, ei ole tegemist õiguspärase andmete töötlemisega. IKS - i kohaselt andmesubjektil on IKS paragrahv 21 ja 22 alusel võimalik nõuda oma andmete ebaseadusliku andmetöötlemise lõpetamist ja kahju hüvitamist (riigivastutuse seaduse alusel). Samas on selline õigus piiratud: töötlemise lõpetamist ei ole õigus nõuda kui andmeid töödeldakse seaduse alusel. Eelnevalt on EL õigusaktidele ja samuti IKS-ile tuginedes järeldusele jõutud, et andmesubjektile tuleb tagada asjakohased tagatised oma õiguste kaitseks. RIHA-s läbiviidavas menetluses antakse hinnang sisuliselt kõikidele IKS paragrahvis 6 sätestatud isikuandmete õiguspärase töötlemise põhimõtetele AKI-i poolt, st menetlus on sisuliselt andmesubjekti õiguste kaitseks. Näiteks POLIS jt eelpool nimetatud

[120] RIHA koduleheküg, *supra* note 2.
[121] Staatused RIHAs seisuga 17.01.2016.
[122] RIHA menetluskord on mitmeks osaks jaotatud põhjusel, et RIHA kooskõlastus on vajalik saada enne hanke väljakuulutamist, kui mõistetavalt ei ole selleks ajaks veel näiteks valmis põhimäärust. Samas nõuab infosüsteemi kasutuselevõttu menetluse läbimine lõpliku dokumentatsiooni esitamist. Asjaolu, et RIHA menetlused on jaotatud mitmesse etappi nähtub ka AvTs § 43^3ja 43^7.
[123] Riigi Infosüsteemi haldusüsteem, *supra* note 78, § 7 lg 9 ja § 10.

infosüsteemides töödeldakse ka delikaatseid isikuandmeid, kuid need infosüsteemid ei ole RIHAs nõuetekohaselt registreeritud, see tähendab, et nende andmekogude puhul ei ole andmesubjektil kindlust kas andmetöötlus on nõuetekohane. POLIS-e andmed on RIHA-s, tuginedes kooskõlastamise andmetele, ajakohastamata alates 2008. aastast, seega andmesubjektid sisuliselt taluvad juba aastaid riigi omavoli oma andmete töötlemisel, see tähendab, et neil ei ole kindlust isikuandmete nõuetekohases töötlemises.

Töö autori hinnangul olukorra parandamiseks RIHA menetluste osas peab rakendama tõhusamat avalikkuse kontrolli. Infotehnoloogilisi vahendeid avalikkuse kontrolli tõhustamiseks käsitletakse käesoleva töö teises peatükis.

1.2.2. Kontrollipõhimõte ja andmesubjekti juurdepääsuõigus tema kohta käivatele andmetele

Kontrollipõhimõte andmesubjekti vaatest on oluline eelkõige seetõttu, et see annab võimaluse ebaadekvaatsete andmete töötlemise, ebaseadusliku töötlemise jne. lõpetamist[124]. Selle põhimõtte alusel on võimalik kontrollida kõiki teisi õiguspärase andmetöötluse põhimõtteid[125].

Männiko nimetab andmesubjekti õigust omada kontrolli oma isikuandmete töötlemise üle üheks põhimõtteks mida võib pidada andmekaitsel läbivaks[126]. Ta rõhutab, et andmesubjektil on õigus eeldada, et tema isikuandmete töötlemine toimub õiguspärase töötlemise põhimõtetega kooskõlas[127].

Nendeks põhimõteteks on eesmärgikohasuse, andmete kvaliteedi, minimaalsuse, kasutuse piiramise, turvalisuse põhimõtted ning juba eelnevas alapunktis käsitletud seaduslikkuse põhimõte. Nimetatud põhimõtteid käsitletakse IKS paragrahvis 6[128] ja Direktiivi preambuli punktides 38–43 ja artiklites 10–14.[129]

Eelnevas alapunktis käsitletud seaduslikkuse põhimõte on lähedalt seotud eesmärgikohasuse põhimõttega. Selle kohaselt isikuandmeid tohib koguda rangelt vaid selgesõnaliselt väljendatud eesmärkidel, milleks on olemas konkreetne volitusnorm. Kui andmeid soovitakse edastada

[124] Ilus (2005), *supra* note 22, lk 525.
[125] Bygrave (2014), *supra* note 29, lk 158.
[126] Männiko, *supra* note 18, lk 52.
[127] Ibid, lk 52.
[128] Isikuandmete kaitse seadus, *supra* note 6, § 6.
[129] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, *supra* note 35, art. 10-14.

kolmandatele isikutele, tuleb seda käsitleda uue eesmärgina. Isikuandmete andmete töötlemine, millel puudub konkreetselt piiritletav eesmärk, ei ole see seaduslik.[130]

Seadusandja on IKS seletuskirjas täiendavalt selgitatud, et enne andmete koguma asumist peab olema andmetöötluse eesmärk kindlaks määratud ja igal järgneval andmete töötlemisel peab olema seos andmete algupärase töötlemise eesmärgiga. Samuti ei ole eesmärgikohasuse põhimõttega vastuolus kui andmeid töödeldakse teadusuuringu läbiviimiseks või statistika kogumise eesmärkidel, kui andmed on kodeeritud, see tähendab, et isikut ei ole võimalik teatud andmekoosseisuga seostada.[131]

Eesmärgikohasuse põhimõte tähendab muuhulgas, et isikuandmete töötlemine on lubatud rangelt üksnes senikaua kui see on vajalik töötlemise eesmärkide saavutamisel[132]. Seega andmed peavad olema kogutud viisil, mis vastaks eesmärgile, milleks neid kogutakse, eesmärk ise peab olema täpne, legitiimne, defineeritud, dokumenteeritud[133]. EIK on samuti korduvalt rõhutanud, et andmete säilitamisel peab olema selge seos nende kogumise eesmärgiga[134].

Eesmärgikohasuse põhimõtte rikkumisest võib tuua näiteks ka Riigikohtu halduskolleegiumi asja 3-3-1-3-12, p. 19, milles Justiitsministeeriumi väljaanne Vangla Ekspress avaldas artikli kriminaalasja kohta, mis oli Harju Maakohtu menetluses (menetlus ise oli avalik). Kohus sedastas, et andmete mingis vormis eelnev avaldamine ei tähenda, et igal järgneval samade andmete avaldamisel puuduvad andmesubjekti jaoks olulised tagajärjed põhjusel, et need on juba niikuinii avalikud. Oluline on hinnata nii konteksti kui infokanalit: näiteks meediaväljaandes avaldatud informatsioon on reeglina kättesaadav märkimisväärselt laiemale isikute ringile kui kohtsaalis avaldatu.[135] Andmetöötlusega seotud eesmärgid on siduvad ja kui on soov neid eesmärke muuta, nõuab see õigusselget alust[136]. Eesmärgikohasuse põhimõtte kohta andmete säilitamise kontekstis on näiteks toodud Ametlike Teadaannete infosüsteem, mille põhimääruses ei olnud reguleeritud andmete kustutamise tingimused. See lõi olukorra kus Internetist oli võimalik leida hulgaliselt

[130] Ibid art 6 lg 1 p b; *supra* note 20, art 5 p b.
[131] Isikuandmete kaitse seaduse seletuskiri, *supra* note 75.
[132] Ibid.
[133] Bygrave (2014), *supra* note 29, lk 153-155.
[134] EIKo 4. detsember 2008, 30562/04 ja 30566/04, *S. ja Marper vs. Ühendkuningriik*; EIKo 13. november 2012, 24029/07, *M.M. vs. Ühendkuningriik*.
[135] RKHKo 12.07.2012,3-3-1-3-12, p. 24.
[136] Albers, M. Isikuandmete kaitse põhiõiguslik alus: kas õigus informatsioonilisele enesemääramisele ja/või eraelu austamisele. Juridica VIII 2005, lk 540.

vananenud andmeid (sh juba tasutud võlgnevuste kohta), [137] mis võisid omada teistes menetlustes (nt laenu taotlemine) negatiivseid tagajärgi andmesubjektile.

Ka AKI menetluste raames on eesmärgikohasuse, kasutuse piiramise ja minimaalsuse põhimõtted käsitlemist leidnud. Näiteks tuvastas AKI, et videokaamerad salvestasid Laagri Koolis informatsiooni kõikides klassides toimuva kohta, kuid põhikooli ja gümnaasiumi seaduse kohaselt on lubatud ohu ennetamiseks küll videokaameraid kasutada, kuid videokaamerate kasutamisel peab lähtuma lisaks IKS põhimõtetest, mistõttu valimatus ulatuses jälgimisseadmete kasutamist ei saa lugeda õiguspäraseks.[138]

Ridamisi näiteid õiguspärase töötlemise eiramisest on samuti e-tervise, rahvastikuregistri ja POLIS-e kohta.

2012 aasta seisuga oli e-tervises üle 6 miljoni tervise dokumendi, andmekoguga liidestunud asutusi 503. E-tervisest saadud andmete avaldamisel volitamata isikutele võib inimesele põhjustada väga tõsist kahju. Näiteks võttis AKI-ga ühendust naine, kes kinnitas, et tema eks-ämm, kellel oli juurdepääs e-tervisele, kasutas kohtuvaidluses, mis puudutas paari ühist last, naise kompromiteerimiseks e-tervisest saadud tervise infot (näiteks varasemate raseduste, nurisünnituste kohta).[139] Arstide ja teiste tervishoiutöötajate poolt uudishimust andmete vaatamine on levinud laialdaselt[140].

Ka rahvastikuregistri andmete töötlemisel on mitteõiguspärane töötlemine seotud eelkõige uudishimuga tuntud inimeste või tuttavate eraelu vastu. Märkimisväärselt arvukalt on väärkasutamisi KOV-ide poolt. [141] Näiteks vaatas üks KOV ametnik andmeid presidendipaari kohta, kuid selgitas, et tõenäoliselt keegi kasutas volitamatult tema arvutit. Kurioosse näitena võib tuua PPA ametniku, kes selgitas seitsme tuntud isiku andmete vaatamist Schengeni viisaruumi piiride säilimise tagamisega. Ta selgitas, et tuntud isiku sissekirjutus võib mõjutada tema fännide eelistust nende elukohavalikul, ning seda informatsiooni on tingimata vaja arvesse võtta üksuse töö planeerimisel. Teine PPA ametnik tunnistas samuti uudishimust ajakirjas „Kroonika“ esitletud

[137] Tupay, Mikiver, *supra* note 117, lk 172-173.
[138] Avaliku teabe seaduse a isikuandmete kaitse seaduse aastal 2014, soovitused aastaks 2015. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat%202014.pdf lk 38, (17.01.2016).
[139] Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2012, soovitused aastaks 2013, lk 68. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202013%20l%C3%B5plik%20PDF.pdf (17.01.2016).
[140] Ibid, lk 76; Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2013, soovitused aastaks 2014, *supra* note 119, lk 46.
[141] Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2013, soovitused aastaks 2014, *supra* note 119, lk 47-48.

ja telesaates „Eesti otsib superstaari“ osalenud isikute ja nende perekonnaliikmete kohta informatsiooni hankimist. Kuid on esinenud ka juhtumeid kus rahvastikuregistrisse on lihtsalt sisestatud suvalisi sõnu ja tähekombinatsioone eesmärgiga saada teavet kas teatud nimelisi isikuid on olemas.[142]

Andmetöötlus peab olema kooskõlas seaduslikkuse ja eesmärgikohasuse põhimõttega, kuid mitte ainult: andmed peavad olema kvaliteetsed, vastupidisel juhul kaotaks nende töötlemine mõtte, kuid järgima peab ka minimaalsuse põhimõtet, mille kohaselt ei tohi andmeid ülemääraselt koguda.

Andmete kvaliteedi ja eesmärgikohasuse põhimõtte näitlikustamiseks negatiivses mõttes on toodud esile e-toimiku süsteemi, milles nõutakse füüsilise isiku kohta lisaks muudele andmetele ka füüsilise isiku sugu. Füüsilise isiku sugu ei saa aga omada tähtsust tsiviilmenetluse raames.[143]

Seadusandja on IKS seletuskirjas täpsustanud, et kuna isikuandmete töötlemise puhul on tegemist põhiõiguste riivega, mida andmetöötleja õigustab üldjuhul mingi konkreetse eesmärgi saavutamisega (nt avaliku korra tagamine), siis ei saa olla põhjendatud ebatäpsete andmete töötlemine, kuna sellisel juhul ei taga see ka eesmärgi saavutamist, milleks andmeid kogutakse. Lisaks piiratakse andmete kvaliteedi põhimõtte kohaselt andmete ülemäärast kogumist[144].

Männiko selgitab, et nö igaks juhuks andmete töötlemine on praktikas levinud laialdaselt, ning hindab seda minimaalsuse põhimõttega vastuolus olevaks[145]. Minimaalsuse põhimõte tähendab ka seda, et andmed, mis tuleb õigeaegselt kustutada või anonümiseerida[146].

Andmete kvaliteedi, minimaalsuse ja eesmärgipärase töötlemise näitena võib tuua EIK asja *Khelili vs Sveits*[147], mille lahendis rõhutatakse, et tuleb alati hinnata kas andmete kogumine on proportsionaalne täitmiseks seatud ülesandega. Politsei leidis kontrolli läbiviimisel kaebajalt visiitkaardi, milles viimane avaldab soovi kohtuda meestega, et nendega aega veeta. Selle asjaolu alusel pidas politsei õigeks lisada oma andmebaasi kaebaja kohta hinnangu „prostituut“ (vaatamata kaebaja vastuväidetele). Kohus hindas, et niivõrd üldine tõend ei saa olla niivõrd intensiivse riive

[142] Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2011, soovitused aastaks 2012. lk 67-68. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202013%20l%C3%B5plik%20PDF.pdf (17.01.2016).
[143] Männiko, *supra* note 18, lk 46.
[144] Isikuandmete kaitse seaduse seletuskiri, *supra* note 75.
[145] Männiko, *supra* note 18, lk 45.
[146] Bygrave (2014) *supra* note 29, lk 151-152.
[147] EIK 18. oktoober 2011, nr 16188/07, *Khelili vs Sveits.*

aluseks viidates muuhulgas ka asjaolule, et ametivõim peab hea seisma ka selle eest, et kogutavad andmed oleksid täpsed.

Minimaalsuse ja kasutuse piiramisega seonduvat on samuti käsitlenud AKI oma aastaaruandes. Näiteks Eesti Hariduse infosüsteemis kehtestati 75 aastase säilitustähtaeg andmetele. AKI hinnangul ei saa olla põhjendatud, et asjaolude nagu õpilase puudumised, õpiabi ja hinded säilitamise vajadus võiks olla niivõrd pikk (75 aastat). [148]

Teise kujuka näitena võib tuua Tallinna ühistranspordi valideerimise süsteemi. Valideerimissüsteemiga seotud andmete 7 aastane säilitustähtaeg viitega raamatupidamise algdokumentidele ei saa olla kuidagi põhjendatud.[149]

Kasutuse piiramist on käsitlenud näiteks ELK liidetud asjas *Volker und Markus Schecke GbR ja Hartmut Eifert vs. Land Hessen*[150]. Küsimuse all oli isikuandmete avaldamine antud juhul põllumajandusega seotud fondidest toetuse saamise menetlustes. Isikuandmete avaldamisel ei tehtud vahet erinevate menetlusliikide vahel, samuti ei omanud tähtsust taotletav summa ega muud erisused. Kohus jõudis järeldusele, et selline lähenemine ei ole proportsionaalne, sedastades, et iga andmekoosseisu avaldamine peab olema läbi mõeldud ja kaalutud millist avalikku huvi sellise teabe avaldamine demokraatlikus ühiskonnas annab.

Isikuandmete kaitseks tuleb rakendada lisaks asjakohaseid turvameetmeid. See tähendab, et tagada tuleb isiku andmete volitamata töötlemine, konfidentsiaalsus ja terviklus. Seda väljendavad Direktiivi artikli 17 lõige 1 ja preambuli punkt 46.[151]

Seadusandja on IKS seletuskirjas täiendavalt selgitanud, et andmetöötlussüsteemide loomisel ja andmete töötlemise ajal peab volitamata töötlemise välistamiseks rakendama turvalisuse tagamiseks asjakohaseid meetmeid. Edasi rõhutatakse, et turvameetmete piisavus on ajas muutuv tulenevalt tehnoloogia arengust, ning seetõttu peab vastutav töötleja alati hindama kättesaadava tehnoloogia kasutamise võimalikkust oma andmekogus.[152]

---

[148] Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2013, soovitused aastaks 2014, *supra* note 138, lk 36.
[149] Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2012, soovitused aastaks 2013, *supra* note 139, lk 67.
[150] ELKo, 9. november 2010, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert vs. Land Hessen*, p 89 ja 86.
[151] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, *supra* note 35, art lg 1 p 17 ja preambula p 46.
[152] Isikuandmete kaitse seaduse seletuskiri, *supra* note 75.

Andmesubjekti osaluse üheks aluspõhimõtteks on juurdepääsuõiguse tagamine. Ilma juurdepääsuõiguse võimaluseta ei oleks võimalik kontrollida ka kõiki eelpool toodud õiguspärase töötlemise põhimõtteid.

Et riik peab tagama andmesubjektile selge arusaama kuidas nende andmeid töödeldakse on käsitletud EIK asjas *Haralambie vs. Rumeenia*[153]. Kaebajal oli võimalik enda kohta käivate andmetega tutvuda alles viis aastat peale taotluse esitamist. Asutus, kes oli kohustatud vastavad andmed kaebajale teatavaks tegema esitas põhjenduseks puudused oma asutuse töö korraldamisel nt puudused arhiivis. EIK sedastas, et andmesubjektile tuleb tagada juurdepääs temaga seotud andmetele mõistliku aja jooksul ning lisas, et juurdepääsu võimaldamisega seotud menetlused peavad olema tõhusad.

Andmesubjekti osaluse põhimõte tähendab, et andmesubjektil on õigus teada kellele tema andmeid on edastatud. Mikiver *et al.* kritiseerivad 1.01.2008. aastast kehtima hakanud uut AvTS-i regulatsiooni. Andmekogu kasutamise üksikküsimused sätestatakse määruse tasandil, kuid AvTSis on põhimäärustele kehtestatud nõuded äärmiselt üldsõnaliselt. Nii ei ole põhimääruses kohustuslik reguleerida näiteks andmete säilitamisega seotud tähtaegu ning haldusorganeid kellele võimaldatakse püsiv andmetele juurdepääs. 2013 aastal töötati AKI eestvõtmisel välja andmekogude juhend[154], selles antakse mitmeid soovitusi eesmärgiga AvTS-i puuduliku regulatsiooni tasandada. Juhendis nähakse põhimäärustes ette nii andmete saajad kui ka saamise kord, samuti andmete hävitamist ja säilitamist puudutav. Samas möönavad Mikiver *et al.*, et „Isegi kui andmekogu asutamine ja seega ka andmekogu asutamisdokumentatsioon läbib AKI kooskõlastamis menetluse, on küsitav, kas AKI soovitusliku iseloomuga juhend saab asendada seadust ning tagada andmekogude ühtsust ja luua sel moel piisav põhiõiguslik kaitse“.[155]

1.2.2.1. Kontrollipõhimõte ja andmesubjekti juurdepääsuõigus tema kohta käivatele andmetele andmekogude regulatsioonis

IKS näeb ette, et andmesubjekti soovil tuleb temale väljastada terve kataloog andmetest viie tööpäeva jooksul taotluse esitamisest arvates. Seaduses sätestatud juhtudel võib ette näha ka erandeid. Nendeks andmeteks IKS kohaselt on:

- tema kohta käivad isikuandmed;

[153] EIKo, 27. oktoober 2009, 21737/03, *Haralambie vs. Rumeenia.*
[154] Andmekogude juhend, http://www.aki.ee/et/juhised, 17.01.2016.
[155] Tupay, Mikiver, *supra* note 117, lk 170.

- isikuandmete töötlemise eesmärgid;
- isikuandmete koosseisu ja allikad;
- kolmandad isikud või nende kategooriad, kellele isikuandmete edastamine on lubatud;
- kolmandad isikud, kellele tema isikuandmeid on edastatud;
- isikuandmete töötleja või tema esindaja nime ning isikuandmete töötleja aadressi ja muud kontaktandmed.[156]

AvTS näeb ette, et andmekogu asutamine on lubatud seadusega või selle alusel antud õigusaktiga. Andmekogu pidamise täpsem kord aga sätestatakse andmekogu põhimäärusega. Andmekogu põhimäärusele kehtestatud nõuete kohaselt peab põhimääruses olema määratletud:

- vastutav töötleja;
- andmekogusse kogutavate andmete koosseis;
- andmeandjad;
- vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused.[157]

Kui võrrelda IKS andmesubjekti osaluse põhimõttest tulenevate nõuete kataloogi asjaoludes, mida andmesubjektil on õigus välja küsida vastutava töötleja käest, andmekogudele esitatavate nõuetega AvTs-is, selgub, et AvTs nõuded andmekogude põhimäärustele on märkimisväärselt tagasihoidlikumad.

Samuti selgus, et volitusnormid andmekogude loomiseks on üldsõnalised ning, et probleemiks on andmekogude põhimäärustele esitatavad nõuded, mis on samuti üldsõnalised ega sätesta näiteks kohustust sätestada selgesõnaliselt andmesaajaid ning andmete säilitamistähtaegu. Lisaks võib järeldada, et üldsõnalised nõuded põhimäärustele on tekitanud probleeme RIHA menetlustes, mistõttu AKI on koostanud mitmeid juhiseid, mille rakendamises selle soovitusliku iseloomu tõttu mitmed autorid kahtlevad.

Kontrollipõhimõte eeldab samuti, et andmesubjektil on võimalik mõistlikult hinnata oma andmete õiguspärast töötlemist. Käesoleval ajal tähendab see, et päringu korral, saades IKS-is ettenähtud enda kohta käivad andmed, peab andmesubjekt hakkama hindama vastutava töötleja poolt saadud informatsiooni vastavust õigusaktidele. Jällegi tekib küsimus kuidas seda vastavust hinnata, kui põhimääruses on näiteks sätestatud, et andmeid võib kolmandatele isikutele edastada seadusest

[156] IKS, *supra* note 6, § 19.
[157] AvTS, *supra* note 3, § 43^5.

tulenevate ülesannete täitmiseks? Kahtlemata eeldab see andmesubjekti poolt laialdasi teadmisi valitsemiskorraldusest ja institutsioonidest.

Töö autor on seisukohal, et andmekogu pidamise kord tuleb AvTs-is selgesõnaliselt sätestada, see muudab läbipaistvamaks ka eesmärgipärasuse ja teiste õiguspärase töötlemise põhimõtete kontrollimise. Seega lisaks AvTs-is juba sätestatule tuleb selgesõnaliselt sätestada ka andmete saajad (kes saavad püsiva ligipääsu) koos neile edastatavate andmete koosseisude ja konkreetsete eesmärkidega ning kõik muud õiguspärase töötlemise aluseks olevad andmed (sh säilitustähtajad). Nimetatud nõuded on leitavad eelpool viidatud AKI poolt koostatud andmekogude soovituslikust juhendist.

Teine oluline küsimus on juurdepääs oma andmetele. Eelnevalt märgiti, et andmesubjektil on õigus IKS-is sätestatud asjaolude kohta teavet saada viie tööpäeva jooksul, pöördudes selleks vastutava töötleja poole. Oluline on märkida, et seadusandja on andmetele juurdepääsu käsitlevat paragrahvi selgitades rõhutanud, et isikuandmete töötleja peab arvestama, et andmetega tutvumine andmesubjekti jaoks toimuks tema võimalikult mugaval viisil ning oleks lihtne, viivituseta ja mõistlike kuludega.[158]

Töö autori hinnangul ei ole selline lahendus ilmselgelt andmesubjekti jaoks lihtne, viivituseta ja mõistlike kuludega[159]. Teabenõude korras sadadest andmekogudest[160] informatsiooni pärimine tähendaks andmesubjekti jaoks lakkamatut initsiatiivi osutamist. Samuti ei ole eluliselt usutav, et vastutavad töötlejad näiteks Siseministeerium, Majandus- ja Kommunikatsiooniministeerium, Justiitsministeerium, kelle vastutusel on igalühel kümneid andmekogusid,[161] oleksid viie tööpäeva jooksul valmis masspäringute korral vastama.

AvTs-i andmekogude regulatsioonis ei ole juurdepääsu küsimust käsitletud, viidatud on RIHA põhimäärusele ja RIHA menetlusele. Seega määrab IKS selles osas suuresti ka andmekogu disaini.

Töö autori hinnangul väärib kaasaegsete tehniliste lahenduste, eelkõige X-tee võimalustest lähtuvalt kaalumist IKS-i paragrahvi 19 muutmine andmesubjektile eelpool toodud andmetele juurdepääsu võimaldamiseks ilma vastutavat töötlejat täiendavalt koormamata ja andmesubjekti aega säästvalt (näiteks X-tee vahendusel). X-tee lahenduse kasutamine juurdepääsu võimaldamisel ei ole ka praegu mõistagi keelatud, kuid töö autori hinnangul väärib kaalumist sellise võimaluse

[158] Isikuandmete kaitse seaduse seletuskiri, *supra* note 75.
[159] Ibid.
[160] RIHA kodulehekülg, *supra* note 2.
[161] Ibid.

loomise kohustusena käsitlemine (antud töö mõistes andmekogude puhul). Võimalikke praktilisi lahendusi käsitletakse käesoleva töö teises peatükis.

Samuti võimaldaks andmesubjekti vaatest X-tee lahenduste kasutuselevõtt andmesubjekti osaluse realiseerimisel andmete kvaliteedi ja minimaalsuse põhimõtte kontrolli. AvTs-is on sätestatud, et andmete töötlemisel, mida kogub põhiandmetena teine riigi infosüsteemi kuuluv andmekogu, tuleb aluseks võtta vastava teise andmekogu põhiandmed.[162] Selline lähenemine tagab ühtlase andmekvaliteedi ja välistab andmete mitmetes andmekogudes üheaegse kogumise.

Lisaks eelnevale on andmesubjekti seisukohalt oluline, et tema andmed ei lekiks, oleks kaitstud hävimise jms eest. Turvalisuse põhimõtte tagamiseks pannakse vastutavale töötlejale kohustus rakendada ISKE meetmeid käideldavuse, konfidentsiaalsuse ja turvalisuse tagamiseks. Käideldavus puudutab andmekogu kättesaadavust, terviklus andmete volitamatut muutmist ja konfidentsiaalsus andmete volitamatut kasutamist.[163]

Eeltoodud meetmete ja seega ISKE määruse rakendamine on siiski praktikas ebaühtlane. Võtame näiteks Rahvastikuregistri, mille turbeastmeks on määratud H, ehk kõrge. Andmekogu sisaldab delikaatseid isikuandmeid. ISKE määruse[164] kohaselt kõrge turbeastmega andmekogu vastutav töötleja peab tellima sõltumatu auditi iga kahe aasta järel. Rahvastikuregistri kohta on aga ISKE kohta märge „rakendatud, auditeerimata“. Võttes arvesse, et auditeerimiskohustus on ISKE määruse alusel H turbeastmega andmekogude puhul juba alates 2010 aastast, oleks audit pidanud olema läbitud juba kolmel korral. Ridamisi näiteid auditeerimata andmekogudest võib veel tuua Sotsiaalministeeriumi vastutusel olevate andmekogude kohta, milles üldjuhul töödeldakse nii isikuandmeid kui delikaatseid isikuandmeid: Eesti HIV positiivsete patsientide andmekogu (mis ei ole lisaks ka RIHAs „kasutuselevõtu“ menetlust läbinud ja seega staatuses „asutamine sisestamisel“), Meditsiiniline sünniregister, milles töödeldakse vastsündinu ja tema vanemate, raseduse ja sünnituse kohta käivaid andmeid, Mürgistusteabe andmekogu, mille kohta on märge, et ISKE on rakendatud üle 25 protsendi, andmekogu on auditeerimata, Tuberkuloosiregister, milles ISKE on auditeerimata, Narkomaaniaravi andmekogu, milles ISKE rakendatud 25 protsenti, Vähiregister, milles ISKE samuti auditeerimata jne.[165]

[162] AvTS, *supra* note 3, § 43^6.
[163] IKS, *supra* note 6, § 25.
[164] Infosüsteemide turvameetmete süsteem, *supra* note 99, 9^1 lg 1.
[165] RIHA koduleheküg, *supra* note 2.

Probleemile, et ISKE auditeid ei viida läbi määrusele vastavalt on tähelepanu juhtinud ka AKI, sedastades, et ilma välise auditita ei ole võimalik asutuse juhil veenduda, et vajalikud andmekaitselised riskid oleksid maandatud. AKI teeb samuti ettepaneku, et kooskõlastamata ja auditeerimata andmekogud tuleks esiteks jätta ilma EL investeeringutest ja teiseks tuleb hakata neid süstemaatiliselt eemaldama X-teelt.[166] Näitena andmeturbe meetmete rakendamata jätmisest võib tuua AKI menetluse, mille käigus, 2012 aastal leiti Harku järve äärest hulk isikute terviseandmeid, sest perearst ei olnud rakendanud turvameetmeid andmekandjate säilitamisel[167].

Töö autori hinnangul ISKE rakendamine on andmesubjekti jaoks äärmiselt oluline, sisaldades tuhandeid turvameetmeid andmesubjekti andmete kaitseks, mistõttu tõhus kontroll vastutavate töötlejate üle on äärmiselt vajalik. Järgmises peatükis vaadeldakse tehnoloogilisi võimalusi selleks.

Töö autori hinnangul ISKE klassi määramine peab olema kohustuslik element andmekogude regulatsioonis. Samuti ei ole töö autori hinnangul põhjendatud andmesubjekti vaatest KOV-idele ja avalik – õiguslikele juriidilistele isikutele erisuste kehtestamine riigi infosüsteemi kindlustavate süsteemide määruse rakendamisel ja infoturbe juhi määramisel.

Eeltoodust tulenevalt teeb töö autor järgnevad ettepanekud:

AvTs § 43^5 sõnastust[168] peab täiendama, andmekogu põhimäärus, mis sisaldab isikuandmeid, peab lisaks seaduses nõutavale andmekogu vastutava töötleja, andmekoosseisu ja andmete andja määratlemisele sisaldama alljärgnevat:

- andmekogu pidamise üldist eesmärki;
- volitatud töötlejaid;
- ISKE osaklasse ja turbeastet;
- kogutavate andmekoosseisude loetelu, millest iga andmekoosseisu juures on määratud konkreetne eesmärk, milleks seda andmekoosseisu kogutakse, kes on selle

[166] Avaliku teabe seaduse a isikuandmete kaitse seaduse täitmisest aastal 2014, soovitused aastaks 2015, *supra* note 138, lk 13.
[167] Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2012, soovitused aastaks 2013, *supra* note 139, lk 76.
[168] § 43^5. Andmekogu põhimääruses sätestatakse andmekogu pidamise kord, sealhulgas andmekogu vastutav töötleja (haldaja), andmekogusse kogutavate andmete koosseis, andmeandjad ja vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused.

andmekoosseisu puhul andmeandja ja kes on õigustatud andmesaajad (püsiva juurdepääsu saajad);

- milline on iga konkreetse andmekoosseisu puhul andmete säilitustähtaeg ja milline on andmete hävitamise korraldus;
- millistel alustel on võimalik andmesubjektil andmeid parandada;
- mida logitakse ja kui kaua logiinformatsiooni säilitatakse;
- kuidas on võimalik andmesubjektil saada logiinfot enda kohta käivate andmete osas.

Kui rakendusakti ei peeta otstarbekaks kehtestada, peab vastav informatsioon olema sätestatud seaduse tasandil.

Olemasolevate andmekogude puhul anda rakendussätetega mõistlik aeg andmekogu regulatsiooni vastavusse viimiseks ülal toodud nõuetega.

Töö autor teeb lisaks ettepanekud sätestada konkreetsed kohustused KOV-idele ja avalik - õiguslikele juriidilistele isikutele turvalisuse põhimõtte tagamiseks isikuandmete töötlemisel.

Selleks tuleb täiendada järgnevaid õigusakte:

- Avaliku teabe seaduse § 43^9 lõiget 3 täiendada avalik õiguslike juriidiliste isikutega.
- Vabariigi Valitsuse 13.03.2012.a määrust „Infoturbe juhtimise süsteem“ täiendada kohustusega KOV-idele ja avalik – õiguslikele juriidilistele isikutele infoturbe juhi määramiseks;
- Vabariigi Valitsuse 20.12.2007.a määrust „Infosüsteemide turvameetmete süsteem“ täiendada ISKE rakendamise ja auditeerimiskohustusega avalikõiguslikele juriidilistele isikutele;
- Vabariigi Valitsuse 20.12.2007.a määrust „Infosüsteemide turvameetmete süsteem“ täiendada ISKE auditeerimiskohustusega KOV-idele.

ISKE rakendamise staatuse kontrollimiseks töö autor teeb ettepaneku täiendada Vabariigi Valitsuse 28.02.2008.a määrust „Riigi infosüsteemi haldussüsteem“[169] viisil, mis võimaldaks RIHA andmetele tuginedes tuvastada millal ISKE on viimati auditeeritud.

Töö autori hinnangul väärib kaasaegsete tehniliste lahenduste, eelkõige X-tee võimalustest lähtuvalt kaalumist IKS-i paragrahvi 19 muutmine. Kuna IKS nõuded määravad suuresti

[169] Riigi Infosüsteemi haldussüsteem, *supra* note 89.

andmekogude disaini, väärib kaalumist 5 tööpäevase tähtaja nõude lühendamine. Mõistetavalt ei pruugi olla tehniliselt võimalik sellist nõuet rakendada ilma ülemineku rakendussäteteta olemasolevate andmekogude puhul, kuid lühema tähtaja nõue oleks koheselt rakendatav uute arenduste elluviimisel.

2. Infotehnoloogilised võimalused andmesubjekti osaluse põhimõtte tagamisel

2.1. Siseriiklikud dokumendid andmesubjekti osaluse põhimõtte tagamisel e-lahenduste abil

Infoühiskonna arengukava 2020[170] käsitleb andmesubjektile tema isikuandmetele juurdepääsu võimaldamist meetmes paremate avalike teenuste arendamine info ja kommunikatsiooni tehnoloogia abil. Selle meetme 5.3.1. punkti b kohaselt luuakse riigi infosüsteemis andmesubjektile võimalused saada lihtsasti informatsiooni kellele on tema andmeid edastatud ning millal ning millistel eesmärkidel andmetöötlus on toimunud. [171]

Valitsuserakondade koalitsioonileppes käsitletakse samuti andmesubjektile tema andmetele juurdepääsu võimaldamist E-riigi meetmete all, punktis 4.20: „Andmete laialdase ristkasutuse taustal peame oluliseks kaitsta inimeste privaatsust, et igal ajahetkel oleks isikul võimalik näha, kes ja milleks tema kohta riigi käes olevaid andmeid kasutab“ [172].

Avalike teenuste korraldamise roheline raamat käsitleb andmesubjektile tema andmetele juurdepääsu teenuste kasutajamugavuse tagamise punkti all, selles rõhutatakse, et oluline on liikuda ühtse kontaktpunkti suunas, seda põhjusel, et klient soovib ühe kontakti vältel läbi viia kõik vajaminevad toimingud mitte otsida telefoninumbreid, asutusi, veebilehti ja muud informatsiooni, mille jaoks on tal vaja lisaaega panustada [173].

E-riigi hartas[174], mis on koostatud Riigikontrolli poolt ning on Riigikontrolli auditite hindamise aluseks, käsitletakse andmesubjekti osaluse põhimõtet laiemalt, see tähendab, et andmesubjekti jaoks ei piisa üksikutest aspektidest endaga seotud andmete kohta, nagu kes on andmetele juurdepääsu saanud, vaid oluline on näiteks ka see kas andmeid töödeldakse turvaliselt, kas eesmärgikohasuse ja kasutamise piiramise põhimõtteid järgitakse jne.

Jätkuks eelpool nimetatule võib pidada Majandus- ja Kommunikatsiooniministeeriumi poolt ettevalmistatud Määruse eelnõu (LISA 1). Selle paragrahvi 9 lõige 1 paneb asutusele kohustuse lisada oma avaliku teenuse kasutamise kohta teave teabeväravasse eesti.ee. Paragrahvis 12 lõikes

[170] Infoühiskonna arengukava 2020, *supra* note 9.
[171] Ibid.
[172] Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta, *supra* note 10, p 4.20.
[173] Avalike teenuste roheline raamat, *supra* note, 11, lk 17-18.
[174] E-riigi harta, *supra* note 12.

4 sätestatakse, et infosüsteemi väljatöötamisel või arendamisel tuleb luua tehnoloogilised ja organisatoorsed tingimused, et teenuse kasutamisel oleks võimalik tuvastada kes ja millal andmesubjekti andmeid infosüsteemis kasutanud on. Määruse andja on selgitanud, et asutus peab olema valmis vastama küsimustele millistel eesmärkidel on teabele juurdepääs võimaldatud (LISA 2).

Eeltoodust nähtub, et Infoühiskonna arengukava[175] ja valitsuserakondade koalitsioonilepe[176] sisaldavad andmesubjektiosaluse mitut aspekti. Esiteks võimalust oma andmetele juurdepääsu e-lahenduste abil, kuid oluline on märkida, et juurdepääsu võimaldamisele on antud sisu: juurdepääs tuleb võimaldada viivitamata ja kasutaja seisukohast lihtsasti. Lisaks peetakse E-riigi hartas[177] oluliseks andmesubjektile informatsiooni andmist ka teiste õiguspäraste töötlemise tingimuste kohta. Väärib märkimist, et käesoleval ajal on andmesubjektile tagatud IKS-ist tulenev võimalus oma andmetele juurdepääsuks viie tööpäeva jooksul, ilma eranditeta.

Määruse eelnõus aga käsitletakse andmesubjekti osaluse põhimõtet märksa kitsendatumalt kui infoühiskonna arengukava 2020[178] ja valituserakondade koalitsioonileping[179] seda ette näevad: andmesubjektile luuakse küll õigus saada teavet kes ja millal on tema andmetele juurde pääsenud, kuid selleks, et saada teavet, millistel eesmärkidel andmetöötlus toimub, peab ta eraldi pöörduma vastutava töötleja poole. Määrusega lihtsustatakse küll märkimisväärselt andmesubjektide juurdepääsuvõimalusi pannes kohustuseks teabe avaldamine eesti.ee teabevärava kaudu, samas eelpool käsitletud avalike teenuste rohelise raamatu käsitlust heast haldusest selline lähenemine ei kanna.

Avalike teenuste rohelises raamatus sedastatakse, et isik soovib ühe kontakti jooksul avaliku sektoriga võimalikult palju erinevaid küsimusi lahendada, mitte liikuda veebilehelt veebilehele, otsides telefoninumbreid ja orienteerudes osakondade ning vastutusalade rägastikus.[180] Lisaks ei ole sellise lahenduse korral tagatud teabe saamine muude õiguspärase töötlemise asjaolude kohta.

Seega siseriiklikes dokumentides, mis puudutavad e-lahendusi küll tähtsustatakse andmesubjekti osaluse põhimõtte realiseerimiseks sammude asutumist, kuid andmesubjekti osaluse põhimõte ei

[175] Infoühiskonna arengukava 2020, *supra* note 9.
[176] Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta, *supra* note 10, p.4.20.
[177] E-riigi harta, *supra* note 12.
[178] Ibid.
[179] Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta, *supra* note 10, p.4.20.
[180] Avalike teenuste roheline raamat, *supra* note 11, lk 17-18.

ole sisustatud ühetaoliselt ning Määruse eelnõu sisu on Infoühiskonna arengukavas 2020[181], koalitsioonileppes[182] ja Rohelises raamatus[183] kantud põhimõtetega kooskõlas vaid osaliselt. Samas on kõikides eelpool nimetatud dokumentides märgitud vajadust luua andmesubjektile võimalused oma andmetele juurdepääsuks lihtsalt, kiiresti ning andmesubjektile mõistetaval viisil.

2.1.1. X-tee andmekogude isikuandmete jälgimise rakendus „Suur vend“

Käesoleval ajal on võimalik oma isikuandmete töötlemist kontrollida rakenduse abil „Suur vend“ (edaspidi Rakendus)[184]. Rakendus on välja töötatud Majandus- ja Kommunikatsiooni ministeeriumi eestvõtmisel.

Rakenduse pilootprojektiga on 1.01.2016.a seisuga liitunud üksikud andmekogud: isikut tõendavate dokumentide register, digilugu ning karistusregister. Rakenduse abil on võimalik kontrollida millisele organisatsioonile andmesubjekti puudutavaid andmeid on edastatud. Eeltoodud Määrusega soovitakse Rakenduse kontseptsioon teha kohustuslikuks ka teistele andmekogudele.

Rakendus vastab Määruse eelnõus sätestatule, mille kohaselt andmekogu peab võimaldama saada teavet kes ja millal tema isikuandmeid infosüsteemis kasutab. Järgnevalt analüüsitakse Rakenduse vastavust andmesubjekti osaluse põhimõttele, mille kohaselt:

1) andmesubjekti andmeid võib töödelda seaduse alusel juhul, kui see on õigusaktides selgesti ette nähtud;
2) andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet milliseid andmeid tema kohta töödeldakse (v.a eelnevalt käsitletud piirangud);
3) andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet millistele kolmandatele isikutele on tema andmeid edastatud (v.a eelnevalt käsitletud piirangud);
4) andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet oma andmete töötlemise eesmärkide kohta (v.a eelnevalt käsitletud piirangud);
5) andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet oma andmete töötleja kohta;
6) andmesubjektil on õigus liigse viivituse ja kuludeta oma andmed töötlemiseks sulgeda, neid kustutada ja parandada kui andmeid ei töödelda Direktiivi põhimõtetega kooskõlas;

[181] Infoühiskonna arengukava 2020, *supra* note 9.
[182] Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta, *supra* note 10, p. 4.20.
[183] Avalike teenuste roheline raamat, *supra* note 11, lk 17-18.
[184] Projekti „Suur Vend“ tutvustus: https://www.x-road.eu/community/20150420/2_20150420_X-tee_suurVend_pirete.odp, (20.01.2016).

7) andmesubjektil on õigus liigse viivituse ja kuludeta saada teavet oma andmete töötlemise protsessi ja loogika kohta st eelnevalt käsitletud minimaalsuse, andmekvaliteedi, eesmärgikohasuse, seaduslikkuse, turvalisuse ja kasutuse piiramise kohta oma andmete töötlemisel.

Nimetatud põhimõtted on otseselt seotud õigusega saada informatsiooni oma andmete töötlemise asjaolude kohta, mis on osa andmesubjekti osaluse põhimõttest. Kui isikuandmete töötlemine ei ole kooskõlas nimetatud põhimõtetega, ei ole tegemist õiguspärase töötlemisega. Seega andmesubjekti osaluse põhimõtte täielikuks realiseerimiseks peab andmesubjektil olema võimalik kontrollida eeltoodud põhimõtete järgimist endaga seotud andmete töötlemisel. Nende põhimõtete kontekstis on tal võimalik hinnata andmetöötluse õiguspärasust ning esitada vastuväiteid oma andmete töötlemisele.

Lisaks peavad vastavalt eelnevas punktis käsitletud dokumentidele vastutavad töötlejad tagama, et eelnev info oleks andmesubjektile kättesaadav „igal ajahetkel“[185], „one stop shop“[186] põhimõttel.

Töö autori hinnangul Rakendus täidab punkti 2 nimetatud nõuet saada enda kohta informatsiooni, punkti 3, milles käsitletakse andmete edastamist kolmandatele isikutele ning punkti 5 informatsiooni andmete töötleja kohta.

Seaduslikkuse ja eesmärgi kohasuse põhimõtete kohaselt andmete töötlemine peab olema andmesubjekti jaoks õiglane ja seaduslik. Andmete töötlemise alusel peab olema selge seos kogutavate andmetega.[187] Lisaks peab andmesubjektil olema võimalik pöörduda andmete töötlemise sulgemiseks ja andmete parandamiseks järelevalve organi või vastutava töötleja poole.[188]

Töö autori hinnangul andmesubjekti osaluse põhimõtet ei täideta andmetöötluse seaduslikkuse ja töötlemise eesmärkide kohta. Andmesubjekt võib küll teatud juhtudel selle seose ise luua näiteks konkreetse menetluse raames, kuid Rakendus selle kohta automatiseeritult infot ei anna. Samuti peab oma andmete parandamiseks või sulgemiseks tegema eraldi pöördumise vastutava töötleja

[185] Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta, *supra* note 10, p 4.20.
[186] Avalike teenuste roheline raamat, *supra* note 11, lk 17-18.
[187] Punktid 1 ja 4.
[188] Punkt 6.

või järelevalveorgani poole, Rakendus ei paku näiteks targa vormi abil koostatud avalduse edastamist pädevale organile. Seega ei ole ka punkt 4 täidetud.

Seaduslikkuse ja eesmärgikohasuse kohta informatsiooni hankimiseks omal käel ja selle kohta hinnangu andmiseks peavad aga andmesubjektil endal olema laialdased teadmised valitsemiskorraldusest ja institutsioonidest. Kuid eelmises peatükis leidis kinnitust, et isegi laialdastest teadmistest ei pruugi abi olla, kuna volitusnormid ja põhimääruste nõuded on liialt üldised. Seega andmesubjektil oleks võimalik, saades Rakenduse abil juurdepääsu oma andmetele ja teadmise, kellele on tema andmeid edastatud, pöörduda eraldi vastutava töötleja poole saamaks teada millistel eesmärkidel teavet edastati. Rakendus ei paku lahendust näiteks olukorrale, kui andmesubjektil tekib kahtlusi kas andmetöötlus vastab eesmärkidele. Seda on võimalik teha andmesubjektil enesel, mis eeldab töö autori poolt eelnevas peatükis tehtud ettepaneku realiseerimist andmekogude regulatsiooni täiendamiseks.

Kasutuse piiramise ja andmete kvaliteedi põhimõtte kohaselt töötlemine ei pea olema üksnes seaduslik, vaid ka vajalik avalikes huvides või avalike ülesannete täitmiseks, andmeid kogutakse vaid selleks ettenähtud eesmärkidel, andmed peavad olema adekvaatsed.[189]

Töö autori hinnangul andmete kvaliteeti on Rakenduse abil vaid teatud ulatuses võimalik kontrollida. Kui andmesubjektil on juurdepääs oma andmetele, on võimalik ka tuvastada ebatäpsed andmed enda kohta, näiteks vale aadress. Kuid Rakendus ei aita hinnata, kas nende andmete kogumine on vajalik seatud eesmärgi jaoks. Seda on võimalik teha andmesubjektil enesel, mis eeldab töö autori poolt eelnevas peatükis tehtud ettepaneku realiseerimist andmekogude regulatsiooni täiendamiseks.

Kasutuse piiramise põhimõtte osas ei saa andmesubjekt samuti Rakendusele täies mahus toetuda, sest siin peab andma hinnangu kas muudel eesmärkidel andmete edastamine on konkreetses olukorras õiguspärane. Ühel eesmärgil kogutud andmeid ei saa hakata volitamatult mingitel teistel eesmärkidel kasutama asuda.[190] Kasutuse piiramise põhimõttele vastavust on võimalik hinnata andmesubjektil enesel, mis eeldab töö autori poolt eelnevas peatükis tehtud ettepaneku realiseerimist andmekogude regulatsiooni täiendamiseks.

[189] Punkt 7.
[190] Vt näiteks Vangla ekspressi näidet.

Minimaalsuse põhimõtte kohaselt andmed peavad olema piisavad ja asjakohased ja ei tohi ületada selle otstarbe piire, mille tarvis neid kogutakse.[191]

Minimaalsuse põhimõtte osas ei saa andmesubjekt samuti Rakendusele täies mahus toetuda, sest siin peab andma hinnangu kas andmete töötlemine on konkreetses olukorras õiguspärane. Seda on võimalik teha andmesubjektil enesel, mis eeldab töö autori poolt eelnevas peatükis tehtud ettepaneku realiseerimist andmekogude regulatsiooni täiendamiseks.

Turvalisuse põhimõtte kohaselt andmete töötleja peab rakendama infotehnoloogilisi ja organisatoorseid meetmeid isikuandmete kaotsi mineku ja hävimise vältimiseks, ebaseadusliku avalikustamise ning ebaseadusliku juurdepääsu võimaldamise eest ning käideldavuse tagamiseks.[192]

Turvalisuse põhimõtte rakendamist andmekogus on võimalik andmesubjektil Rakenduse abil teatud ulatuses kontrollida, näiteks kui andmesubjekt tuvastab, et tema uuringute tulemused on andmekogust digilugu kadunud, on tegemist tervikluse ja võib-olla ka konfidentsiaalsuse osaklassi puudutava intsidendiga. Samas ei ole võimalik Rakenduse abil saada informatsiooni kas ISKE on andmekogus rakendatud või mitte. ISKE rakendatust on võimalik andmesubjektil enesel kontrollida näiteks tuginedes RIHA andmetele. Samas eeldab ISKE asjaolude kontrollimine, töö autori poolt tehtud ettepaneku, et ISKE peab olema andmekogu alusakti kohustuslik element, realiseerumist. Lisaks ei võimalda Rakendus kontrollida teenustaseme parameetrite vastavust määratud käideldavuse osaklassile. Informatsiooni selle kohta on andmesubjektil enesel võimalik saada RIHA-st. Eelnevate asjaolude andmesubjekti poolt kontrollimine eeldab aga märkimisväärseid teadmisi, Rakendus selle kohta informatsiooni ei anna.

Kui andmesubjektil õnnestub omal käel tuvastada eelpool nimetatud õiguspärase töötlemise nõuete rikkumine, on tal võimalik pöörduda järelevalve organi või vastutava töötleja poole. Samas eeldab sellise õiguse realiseerimine samuti laialdasi teadmisi andmesubjekti jaoks. Kumbki võimalustest ei ole andmesubjekti jaoks lihtne ega aega säästev.

Seega Rakenduse abil on võimalik kontrollida vaid üksikuid aspekte õiguspärase töötlemise kohta ning see saab olla pigem juhuslikult avastatud. Lisaks jääb probleemiks andmekogude rohkus: Rakendus võimaldab saada informatsiooni korraga ühest andmekogust, selline lähenemine aga eeldab andmesubjektilt märkimisväärset ajakulu oma andmete kontrollimisel. Eelnevale lisandub

[191] Punkt 7.
[192] Analüüsitav Punkt 7.

eelpool käsitletud õiguspärase töötlemise aluspõhimõtetele hinnangu andmise ajakulu, mis eeldab andmesubjekti kõrget teadlikkust valitsemiskorraldusest ja institutsioonidest. Isegi juhul, kui andmesubjektil on piisavalt aega lakkamatult erinevates andmekogudes päringuid teostada ning piisavad teadmised seaduste ja põhimääruste abil volitamata töötlemise tuvastamiseks, eeldab andmesubjekti osaluse põhimõtte realiseerimine kompleksset lähenemist, mis tähendab, et töö autori poolt eelnevas peatükis käsitletud ettepanekud andmekogude regulatsiooni täiendamise osas (nt. andmete saajad-koosseisud-eesmärgid) peavad olema andmekogude regulatsioonis kajastatud.

Seega eelnevalt käsitletud tingimused saada informatsiooni ühest kohast ja kiiresti Rakenduse abil ei realiseeru. Rakenduse abil on võimalik kontrollida üksikuid andesubjekti osaluse põhimõtte aspekte.

2.2. Agendid

Tarkvaralisi lahendusi on teoreetikute poolt nimetatud Agentideks. Agendi mõistet kasutati esimest korda 1960 aastatel ning viimastel aastakümnetel on Agendi tehnoloogiat integreeritud edukalt erinevates valdkondades[193]. Kõige lihtsamaks näiteks Agendi näitlikustamisel on igapäevaselt kasutatavad otsingumootorid[194]. Agentide kasutuselevõtt kasvab kõige kiiremini e-kaubanduse valdkonnas. Mõnede autorite hinnangul lähitulevikus traditsioonilised veebi poed asenduvad Agendi põhiste lahendustega kus kasutajad saavad piirduda minimaalsete tegevustega.[195] Tarkvaraliste agentide kontseptsiooni on kasutatud näiteks müügitöös klientide soovide ennustamiseks[196], interneti kelmustega seoses[197], andmesubjektide kohta käiva informatsiooni eesmärgipärase kasutamise tagamisel[198], ettevõtte ümberorganiseerimise

[193] Serenko, A.; Detlor, Ę. B., *supra* note 7, lk 366.
[194] Cruquenaire, A. Electronic Agents as Search Engines: Copyright related aspects. International Journal of Law and Information Tehnology, Vol 9. lk. 328.
[195] Oren, J. S. T. Electronic Agents and the Notion of Establishment. International Journal of Law and Information Technology,Vol 9, No. 3, Oxford University Press, 2001, lk. 249-274; Gonzalo, S. A. Business Outlook regarding Electronic Agents. International Journal of Law and Information Technology, Vol. 9 No. 3, 2001, lk. 190-191.
[196] Gowda, R. S. Role of Software Agents in E-Commerce. International Journal of Computational Engineering Research, vol. 3, 2013, lk 246-251.
[197] Norta *et al.* My agent will not let me talk to the General. Software agents as a tool against Internet Scams. The Future of Law and eTechnologies. Springer 2016, lk 11-44.
[198] Rull *et al. supra* note 8, lk. 73-94.

korraldamisel[199], tervishoiu teenuse tõhustamisel[200], otsuste vastuvõtmise toetamisel[201] ning isegi õigusteaduses[202].

Tarkvaralise agendi tunnuseks on võimekus tegutseda autonoomselt, ta on toetatud teiste protsesside poolt[203]. Agent tegutseb volitatud isiku poolse pideva sekkumise ja suunisteta,[204] suudab reageerida iseseisvalt, monitoorida ümbritsevat iseseisvalt[205] ning teda iseloomustab koosvõimelisus teiste Agentidega.[206]

Agente on püütud ka kategoriseerida: Agendid, kes tegutsevad konkreetse kasutaja huvides, näiteks veebi juhised, Agendid, mille eesmärgid on üldisemad, näiteks veebi indekseerimine, telefoniside võrgu koormuste jaotamine, [207] töövoogude agendid, mis automatiseeritult teostavad erinevaid ülesandeid, maakler agendid, mis vahendavad ostjate-müüjate vahelisi pakkumisi.[208]

Näiteks võib tuua Agendi, mis nõustab andmesubjekti Interneti vahendusel kaupade ostmisel. Agent võtab arvesse kasutaja käitumuslikke eelistusi, analüüsib erinevate veebilehtede privaatsuspoliitikaid, teiste kasutajate varasemad hinnanguid teatud veebilehtede kohta ning nõustab kasutajat vastavalt.[209]

Taveter ja Sterling sisutavad Agendile esitatavad nõuded läbi kaasaegse ühiskonna vajaduste. Kaasaegses ühiskonnas Agent peab vastama alljärgnevatele tingimustele:

- olema suuteline kohanema ja reageerima võimalike uutele tingimustele ja muutustele;
- olema intelligentne, see tähendab võimekust lahendada keerulisi ülesandeid iseseisvalt;
- olema suuteline tegutsema kiiresti, efektiivselt ja sihipäraselt.

[199] McCarty, L. T. Reflections on TAXMAN: An experiment in artificial intelligence and legal reasoning. Harward Law Review, 90(5), 1977, lk 837-893.
[200]Smith *et al.* Evaluation of inherent performance of intelligent medical decision support systems: utilising neural networks as an example. Artifical Intelligent in Medicine, 2003, vol. 27, lk. 1–27.
[201] Carlsson, C. Decision Support in virtuaal Organizations: The case for Multi-Agent Support. Kluwer Academic Publishers, 2002. lk 185-221.
[202] Sartor G.; Branting L. K. Introduction: judicial applications of artificial intelligence. Artificial Intelligence and Law: 6, 1998, lk. 105–110.
[203] Bygrave, L. A. Electronic Agents and Privacy: A Cyberspace Odyssey. International Journal of Law and lnformation Technology, Vol.9 No. 3 Oxford University Press, 2001, lk. 278-279.
[204] Ibid.
[205] Serenko, A.; Detlor, Ę. B., *supra* note 7, lk. 366.
[206] Bygrave (2001), *supra* note 203, lk. 278-279.
[207] Serenko, A.; Detlor, Ę. B., *supra* note 7, lk. 367-368.
[208] Bygrave, (2001), *supra* note 203, lk. 277.
[209] Lee, H. H.; Stamp, M. An agent based privacy-enhancing model. Information Management & Computer Security, Vol.16(3), 2008, lk 305-306.

- olema lihtsasti mõistetav.[210]

Norta *et al.* pakuvad välja lahenduse, mida on võimalik kasutada Interneti suhtlusel pettuste tuvastamisel. Nad väidavad, et on võimalik välja tuua teatud tüüpilised käitumismustrid Interneti suhtlusel, mis peaks andmesubjektis kahtlusi äratama. Agent saabki nende elementide abil andmesubjektile hoiatavaid signaale edastada.[211] Näiteks andmesubjekti vestluspartner väidab end olevat sünnipärane Ameerika Ühendriikide kodanik, kuid tema halval tasemel inglise keel viitab, et tegemist ei saa olla sünnipärase Ameerika kodanikuga. Vestluspartner soovib laenata raha lubadusega see tulevikus kindlasti tasuda, IP aadress ei vasta asukohale, kus isik tegelikult väidab end viibivat, liiga üldised või ebaloogilised andmed vestluspartneri poolt. Agent saab eelneva põhjal anda andmesubjektile hoiatavaid signaale.[212]

Rull *et al.* käsitlevad Agendi teooria näitel infosüsteemi KAIRI. KAIRI on osa POLIS-e infosüsteemist ja selles töödeldakse muuhulgas delikaatseid isikuandmeid. Probleemiks on infosüsteemi KAIRI mitte eesmärgipärane kasutamine politseiametnike poolt. Näiteks võib politseiametnik võtta KAIRI-s olevaid asjaolusid arvesse mingi uue juhtumi asjaolusid kaaludes, mis ei pruugi andmesubjekti jaoks tähendada õiglast lahendit. Lisaks on leidnud kinnitust KAIRI kasutamine politseiametnike poolt isiklikel eesmärkidel. Süsteemile on ligipääs ca 5000 ametnikul, nende ligipääsud on määratletud ja süsteem kogub logiinformatsiooni, kuid ei analüüsi näiteks kas konkreetsel ametnikul konkreetses asjas oli/on vajalik mingit andmekoosseisu töödelda. KAIRI puhul uuritigi kas on võimalik Agendi teooriat aluseks võttes lahendada KAIRI volitamata kasutamise probleemi. Autorid peavad samuti võimalikuks sensortehnoloogia kasutamist: näiteks kui sensortehnoloogia tuvastab politseiametnikul mingi terviseprobleemi, piirab Agent politseiametniku juurdepääsu KAIRi-le ja suunab ta tervisekontrolli, informeerides samal ajal teenistuja vahetut juhti.[213] Rolli mudelis on määratletud õigused, kompetentsid, juurdepääsuõigused jne, mis võimaldab piirata vajadusel teenistuja juurdepääsu ning reageerida kui teenistuja ülesanded, näiteks ametijuhend on muutunud.[214]

Seega andmesubjekti vaatest ja vastavalt eelnevalt käsitletule oluline on pakkuda rakendust, mis oleks kiire, efektiivne, intelligentne ja mõistetav andmesubjekti jaoks. Arvestades, et Eestis on andmekogusid arvult sadades, peab rakendus olema suuteline andmesubjekti vaatest nö. ühe

[210] Sterling, L. S.; Taveter, K. The Art of Agent-Oriented Modeling. The MIT Press, Cambridge, 2009, lk. 5-6.
[211] Norta *et al. supra* note 197.
[212] Ibid, lk 18-21.
[213] Rull *et al. supra* note 8, lk. 77-82 ja 85.
[214] Rull *et al. supra* note 8, lk. 89-92.

klikiga hankima ja analüüsima võimalikult palju informatsiooni, teostama andmesubjekti volitusel teatud toiminguid, näiteks saatma teavitusi järelevalveasutusele ning informeerima vajadusel andmesubjekti. Siit järeldub, et tarkvaraline lahendus ei saa tugineda üksnes ühele allikale nagu eelnevalt käsitletud Rakendus seda teeb, allikaid peab olema mitmeid. Lisaks on tarkvaralise lahenduse rakendamise eelduseks, et andmesubjekt saab ise määrata, kas ta soovib saada informatsiooni kõikide X-teel olevate andmekogude kohta või ainult üksikute kohta, andmesubjektil peab olema võimalus sisestada teatud andmekoosseise, mis on tema jaoks olulised, et need oleksid igas andmekogus õiged, nt elukoha andmed. Tal peab olema võimalik valida teavituste kriteeriume ja võimalus volitada enda nimel pöörduma järelevalve asutuse või vastutava töötleja poole.

Eelnevas peatükis järeldati, et määrava tähtsusega andmesubjekti õiguste kaitsel on RIHA menetluste läbimine, selge seaduslik alus andmete töötlemisel, täpsustatud nõuded põhimäärustele ja ISKE rakendamine ning auditeerimine jne. Seega peab Agendil olema võimekus kõiki neid asjaolusid kontrollida. Samuti järeldati, et õiguspärase töötlemise põhimõtteid on võimalik kontrollida nii RIHA kui ka X-tee vahendusel. Töö autori poolt eelmises peatükis tehtud ettepanekute realiseerumisel on õiguspärase töötlemise põhimõtteid võimalik kontrollida järgnevate allikate toel:

- Seaduslikkuse põhimõtet on võimalik kontrollida eRT vahendusel.
- ISKE rakendatust ja auditeerimise staatust RIHA vahendusel.
- Töötlemise eesmärgi seose kohta konkreetse töötlejaga on võimalik saada eRT-ist.
- Oma andmete töötleja ja juurdepääsude kohta konkreetsetele andmekoosseisudele on võimalik saada X-tee vahendusel.
- Kasutuse piiramise, minimaalsuse, andmekvaliteedi ja turvalisuse põhimõtteid on samuti võimalik kontrollida automatiseeritult X-tee, eRT ja RIHA koostoimes.
- Andmekogu staatuse kontroll (nt. „kasutusel“, „asutamine kooskõlastatud“ vms) RIHA vahendusel.
- Delikaatsete isikuandmete töötlemise puhul vastutava töötleja olemasolu vastavas registris, mida saab kontrollida isikuandmete töötlejate ja isikuandmete töötlemise eest vastutavate isikute registri vahendusel (edaspidi DIAT register).

Seega on tegelikkuses mitmeid allikaid mis võimaldavad saada ja analüüsida märkimisväärselt enam informatsiooni kui Rakendus seda käesoleval ajal teeb. Kui neid allikaid oleks andmesubjektil oma andmete töötlemise õiguspärasuse hindamisel võimalik kasutada viisil, mis

oleks lihtne ja kiire, ning see haaraks kõiki käesoleva töö mõistes andmekogusid, tagaks see andmesubjekti märkimisväärselt parema informeerituse ja õiguskaitse. Veelgi tõhusam oleks andmesubjekti jaoks oma andmete õiguspärase töötlemise kontrollimine volitada näiteks tarkvaralisele lahendusele, mis tegutseb pidevalt ja annab andmesubjektile tagasisidet.

2.2.1. Agendi rakendamise võimalikkus andmesubjekti osaluse põhimõtte tagamisel

Järgnevalt analüüsitakse Agentide rakendamise võimalikkust andmesubjekti osaluse põhimõtte realiseerimisel andmekogudes vastavalt andmesubjekti osaluse põhimõttele.[215]

Järgnevate ettepanekute realiseerimine eeldab töö autori poolt eelnevas peatükis tehtud ettepanekute realiseerumist, mis puudutab kehtivat andmekogude regulatsiooni täiendamist ja põhjalikuma nõuete analüüsi läbiviimist.

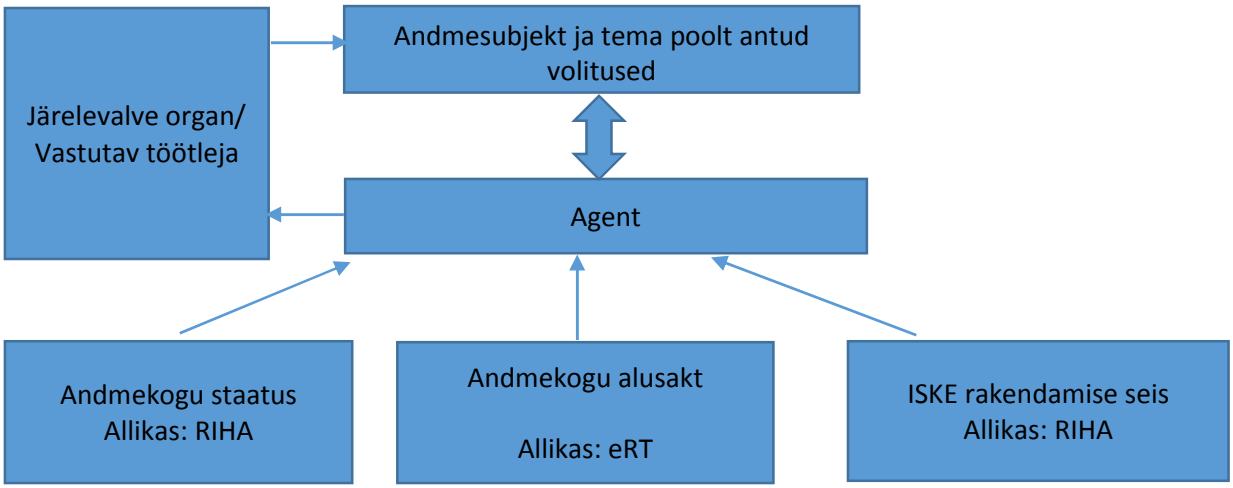
Esmaselt, enne seadusliku töötlemise aluspõhimõtete kontrollima asumist peab Agent kontrollima kas:

- andmekogu on RIHA-s kõik menetlusetapid läbinud ja staatuses „kasutusel“;
- andmekogu õigusakt on kehtiv (eRt vahendusel);
- RIHA-s kooskõlastatud õigusakt on vastavuses eRT-is olevaga;
- ISKE rakendamise seis on „rakendatud, auditeeritud märkuste ja/või soovitustega“, „rakendatud, auditeeritud märkuste ja soovitusteta“.

Kui toiming lõpeb põhjusel, et RIHA menetlus ei ole läbitud, puudub õigusakt või on ISKE rakendamata/auditeerimata, peab Agendil olema volitus pöörduda omal initsiatiivil, näiteks targa vormi abil, mille sisu koostatakse automaatselt, vastutava töötleja või järelevalveasutuse poole, teavitades sellest samaaegselt andmesubjekti. Informatsiooni, millise institutsiooni poole pöörduda saab Agent eRT abil IKS-ist (vt. Joonis 2).

Metatasandi kontrollil on kaks tulemust: 1. Metatasandil nõutavad õiguspärase töötlemise tingimused on täidetud, liikuda edasi seaduslikkuse ja eesmärgikohasuse hindamise juurde. 2. Metatasandil nõutavad õiguspärase töötlemise tingimused ei ole täidetud, liikuda edasi automatiseeritud teavituse/avalduse/pöördumise koostamise juurde järelevalveasutusele/vastutavale töötlejale ning teavitada õiguspärase töötlemise nõuete rikkumisest andmesubjekti.

[215] Vt loetelu käesoleva töö lk. 43-44.



Joonis 2. Õiguspärase töötlemise kontroll metatasandil.

Kui kõik eelpool nimetatud tingimused on täidetud, kontrollib Agent seaduslikkuse ja eesmärgikohasuse põhimõtetele vastavust.

Seaduslikkuse ja eesmärgi kohasuse põhimõtete kohaselt andmete töötlemine peab olema andmesubjekti jaoks õiglane ja seaduslik. Andmete töötlemise alusel peab olema selge seos kogutavate andmetega.

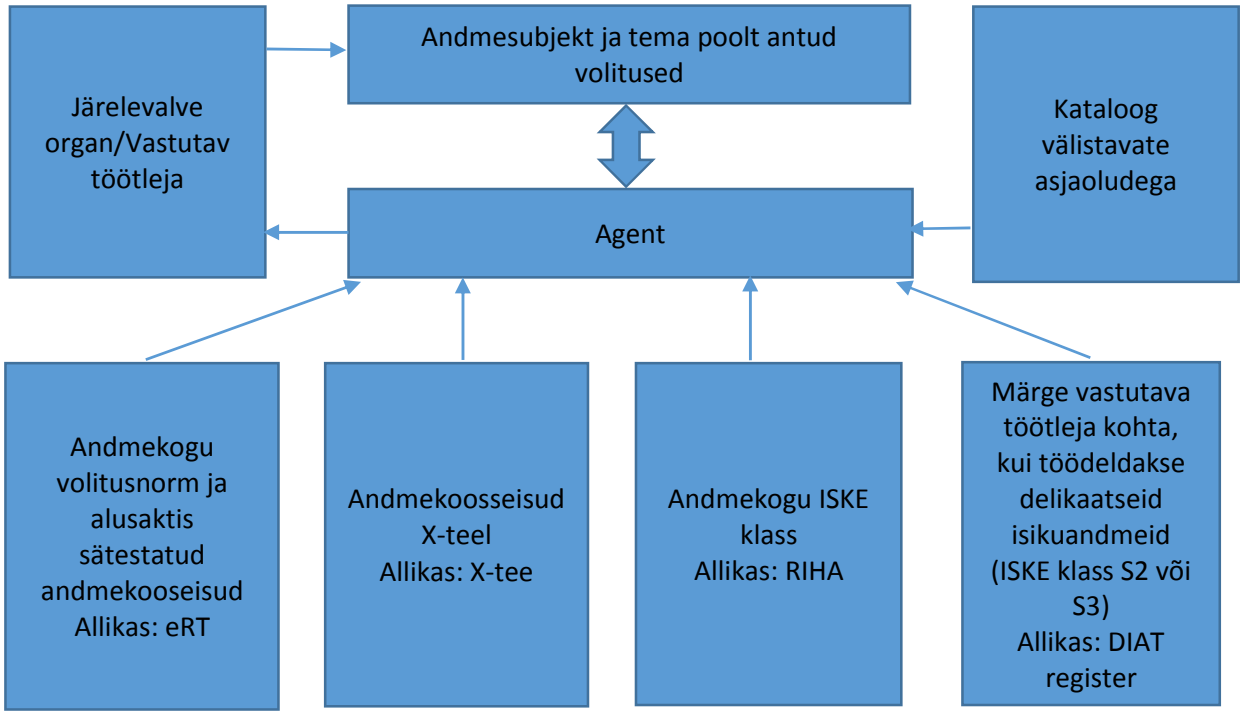
Seaduslikkuse ja eesmärgikohasuse põhimõtete vastavuse kontrolli läbiviimiseks on Agendil vaja analüüsida volitusnormi ennast vastavuses andmekoosseisuga. Võtame näiteks käesolevas töös käsitletud isikustatud andmete kogumise puugihammustuste kohta terrorismivastase võitluse eesmärgil. Puugihammustuste kohta info kogumine on eelkõige seotud rahvatervise kaitsmise eesmärgiga. Terrorismivastane võitlus on aga seotud riigi julgeoleku küsimusega. Agendile peaks olema selline informatsioon alarmeeriv. Kahtlemata eeldab selline analüüs Agendi jaoks kataloogi olemasolu välistavatest asjaoludest. Kataloogi loomist, milles on teatud üldistatud elemendid, on oma töös kasutanud samuti Norta *et al*. [216] Interneti suhtlusel võimalike petuskeemide tuvastamisel.

Lisaks kontrollib Agent ISKE konfidentsiaalsuse osaklassi, kui andmekogu ISKE osaklass on S2 või S3 ning andmekoosseisust nähtub, et toimub delikaatsete isikuandmete töötlemine, peab vastutav töötleja olema registreeritud DIAT registris.

[216] Norta *et al. supra* note 197.

Kui toiming lõpeb põhjusel, et Agendi jaoks on alarmeeriv andmekoosseisu kogumine ja selle seos eesmärgiga või vastutava töötleja puudumine DIAT registrist, peab Agendil olema volitus pöörduda targa vormi abil, mille sisu koostatakse automaatselt, vastutava töötleja või järelevalveasutuse poole teavitades sellest samaaegselt andmesubjekti. Informatsiooni, millise institutsiooni poole pöörduda, saab Agent eRT abil IKS-ist.

Seega seaduslikkuse ja eesmärgikohasuse kontrollil on kaks tulemust: 1. Volitusnormil ja kogutavatel andmekoosseisudel on loogiline ja õiguslik seos, delikaatsete isikuandmete töötlemise puhul vastutav töötleja on kantud DIAT registrisse, seega seaduslikkuse ja eesmärgikohasuse tingimused on täidetud, liikuda edasi kasutuse piiramise ja andmekvaliteedi põhimõtte hindamise juurde. 2. Seaduslikkuse ja/või eesmärgikohasuse töötlemise tingimused ei ole täidetud, liikuda edasi automatiseeritud teavituse/avalduse/pöördumise koostamise juurde järelevalveasutusele/vastutavale töötlejale ning teavitada õiguspärase töötlemise nõuete rikkumisest andmesubjekti (vt Joonis 3).



Joonis 3. Seaduslikkuse ja eesmärgipärasuse tagamise kontroll.

Kasutuse piiramise ja andmete kvaliteedi põhimõtte kohaselt töötlemine ei pea olema üksnes seaduslik, vaid ka vajalik avalikes huvides või avalike ülesannete täitmiseks, andmeid tuleb koguda ja kasutada vaid selleks ettenähtud eesmärkidel ja andmed peavad olema adekvaatsed.

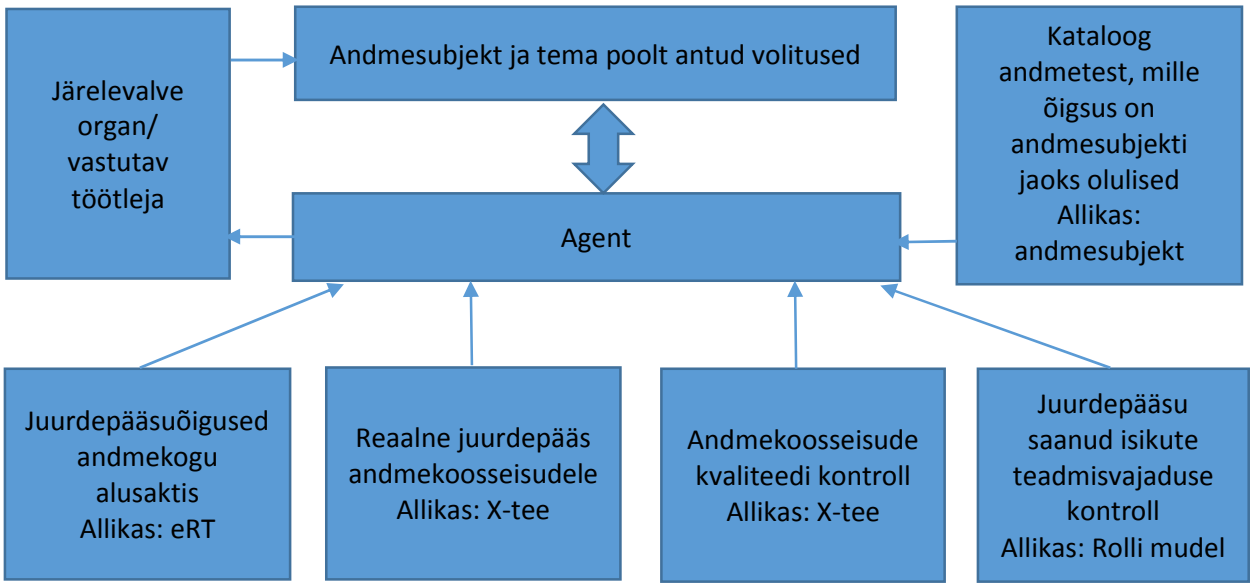
Kasutuse piiramise analüüsimiseks peab Agent analüüsima õigusakti vastavust sellega, millistel eesmärkidel andmeid kasutatakse. Näiteks kui Agent tuvastab, et teatud andmekoosseise, mida on küll lubatud töödelda, töödeldakse lisaks muudel eesmärkidel, peab Agent suutma sellise lubatavuse aluse õigusaktist leida ja seda analüüsima. Seejuures peab Agent õigusaktist lähtuvalt hindama kas kolmandad isikud, kellele juurdepääs on võimaldatud, on õigustatud teavet saama. Agent saab õiguspärast juurdepääsu kontrollida andmekogu alusaktis olevate juurdepääsuõiguste võrdlemisel reaalselt X-teel töödeldavate andmetega. Keeruline on kontrollida, kas isikul, kes juurdepääsu saab, on reaalne teadmisvajadus teatud menetluse kontekstis või mitte, sest see on tugevalt seotud organisatsiooni, kes andmeid töötleb, sisemise tegevusega.

Rull *et al.* pakuvad andmekogu väärkasutamiste vältimiseks välja kontseptsiooni koos rolli mudeliga, mis tagab, et andmekoosseisudele saavad organisatsioonis juurdepääsu õigustatud isikud ning, et õigustatud isikud kasutavad andmekoosseise eesmärgipäraselt (edaspidi Rolli mudel).[217] Kasutuse piiramise kontrolli üks osa peab olema ka Rolli mudel.

Andmete kvaliteeti on võimalik Agendil kontrollida vastavuses andmete kategooriatega, näiteks kui isiku aadressandmed on erinevates andmekogudes erinevad, teavitab Agent sellest andmesubjekti. Siin peab olema andmesubjektil samuti võimalik minimaalsete tegevustega piirduda: sisestanud Agendile aadressi, mida andmesubjekt peab õigeks, Agent kontrollib RIHA vahendusel millise andmekogu põhiandmetega on tegemist ja edastab vastava automatiseeritud targa vormi abil teavituse vastava andmekogu vastutavale töötlejale andmete parandamiseks.

Seega kasutuse piiramise ja andmekvaliteedi kontrollil on kaks tulemust: 1. Juurdepääsuõigused on antud õiguspäraselt ja teadmisvajaduse põhimõtet arvestavalt, andmed on kvaliteetsed ja ühetaolised, liikuda edasi minimaalsuse põhimõtte hindamise juurde. 2. Kasutuse piiramise ja/ või andmekvaliteedi tingimused ei ole täidetud, liikuda edasi automatiseeritud teavituse/avalduse/pöördumise koostamise juurde järelevalveasutusele/vastutavale töötlejale ning teavitada õiguspärase töötlemise nõuete rikkumisest andmesubjekti (vt Joonis 4).

[217] Rull *et al. supra* note 8, lk. 89-92.

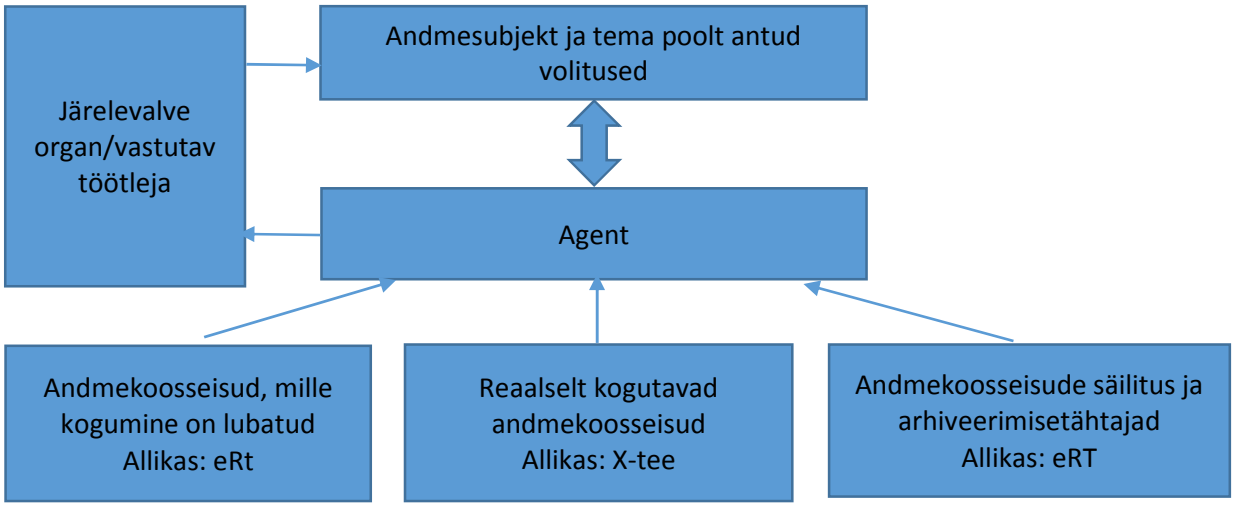


Joonis 4. Kasutuse piiramise ja andmekvaliteedi tagamise kontroll.

Minimaalsuse põhimõtte kohaselt andmed peavad olema piisavad ja asjakohased ja ei tohi ületada selle otstarbe piire, mille tarvis neid kogutakse.

Minimaalsuse põhimõtet on võimalik Agendil kontrollida õigusaktis olevate lubatavate andmekoosseisude võrdlemisel reaalselt kogutava informatsiooniga. Näiteks kui politsei andmekogusse sisestatakse lisaks rikkumistele veel informatsiooni mingite muude asjaolude kohta isiku suhtes, peab see olema alarmeeriv Agendi jaoks. Lisaks peab Agent võrdlema töödeldavat informatsiooni andmete säilitus ja arhiveerimis tähtaegadega. Kui andmed peaks olema õigusakti kohaselt hävitatud või arhiveeritud, ei saa need enam aktiivses kasutuses olla. Seega peab Agent omama teavet millal andmeobjekti esmakordselt töötlema asuti ning milline on andmeobjekti säilitustähtaeg. Kui näiteks andmekogus digilugu on aktiivses töötluses andmed, mis peaks olema arhiveeritud või kustutatud, peab Agent edastama sellekohase automatiseeritud teavituse vastutavale töötlejale ja andmesubjektile.

Seega minimaalsuse kontrollil on kaks tulemust: 1. Andmekoosseise kogutakse ulatuses, mis on määratud andmekogu alusaktis, andmed on säilitatud/arhiveeritud/kustutatud vastavalt andmekogu alusaktis kehtestatud tähtaegadele, liikuda edasi turvalisuse põhimõtte hindamise juurde. 2. Minimaalsuse põhimõtte tingimused ei ole täidetud, liikuda edasi automatiseeritud teavituse/avalduse/pöördumise koostamise juurde järelevalveasutusele/vastutavale töötlejale ning teavitada õiguspärase töötlemise nõuete rikkumisest andmesubjekti (vt Joonis 5).



Joonis 5. Minimaalsuse põhimõtte tagamise kontroll.

Turvalisuse põhimõtte kohaselt andmete töötleja peab rakendama infotehnoloogilisi ja organisatoorseid meetmeid isikuandmete kaotsi mineku ja hävimise vältimiseks, ebaseadusliku avalikustamise ning ebaseadusliku juurdepääsu võimaldamise eest ning käideldavuse tagamiseks.

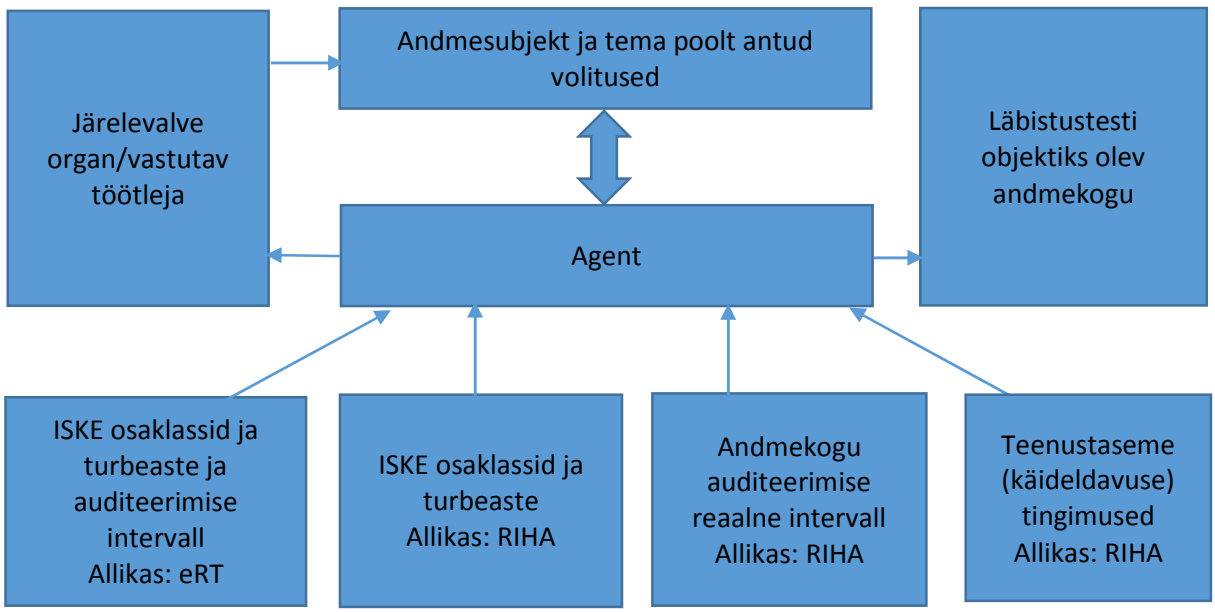
Agendi jaoks saab selle info analüüsimisel esmaseks allikaks olla RIHA, mille vahendusel on võimalik saada infot ISKE staatuse ja rakendatuse kohta. ISKE on samuti metatasandi kontrolli objektiks. Kui esmaselt kontrollitakse kas andmekogu puhul ISKE on rakendatud ja auditeeritud, siis käesolevas etapis peab Agent kontrollima ISKE osaklasside ja turbeastme vastavust õigusaktis oleva ja RIHA-s märgitu vahel. Eelnev eeldab, et töö autori poolt tehtud ettepanek sätestada ISKE osaklasside ja turbeastme määramine õigusaktis kohustusena oleks realiseeritud. Teiseks peab Agent kontrollima vastavust andmekogu turbeastme ja auditeerimise intervalli vahel. Turbeastme kontrolli osas on aluseks andmekogu alusakt ja eelnevas peatükis käsitletud infosüsteemide turvameetmete süsteemi määrus, mis on aluseks auditeerimise intervalli määramisel. Näiteks kõrge turbeastme puhul on intervalliks kaks aastat, keskmise puhul 3 aastat. Kui RIHA-s on informatsioon, et auditeeritud on kõrge turbeastmega andmekogu näiteks kuus aastat tagasi, ei ole see õiguspärane töötlemine. Käesoleval ajal RIHA-st saab informatsiooni ainult rakendamise seisu koht, mitte aga auditeerimise intervalli kohta. Seega sellise informatsiooni saamiseks peab realiseeruma töö autori poolt eelnevas peatükis tehtud ettepanek RIHA põhimääruse täiendamiseks viisil, mis võimaldaks RIHA vahendusel tuvastada millal ISKE on viimati auditeeritud.

Lisaks peab Agent suutma kontrollida andmekogu käideldavuse, tervikluse ja konfidentsiaalsuse aspektist. Üheks võimaluseks käideldavuse, tervikluse ja konfidentsiaalsuse tagamise tuvastamisel on, et Agent teeb regulaarseid läbistusteste andmekogude vastu, milles andmesubjekti andmeid

töödeldakse. Täiendavat uurimist vajab kuidas Agendi poolset läbistustestide läbiviimist õiguslikult reguleerida.

Esmatasandil on võimalik käideldavuse nõudeid kontrollida RIHA andmetele tuginedes. Näiteks kui ISKE käideldavuse osaklass on K2, andmekogu ühekordse planeeritud/planeerimata katkestuse pikkus saab olla 24/7 süsteemi puhul 2 tundi. Mida lühem on andmekogu tööaeg, seda lühem saab olla ka katkestuse pikkus K2 puhul. Seega kui andmekogule on määratud käideldavuse osaklassiks K2 ja tegemist on tööajaga 24/7 andmekoguga, kuid RIHA andmete kohaselt võib andmekogu planeeritud või planeerimata katkestuse aeg olla 8 tundi, ei ole reaalsus määratud ISKE osaklassiga vastavuses.

Seega turvalisuse kontrollil on kaks tulemust: 1. Andmekogu alusaktis määratud ISKE osaklassid ja turbeaste on vastavuses RIHA-s kirjeldatud ISKE klassiga, ISKE reaalne auditeerimise intervall on vastavuses määratud turbeastmega, andmekogule on määratud käideldavuse nõuded ja need vastavad määratud ISKE osaklassile ning läbistustest ei tuvasta tervikluse ja konfidentsiaalsuse kadu. 2. Andmekogu alusaktis määratud ISKE osaklassid ja turbeaste ei ole vastavuses RIHA-s kirjeldatud ISKE klassiga, ISKE reaalne auditeerimise intervall ei ole vastavuses määratud turbeastmega, andmekogule määratud käideldavuse nõuded ei vasta määratud ISKE osaklassile, läbistustest tuvastas tervikluse ja konfidentsiaalsuse kao, liikuda edasi automatiseeritud teavituse/avalduse/pöördumise koostamise juurde järelevalveasutusele/vastutavale töötlejale ning teavitada õiguspärase töötlemise nõuete rikkumisest andmesubjekti (vt Joonis 6).



Joonis 6. Turvalisuse põhimõtte tagamise kontroll.

Analüüsi käigus selgus, et lisaks eeltoodud allikatele eeldab seaduslikkuse ja eesmärgi kohasuse põhimõtte kontroll kataloogi loomist välistavatest asjaoludest, mis aitavad hinnata kas andmekasutus on seaduslikkuse ja eesmärgikohasuse põhimõtetega kooskõlas. Kataloogi loomist, milles on teatud üldistatud elemendid, on oma töös kasutanud samuti Norta *et al*. [218] Interneti suhtlusel võimalike petuskeemide tuvastamisel.

Lisaks selgus, et kasutuse piiramise analüüsimiseks ei piisa eelpool nimetatud allikatest, see tähendab, et keeruline on kontrollida, kas isikul, kes juurdepääsu saab, on reaalne teadmisvajadus teatud menetluse kontekstis või mitte, sest see on tugevalt seotud organisatsiooni, kes andmeid töötleb, sisemise tegevusega. Selle probleemi lahendamiseks töö autori hinnangul on võimalik kasutada Rull *et all.* poolt pakutud Rolli mudelit, mis tagab, et andmekoosseisudele saavad organisatsioonis juurdepääsu õigustatud isikud ning, et õigustatud isikud kasutavad andmekoosseise eesmärgipäraselt.[219]

Turvalisuse põhimõtte tagamiseks ei piisa samuti vaid eelpool nimetatud allikatest, kuigi esmatasandil on võimalik käideldavuse nõudeid kontrollida RIHA andmetele tuginedes. Agent peab suutma lisaks kontrollida andmekogu andmekasutust tervikluse ja konfidentsiaalsuse aspektist. Selleks Agent peab tegema regulaarseid läbistusteste andmekogude vastu, milles andmesubjekti andmeid töödeldakse. Täiendavat uurimist vajab kuidas Agendi poolt läbiviidavaid läbistusteste õiguslikult reguleerida.

Seega Agendi abil on võimalik kontrollida õiguspärase töötlemise põhimõtteid märkimisäärselt laiemas ulatuses kui Rakendus seda võimaldab. Andmesubjekti jaoks tähendab Agendi rakendamine, et õiguspärase töötlemise põhimõtteid on võimalik kontrollida automatiseeritult, andmesubjektil ei ole vajadust oma õiguste kaitsmise eesmärgil teostada lakkamatut otsinguid sadade andmekogude vastu, tal on võimalik piirduda minimaalsete toimingutega. Samuti ei eelda Agendi rakendamine andmesubjektilt laialdasi teadmisi andmekogude regulatsioonist, järelevalve pädevustest ega valitsemiskorraldusest, Agent korraldab iseseisvalt vajamineva analüüsi ja teavitused.

[218] Norta *et al. supra* note 197.
[219] Rull *et al. supra* note 8, lk. 89 -92.

Kokkuvõte

Käesoleval ajal on isikuandmete kaitse sätestatud põhiõigusena. Samas avalike teenuste pakkumine toimub üha enam infotehnoloogia vahendusel, mis võimaldab andmeid lihtsasti suures mahus töödelda. Valdav osa andmekogudest sisaldavad isikuandmeid ja delikaatseid isikuandmeid. Andmevahetuseks kasutatakse laialdaselt X-teed, mis aitab vahendada andmekogude vahel iga päev tuhandeid andmeid.

Samas andmekogude väärkäitlemise juhtumeid on arvukalt ja need on leidnud käsitlemist meedias, eriala kirjanduses ja AKI ülevaadetes. Kui muudel juhtudel isikul on võimalik oma nõusolekust isikuandmete töötlemisel taganeda, siis seaduse alusel töötlemisel on isik, kelle andmeid töödeldakse, täielikult vastutava töötleja meelevallas. Eelnevale lisandub laia kõlapinda leidnud avaandmete kontseptsiooni realiseerumine, mis tähendab, et üha enam hakatakse avaliku sektori poolt kogutavaid andmeid kasutama viisil, mis loob isikuandmete töötlemisel täiendavaid ohte. Seetõttu on äärmiselt oluline, et seaduse alusel töötlemisel oleks õiguspärane töötlemine tagatud. Andmesubjekti seisukohalt oluline, et andmevahetus oleks selgesti reguleeritud. Selge regulatsioon võimaldab andmesubjektil hinnata kas andmete töötlemine on õiguspärane või mitte.

Käesoleval ajal on vaid üksikutes andmekogudes olemas funktsionaalsus, mis võimaldab andmesubjektil ennast autentides saada informatsiooni endaga seotud andmete kohta ja kellele neid andmeid on edastatud. Samas ei ole võimalik kiiresti ja lihtsalt saada teavet andmetöötluse eesmärkide ja andmete töötlemise loogika kohta üldiselt. Seega käesoleval ajal ei ole andmesubjektile tagatud efektiivset lahendust oma õiguste kaitsel.

Töö autori arvates ei ole eluliselt usutav, et andmesubjektil oleks oma õiguste kaitsmise eesmärgil võimalik teha lakkamatult päringuid sadadele volitatud töötlejatele informatsiooni saamiseks. Lisaks eeldaks see, et andmesubjekt on kursis andmekogude regulatsiooniga.

Samas üha enam erinevates eluvaldkondades leiavad kasutust Agendid, mida kasutatakse väga erinevatel eesmärkidel, näiteks informatsiooni analüüsimiseks. Kasutajal on lihtne juba eelnevalt analüüsitud info põhjal otsuseid teha. Seega andmesubjekti osaluse põhimõtte realiseerimise tagamiseks e-lahenduste abil on mitmeid erinevaid võimalusi.

Töös püstitati hüpotees, et kehtiv andmekogude regulatsioon, mis sätestab nõuded andmekogudele, ei taga andmesubjektile võimalust realiseerida oma õigusi, mis tulenevad andmesubjekti osaluse põhimõttest.

Esimese uurimisküsimuse lahendamise käigus sisustati andmesubjekti osaluse põhimõte, selleks käsitleti andmesubjekti osaluse põhimõtte kujunemist nii läbi EL privaatsusõigust käsitlevate olulisemate õigusaktide, EIK ja ELK kohtupraktika, kui ka Eesti isikuandmete kaitse ja andmekogude regulatsiooni. Lisaks kasutati andmesubjekti osaluse põhimõtte sisustamisel töös AKI ülevaateid ja erialakirjandust. Uurimisküsimuse lahendamise käigus sisustati andmesubjekti osaluse põhimõte:

- andmesubjekti andmeid võib töödelda seaduse alusel juhul, kui see on õigusaktides selgesti ette nähtud;
- andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet milliseid andmeid tema kohta töödeldakse (v.a eelnevalt käsitletud piirangud);
- andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet millistele kolmandatele isikutele on tema andmeid edastatud (v.a eelnevalt käsitletud piirangud);
- andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet oma andmete töötlemise eesmärkide kohta (v.a eelnevalt käsitletud piirangud);
- andmesubjektil on õigus saada liigse viivituse ja kuludeta teavet oma andmete töötleja kohta;
- andmesubjektil on õigus liigse viivituse ja kuludeta oma andmed töötlemiseks sulgeda, neid kustutada ja parandada kui andmeid ei töödelda Direktiivi põhimõtetega kooskõlas;
- andmesubjektil on õigus liigse viivituse ja kuludeta saada teavet oma andmete töötlemise protsessi ja loogika kohta st eelnevalt käsitletud minimaalsuse, andmekvaliteedi, eesmärgikohasuse, seaduslikkuse, turvalisuse ja kasutuse piiramise kohta oma andmete töötlemisel.

Järgnevalt võrreldi andmesubjekti osaluse põhimõtet kehtiva andmekogude regulatsiooniga ja jõuti järeldusele, et kehtivat andmekogude regulatsiooni peab täiendama olulisel määral. Probleemina toodi esile, et kehtiv AvTs regulatsioon nõuab vaid üksikute aspektide reguleerimist andmekogu vastutava töötleja poolt. Selline lähenemine võimaldab andmesubjektil oma andmete õiguspärast töötlemist kontrollida vaid piiratud ulatuses. Ettepanekute koostamisel andmekogude regulatsiooni täiendamiseks võeti arvesse AKI poolt koostatud juhendis toodud suuniseid andmekogude pidajale. Töö autor peab tuginedes mitmete töös käsitletud autorite poolt antud hinnangule oluliseks, et AKI poolt koostatud soovituslikus juhendis sisalduv oleks reguleeritud andmekogude regulatsioonis. Ilma konkreetseid sisunõudeid andmekogude regulatsioonis määratlemata ja ei ole võimalik õiguspärase töötlemise nõudeid kontrollida ega nende nõuete

täitmist tagada. Analüüsi tulemusel töö autor teeb järgnevad ettepanekud andmekogude regulatsiooni täiendamiseks ja muutmiseks:

AvTs § 43^5 sõnastust[220] peab täiendama: andmekogu põhimäärus peab lisaks seaduses nõutavale andmekogu vastutava töötleja, andmekoosseisu ja andmete andja määratlemisele sisaldama alljärgnevat:

- andmekogu pidamise üldist eesmärki;
- volitatud töötlejaid;
- ISKE osaklasse ja turbeastet;
- kogutavate andmekoosseisude loetelu, millest iga andmekoosseisu juures on määratud konkreetne eesmärk, milleks seda andmekoosseisu kogutakse, kes on selle andmekoosseisu puhul andmeandja ja kes on õigustatud andmesaajad (püsiva juurdepääsu saajad);
- milline on iga konkreetse andmekoosseisu puhul andmete säilitustähtaeg ja milline on andmete hävitamise korraldus;
- millistel alustel on võimalik andmesubjektil andmeid parandada;
- mida logitakse ja kui kaua logiinformatsiooni säilitatakse;
- kuidas on võimalik andmesubjektil saada logiinfot enda kohta käivate andmete osas.

Kui rakendusakti ei peeta otstarbekaks kehtestada, peab eelnev olema sätestatud seaduse tasandil.

Olemasolevate andmekogude puhul anda rakendussätetega mõistlik aeg andmekogu regulatsiooni vastavusse viimiseks ülal toodud nõuetega.

Töö autor teeb lisaks ettepanekud sätestada konkreetsed kohustused KOV-idele ja avalik - õiguslikele juriidilistele isikutele turvalisuse põhimõtte tagamiseks isikuandmete töötlemisel.

Töö autori hinnangul ISKE rakendamine on andmesubjekti jaoks äärmiselt oluline, sisaldades tuhandeid turvameetmeid andmesubjekti andmete kaitseks, mistõttu tõhus kontroll vastutavate töötlejate üle on äärmiselt vajalik.

[220] § 43^5. Andmekogu põhimääruses sätestatakse andmekogu pidamise kord, sealhulgas andmekogu vastutav töötleja (haldaja), andmekogusse kogutavate andmete koosseis, andmeandjad ja vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused.

Samuti ei ole töö autori hinnangul põhjendatud andmesubjekti vaatest KOV-idele ja avalik – õiguslikele juriidilistele isikutele erisuste kehtestamine riigi infosüsteemi kindlustavate süsteemide määruse rakendamisel ja infoturbe juhi määramisel.

Selleks tuleb täiendada järgnevaid õigusakte:

- Avaliku teabe seaduse § 43^9 lõiget 3 täiendada avalik õiguslike juriidiliste isikutega.
- Vabariigi Valitsuse 13.03.2012.a määrust „Infoturbe juhtimise süsteem“ täiendada kohustusega KOV-idele ja avalik – õiguslikele juriidilistele isikutele infoturbe juhi määramiseks;
- Vabariigi Valitsuse 20.12.2007.a määrust „Infosüsteemide turvameetmete süsteem“ täiendada ISKE rakendamise ja auditeerimiskohustusega avalikõiguslikele juriidilistele isikutele;
- Vabariigi Valitsuse 20.12.2007.a määrust „Infosüsteemide turvameetmete süsteem“ täiendada ISKE auditeerimiskohustusega KOV-idele.

ISKE rakendamise staatuse kontrollimiseks töö autor teeb ettepaneku täiendada Vabariigi Valitsuse 28.02.2008.a määrust „Riigi infosüsteemi haldussüsteem“ viisil, mis võimaldaks RIHA andmetele tuginedes tuvastada ISKE auditeerimise intervall.

Töö autori hinnangul väärib kaasaegsete tehniliste lahenduste, eelkõige X-tee võimalustest lähtuvalt kaalumist IKS-i paragrahvi 19 muutmine: sätte kohaselt peab andmesubjektile andma teavet tema kohta käivate andmete osas 5 tööpäeva jooksul. Töö autori hinnangul väärib andmesubjekti vaatest ja tehnilistest võimalustest lähtuvalt kaalumist selle tähtaja lühendamine. Kuna IKS nõuded määravad suuresti andmekogude disaini, 5 tööpäevase tähtaja lühendamine avaldab otsest mõju uute arenduste väljatöötamisele. Mõistetavalt ei ole tehniliselt võimalik sellist nõuet rakendada ilma ülemineku rakendussäteteta olemasolevate andmekogude puhul, kuid lühema tähtaja nõue oleks koheselt rakendatav uute arenduste elluviimisel.

Kolmanda uurimisküsimuse lahendamise käigus käsitleti nõudeid e-lahendustele andmesubjekti osaluse põhimõtte realiseerimisel Määruse eelnõu (LISA 1), Infoühiskonna arengukava 2020[221], Valitsuserakondade koalitsioonileppe[222], Avalike teenuste korraldamise rohelise raamatu[223] ja E-

[221] Infoühiskonna arengukava 2020, *supra* note 9.
[222] Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta, *supra* note 10, p. 4.20.
[223] Avalike teenuste roheline raamat, *supra* note 11, lk 17-18.

riigi harta[224] põhjal. Uurimisküsimuse lahendamise käigus selgus, et siseriiklikes dokumentides, mis puudutavad e-lahendusi küll tähtsustatakse andmesubjekti osaluse põhimõtte realiseerimiseks sammude asutumist, kuid andmesubjekti osaluse põhimõte ei ole sisustatud ühetaoliselt ning Määruse eelnõu sisu on kantud Infoühiskonna arengukavas 2020[225], koalitsioonileppes ja Rohelises raamatus kantud põhimõtetest vaid osaliselt. Samas on kõikides eelpool nimetatud dokumentides märgitud vajadust luua andmesubjektile võimalused oma andmetele juurdepääsuks lihtsalt, kiiresti ning andmesubjektile mõistetaval viisil.

Neljanda küsimuse analüüsimiseks käsitleti töös tehnoloogilisi võimalusi andmesubjekti osaluse põhimõtte realiseerimisel. Selleks võrreldi Rakendust eelnevalt sisustatud andmesubjekti osaluse põhimõttega ja nõuetega e-lahendustele.

Rakenduse pilootprojektiga[226] on liitunud üksikud andmekogud: isikut tõendavate dokumentide register, digilugu ning karistusregister. Rakenduse abil on võimalik kontrollida millisele organisatsioonile andmesubjekti puudutavaid andmeid on edastatud. Töös käsitletud Määrusega (LISA 1) soovitakse Rakenduse kontseptsioon teha kohustuslikuks ka teistele andmekogudele.

Rakenduse funktsionaalsuse võrdlemisel eelnevalt sisustatud andmesubjekti osaluse põhimõtte ja nõuetega e-lahendustele selgus, et Rakenduse abil on võimalik kontrollida vaid üksikuid aspekte õiguspärase töötlemise kohta ning see saab olla pigem juhuslikult avastatud. Lisaks jääb probleemiks andmekogude rohkus: Rakendus võimaldab saada informatsiooni korraga ühest andmekogust, selline lähenemine aga eeldab andmesubjektilt märkimisväärset ajakulu. Eelnevale lisandub õiguspärase töötlemise aluspõhimõtetele hinnangu andmise ajakulu, mis eeldab andmesubjekti poolset kõrget teadlikkust valitsemiskorraldusest ja institutsioonidest. Isegi juhul, kui andmesubjektil on piisavalt aega lakkamatult erinevates andmekogudes päringuid teostada ning piisavad teadmised seaduste ja põhimääruste abil volitamata töötlemise tuvastamiseks, eeldab andmesubjekti osaluse põhimõtte realiseerimine kompleksset lähenemist, mis tähendab, et töö autori poolt tehtud ettepanekud andmekogude regulatsiooni muutmiseks ja täiendamiseks peavad olema realiseeritud.

[224] E-riigi harta, *supra* note 12.
[225] Ibid.
[226] Projekti „Suur Vend“ tutvustus, *supra* note 183.

Seega uurimise tulemusel leidis kinnitust, et eelnevalt käsitletud tingimused saada informatsiooni ühest kohast ja kiiresti Rakenduse abil ei realiseeru. Rakenduse abil on võimalik kontrollida üksikuid andesubjekti osaluse põhimõtte aspekte.

Viienda küsimuse uurimise objektiks oli Agendi rakendamise võimalikkus andmesubjekti kaitsel. Agenditeooria uurimiseks kasutati teadusartikleid. Eelnevalt sisustatud andmesubjekti osaluse põhimõtte ja e-lahendustele esitatud nõuete kontekstis oli lähteülesandeks, et andmesubjekti vaatest on oluline pakkuda rakendust, mis oleks lihtne, kiire ja mõistetav andmesubjekti jaoks. Seega arvestades, et Eestis on andmekogusid arvult sadades, peab rakendus olema suuteline andmesubjekti vaatest nö. ühe klikiga hankima ja analüüsima võimalikult palju informatsiooni, teostama andmesubjekti volitusel teatud toiminguid, näiteks saatma teavitusi targa vormi abil järelevalveasutusele ning informeerima vajadusel andmesubjekti. Seega tarkvaralise lahenduse rakendamise eelduseks oli, et see ei saa tugineda üksnes ühele allikale nagu eelnevalt käsitletud Rakendus seda teeb, allikaid peab olema mitmeid. Lisaks oli tarkvaralise lahenduse rakendamise eelduseks, et andmesubjektil peab olema võimalik määrata, kas ta soovib saada informatsiooni kõikide X-teel olevate andmekogude kohta või ainult üksikute kohta. Samuti peab andmesubjektil olema võimalus sisestada teatud andmekoosseise, mis on tema jaoks olulised, näiteks elukoha andmed, et need oleksid igas andmekogus õiged. Tal peab olema võimalik valida teavituste kriteeriume ja võimalus volitada Agenti enda nimel pöörduma järelevalve asutuse või vastutava töötleja poole.

Kuna töös jõuti samuti järeldusele, et määrava tähtsusega andmesubjekti õiguste kaitsel on RIHA menetluste läbimine, selge seaduslik alus andmetöötlusel, täpsustatud nõuded põhimäärustele ja ISKE rakendamine ning auditeerimine, töö autor hindas, kas ja milliseid õiguspärase töötlemise nõudeid on võimalik kontrollida automatiseeritult. Agendi kontseptsiooni rakendamise võimalikkuse uurimisel lähtuti alljärgnevast:

- Seaduslikkuse põhimõtet on võimalik kontrollida eRT vahendusel.
- ISKE rakendatust ja auditeerimise staatust on võimalik kontrollida RIHA vahendusel.
- Töötlemise eesmärgi seose kohta konkreetse töötlejaga on võimalik saada eRT vahendusel.
- Oma andmete töötleja ja juurdepääsude kohta konkreetsetele andmekoosseisudele on võimalik saada X-tee vahendusel.
- Kasutuse piiramise, minimaalsuse, andmekvaliteedi ja turvalisuse põhimõtteid on samuti võimalik kontrollida automatiseeritult X-tee, eRT ja RIHA koostoimes.

- Andmekogu staatuse kontrolli (nt. „kasutusel“, „asutamine kooskõlastatud“ vms) on võimalik teostada RIHA vahendusel.
- Delikaatsete isikuandmete töötlemise puhul on võimalik kontrollida vastutava töötleja olemasolu vastavas registris (DIAT).

Edasise analüüsi käigus selgus, et lisaks eeltoodud allikatele eeldab seaduslikkuse ja eesmärgi kohasuse põhimõtte kontroll kataloogi loomist välistavatest asjaoludest, mis aitavad hinnata kas andmekasutus on seaduslikkuse ja eesmärgikohasuse põhimõtetega kooskõlas. Kataloogi loomist, milles on teatud üldistatud elemendid, on oma töös kasutanud samuti Norta *et al*. [227] Interneti suhtlusel võimalike petuskeemide tuvastamisel.

Lisaks selgus, et kasutuse piiramise analüüsimiseks ei piisa eelpool nimetatud allikatest, see tähendab, et keeruline on kontrollida, kas isikul, kes juurdepääsu saab, on reaalne teadmisvajadus andmetele teatud menetluse kontekstis või mitte, sest see on tugevalt seotud organisatsiooni, kes andmeid töötleb, sisemise tegevusega. Selle probleemi lahendamiseks töö autori hinnangul on võimalik kasutada Rull *et all.* poolt pakutud kontseptsiooni andmekogu väärkasutamiste vältimiseks koos rolli mudeliga, mis tagab, et andmekoosseisudele saavad organisatsioonis juurdepääsu õigustatud isikud ning, et õigustatud isikud kasutavad andmekoosseise eesmärgipäraselt.[228]

Turvalisuse põhimõtte tagamiseks ei piisa samuti vaid eelpool nimetatud allikatest, kuigi esmatasandil on võimalik käideldavuse nõudeid kontrollida RIHA andmetele tuginedes. Põhjalikuma analüüsi jaoks Agent peab suutma kontrollida andmekogu andmekasutust tervikluse ja konfidentsiaalsuse aspektist. Turvalisuse tagamiseks töö autor teeb ettepaneku, et Agent peab tegema regulaarseid läbistusteste andmekogude vastu, milles andmesubjekti andmeid töödeldakse. Täiendavat uurimist vajab kuidas Agendi poolt läbiviidavaid läbistustestide läbiviimist õiguslikult reguleerida.

Seega Agendi rakendamiseks on juba käesoleval ajal olemas mitmeid allikaid, mis võimaldaksid andmesubjekti õiguseid kaitsta märkimisväärselt laiemas ulatuses kui see käesoleval ajal võimalik on. Samas Agendi rakendamine eeldab andmekogude regulatsiooni muutmist ja täiendamist, mis võimaldab Agendil efektiivselt infot analüüsida.

[227] Norta *et al. supra* note 197.
[228] Rull *et al. supra* note 8, lk. 89-92.

Andmesubjekti jaoks tähendab Agendi rakendamine, et õiguspärase töötlemise põhimõtteid on võimalik kontrollida automatiseeritult, see tähendab, et andmesubjekti on võimalik piirduda minimaalsete toimingutega. Samuti ei eelda Agendi rakendamine andmesubjektilt laialdasi teadmisi andmekogude regulatsioonist, järelevalve pädevustest ega valitsemiskorraldusest, Agent korraldab iseseisvalt vajamineva analüüsi ja teavitused.

Töös väljapakutud Agendi kontseptsiooni rakendamine eeldab täiendava nõuete analüüsi läbiviimist.

Töös kasutati kvalitatiivset meetodit, analüüsiti asjakohaseid õigusakte, eriala kirjandust, Andmekaitse Inspektsiooni aasta aruandeid ja muid andmesubjekti osaluse põhimõtet käsitlevaid dokumente.

The Possibilities of Using A Software-Agent to Ensure the Principle of Data Subject Participation

Summary

Personal data protection is one of the fundamental rights. Nowadays public services are provided using information technology, which makes it easy to process large amounts of data. However, most databases contain personal data and sensitive personal data. Most commonly used data exchange system is the X-road, which is employed to exchange thousands of units of data every day.

There have been many cases of database misuse which have been covered in the media and in the academic publications as well as in the Data Protection Inspectorate reviews. Therefore, it is in the interests of the data subject that the data exchange should be carefully regulated.

Currently there are only a few databases with a bulit-in function of a verified data subject access to the stored data and its use by third parties. However, it is impossible to quickly and easily access the information on the purposes and the logic of the data processing. Therefore, currently data subjects have not been provided an effective solution to protect their rights. The author of this thesis believes that it is not feasible for a data subject exercising their right to data protection to constantly make enquires of hundreds of chief processors in order to access the information. This would also mean that the data subjects would have to have extensive knowledge of the regulations governing data protection and processing.

One of the solutions could be the use of Agents, which are already being used in different fields for many different purposes such as information analysis, for example.

The author of this thesis formulated the hypothesis that suggests that the current Databases Regulation Act, which sets the requirements for databases, does not cover the data subject participation rights.

Firstly, the author explores the principles of the data subject participation. Next, the author compares the principles of the data subject participation with the current Databases Regulation Act and finds that the Databases Regulation Act needs major improvements. Without precisely defined requirements on data contents, it is not possible to check the lawful objectives of data processing.

Secondly, the author analyses the requirements for digital solutions and concludes that the systems providing data subjects with access to data should be made easy and quick for the data subjects to use.

The author then proceeds to look at solutions currently used by some databases to enable data subject access the data concerning him or her to see whether they meet the requirements set for the digital systems and the clause of the data subject participation. The findings show that the solutions currently in use do not provide the data subject with a full overview of the lawful objectives of the data concerning the data subject. Another problem is that nowadays there are so many databases which means that a data subject wishing to exercise their right to information would have to constantly search different databases.

The author then proceeds to analyse whether using a software Agent as an alternative solution for protecting the rights of the data subject would grant the data subject a quick and easy access to the lawful objectives of their data. The premise of employing such an Agent would have to be that the Agent would work constantly and independently and would have to be able to check the lawful objectives of all data processed. The Agent would also have to be able to make automated enquiries from cheif processors and the governing bodies. The author of this thesis presumes that employing an Agent as a solution would require it to have access to the administration system of the state information system, The State Gazette and the X-road as well as the data held by Register of processors of personal data and persons responsible for protection of personal data.

The analysis shows that for the principle of legality and the principle of purposefulness to be met a separate catalogue would have to be set up in addition to the aforementioned sources to include exclusions which would help determine the principle of legality and the principle of purposefulness of data use.

The author also concludes that the aforementioned sources would not be enough to analyse the principle of restricted use of data. The author of the thesis therefore suggests, based on the theory covered in this thesis, a concept which ensures that only authorised persons are given access to databases within organisations, also ensuring the lawful objectives of the authorised persons.

The analysis of the concept of an Agent also revealed that the aforementioned sources would not ensure the principle of security. Therefore, the author proposes the Agent perform regular penetration and availability tests on the databases which process the data subjects' data.

The findings of this thesis show that some of the sources required to employ the Agent already exist, and that using such an Agent would significantly improve the protection of the rights of the data subjects. However, for the Agent to successfully analyse the data, changes and improvements have to be made to The Data Regulations Acts.

For the data subject, employing an Agent would mean that the checking of the principles of legality of data processing would become automated, making data enquiry a much easier process. Using an Agent would be easy as it would not require specialist knowledge of Data Regulation Acts or the governing bodies. The Agent would perform all necessary analyses and notifications.

The research method used for this thesis was the qualitative method for which relevant law Acts, academic ions and the other different documents on the principles of Data Subject participation were analysed.

Kasutatud allikad

Artiklid ja raamatud

1. Albers, M. Isikuandmete kaitse põhiõiguslik alus: kas õigus informatsioonilisele enesemääramisele ja/või eraelu austamisele. Juridica VIII/2005, lk 537-543.
2. Alexy, R. Põhiõigused Eesti põhiseaduses. Juridica eriväljanne, Tallinn 2001, lk. 5-96.
3. Bainbridge, D., I. Processing Personal Data and the Data Protection Directive. Information & Communications Technology Law, Vol. 6, No. 1, 1997, lk. 17-40.
4. Bygrave, L. A. Data Protection Law: Approaching Its Rationale, Logic and Limits. Kluwer Law International, 2002, 456 lk.
5. Bygrave, L. A. Data Privacy Law An International Perspective. Oxford University Press, 2014, 233 lk.
6. Bygrave, L. A. Electronic Agents and Privacy: A Cyberspace Odyssey. International Journal of Law and lnformation Technology, Vol. 9 No. 3 Oxford University Press, 2001, lk. 275-294.
7. Carlsson, C. Decision Support in virtuaal Organizations: The case for Multi-Agent Support. Group Decision and Negotiation 11. Kluwer Academic Publishers, 2002, lk 185-221.
8. Cruquenaire, A. Electronic Agents as Search Engines: Copyright related aspects. International Journal of Law and Information Tehnology, Vol 9, 2001, lk. 327-343.
9. Gonzalo, S. A. Business Outlook regarding Electronic Agents. International Journal of Law and Information Technology, Vol. 9 No. 3, 2001, lk. 189-203.
10. Gowda, R. S. Role of Software Agents in E-Commerce. Vol.3, Issue. 3, Computational Engineering Research, Vol. 3 Issue. 3, 2013, lk. 246-251.
11. Gundermann, L. Euroopa Liidu andmekaitseõigus – andmekaitse ja andmetele avaliku juurdepääsu suhtest ning andmekaitse järelevalve olukorrast. Juridica VIII/2005, lk. 511-518.
12. Hornung, G. Regulating privacy enhancing technologies: seizing the opportunity of the future European Data Protection Framework. Innovation: The European Journal of Social Science Research, Vol. 26, Nos. 1-2, 2013, lk 181-196.
13. Ilus, T. Andmesubjekti osaluse põhimõte Euroopa Nõukogu konventsioonide ning Euroopa Inimõiguste Kohtu lahendite valguses. Juridica VIII/2005, lk. 519-531.
14. Ilus, T. Isikuandmete kaitse olemus ja arengusuunad. Juridica VII/2002, lk 435-446.
15. Kemp, R., Moore, A. D. Privacy. Library Hi Tech, Vol.25(1), 2007, lk. 58-78.
16. Laurand, A. Euroopa Liidu liitumine Euroopa põhivabaduse kaitse konventsiooniga. Juridica IX 2013, lk. 676-690.

17. Lee, H. H.; Stamp, M. An agent-based privacy-enhancing model. Information Management & Computer Security, 2008, Vol.16(3), lk. 305-320.
18. Lillemaa, P. F. Märkusi isikuandmete kaitse seaduse eelnõu kohta. Juridica VII, 2002, lk 447-453.
19. McCarty, L. T. Reflections on TAXMAN: An experiment in artificial intelligence and legal reasoning. Harward Law Review, 90(5), 1977, lk 837-893.
20. Männiko, M. Õigus privaatsusele ja andmekaitse. Tallinn, Juura 2011, 255 lk.
21. Norta, A.; Nyman-Metcalf, K.; Othman, A. B.; Rull, A. My agent will not let me talk to the General, Software agents as a tool against Internet Scams. Springer, 2016, lk 11-44.
22. Oren, J. S. T. Electronic Agents and the Notion of Establishment. International Journal of Law and Information Technology,Vol 9 No. 3, Oxford University Press, 2001, lk. 249-274.
23. Ovey, C.; White R. C. A. European Convention on Human Rights. 3rd ed. Oxford University Press 2002. 506 lk.
24. Pilving, I. Õigus isikuandmete kaitsele. Juridica VIII/2005. lk. 532-536.
25. Rull, A.; Täks, E.; Norta, A. Towards Software-Agent Enhanced Privacy Protection. Springer, lk. 73-94.
26. Sartor G.; Branting L. K. Introduction: judicial applications of artificial intelligence. Artificial Intelligent Law, 1998, lk. 105-110.
27. Serenko, A., Detlor, Ę. B. Intelligent agents as innovations. Springer, 2004, lk. 364-381.
28. Smith, A. E.; Nugent, C. D.; McClean, S. I. Evaluation of inherent performance of intelligent medical decision support systems: utilising neural networks as an example. Artificial Intelligent in Medicine, 2003, lk 1-27.
29. Sterling, L. S.; Taveter, K. The Art of Agent-Oriented Modeling. The MIT Press, Cambridge, 2009, 367 lk.
30. Solove, D. J. Conceptualizing Privacy. California Law Review, Vol. 90:1087, lk. 1088-1154, 2002.
31. Solove, D. J. Access and Aggregation: Public Records, Privacy and the Constitutions. Minnesota Law Review. Vol. 86, 2002, lk 1138-1176.
32. Tikk, E.; Nõmper, A. Informatsioon ja õigus. Tallinn, Juura 2007, 186 lk.
33. Truuväli, E. J. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. Tallinn: Juura 2002, 757 lk.
34. Tupay, P. K.; Mikiver, M. E-riik ja põhiõigused. Juridica III/2015, lk 163-176.

Määrused

35. Infosüsteemide andmevahetuskiht RT I, 15.09.2015, 11.
36. Infosüsteemide turvameetmete süsteem RT I, 15.09.2015, 11.
37. Infoturbe juhtimise süsteem RT I, 19.03.2012, 4.
38. Riigi infosüsteemi haldussüsteem RT I, 04.07.2014, 7.

Seadused

39. AvTS RT I RT I, 06.01.2016, 7.
40. IKS RT I, 06.01.2016, 10.
41. PS RT I, 15.05.2015, 2.

EL õigusaktid

42. Inimõiguste ja põhivabaduste kaitse konventsioon. RT II 1996, 11, 34.
43. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. RT II 2001, 1, 3.
44. Euroopa Liidu põhiõiguste Harta. C 326/391, 26.10.2012 art 8.
45. Euroopa Parlamendi ja Nõukogu 24. oktoober 1995 aasta direktiiv 95/46/EÜ, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ELT L 281/31.
46. Euroopa nõukogu ja komisjoni määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta COM(2012) 11 final, 2012/0011 (COD).

Kohtulahendid

47. EIKo 04.05.2000, 28341/95, *Rotaru vs Rumeenia* p 57.
48. EIKo nr 47114/99, 22. oktoober 2002, *Taylor-Sabory vs Ühendkuningriik.*
49. ELK, 16.12.2008, C-524/06, *Huber vs. Saksamaa.*
50. EIKo 4. detsember 2008 , nr 30562/04 ja 30566/04, *S. ja Marper vs. Ühendkuningriik.*
51. EIKo, 27. oktoober 2009, 21737/03, Haralambie vs. Rumeenia.
52. ELKo, 9. november 2010, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert vs. Land Hessen*, p 89 ja 86.
53. EIK 18. oktoober 2011, nr 16188/07 *Khelili vs Sveits.*
54. RKHKo 12.07.2012,3-3-1-3-12, p. 24.
55. EIKo 13. november 2012, *M.M. vs. Ühendkuningriik*, nr 24029/07.

Seletuskirjad, käskkirjad, aastaaruanded, arengukavad

56. Isikuandmete kaitse seaduse seletuskiri http://www.aki.ee/et/eraelu-kaitse/oigusaktid (17.01.2016).
57. Andmekaitse inspektsiooni peadirektori 14.08.2013.a käskkiri „Andmekaitse Inspektsiooni menetluskord Riigi infosüsteemi haldussüsteemis: http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/AKI%20menetluskord%20RIHAs%20uuendatud%2019092014_0.pdf (17.01.2016).
58. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2011, soovitused aastaks 2012. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202013%20l%C3%B5plik%20PDF.pdf, (17.01.2016).
59. Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2012, soovitused aastaks 2013. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202013%20l%C3%B5plik%20PDF.pdf (17.01.2016).
60. Avaliku teabe seadus ja isikuandmete kaitse seaduse täitmisest aastal 2013, soovitused aastaks 2014. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Aastaraamat%202013%20l%C3%B5plik%20PDF.pdf (17.01.2016).
61. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2014 aastal. Soovitused aastaks 2015. http://www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/aastaraamat%202014.pdf (20.01.2016).
62. Infoühiskonna arengukava 2020 https://www.mkm.ee/et/arengukavad (20.01.2016).
63. Eesti Reformierakonna, Sotsiaaldemokraatliku erakonna ning erakonna Isamaa ja Respublica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta http://www.sotsdem.ee/wp-content/uploads/2015/04/RE-SDE-ja-IRLi-valitsusliidu-lepe.pdf (20.01.2016).
64. Avalike teenuste roheline raamat https://www.mkm.ee/sites/default/files/avalike_teenuste_korraldamise_roheline_raamat.pdf (20.01.2016).

65. E-riigi harta http://www.riigikontroll.ee/Riigikontrollipublikatsioonid/Muudpublikatsioonid/tabid/113/language/et-EE/Default.aspx (20.01.2016).

Viidatud veebilehed

66. RIA koduleht https://www.ria.ee/ee/x-tee-tutvustus.html#mis (17.01.2016).
67. RIHA kodulehekülg https://riha.eesti.ee/riha/main#1453152134558ngpeupfKIcVNwvU (17.01.2016)
68. ISKE rakendamise juhendid ja kataloogid https://www.ria.ee/ee/x-tee-tutvustus.html#mis (17.01.2016)
69. Projekti „Suur Vend“ tutvustus: https://www.x-road.eu/community/20150420/2_20150420_X-tee_suurVend_pirete.odp (17.01.2016)

Muud materjalid

Susi, M. Euroopa Inimõiguste Kohtu 2010. aasta kohtulahendite ülevaade, Tartumaa, OÜ Greif, 2011, 366 lk.

LISA 1 Vabariigi Valituses määruse eelnõu „Teenuste korraldamise ja teabehalduse alused“

EELNÕU
24.11.2015

VABARIIGI VALITSUS

MÄÄRUS

Teenuste korraldamise ja teabehalduse alused

Määrus kehtestatakse Vabariigi Valitsuse seaduse § 27 lõike 3 ja arhiiviseaduse § 6 lõike 2 alusel.

1. peatükk
ÜLDSÄTTED

§ 1. Reguleerimis- ja kohaldamisala

(1) Määrusega kehtestatakse teenuste korraldamise ja teabehalduse alustena nõuded:
1) teenuste korraldamisele ja arengule;
2) teabehalduse korraldamisele.

(2) Määrust kohaldatakse valitsusasutustele.

(3) Valitsusasutused (edaspidi *asutus)* tagavad määrusega kehtestatud nõuete järgmise oma hallatavates asutustes.

(4) Peatükis 4 sätestatut kohaldatakse kõigile avalikke ülesandeid täitvatele asutustele ja isikutele.

(5) Määruses sätestatut ei kohaldata:
1) riigisaladuse ja salastatud välisteabe töötlemisele;
2) dokumendivahetusele välisriikidega.

§ 2. Teenused

(1) Teenus määruse tähenduses on avalik teenus ja tugiteenus.

(2) Avalik teenus määruse tähenduses on teenus, mida asutus osutab eraõiguslikule isikule (edaspidi *isik)* mis tahes suhtluskanali (edaspidi *kanal)* kaudu, et võimaldada isikul täita seadusest tulenevat kohustust või kasutada seadusest tulenevat õigust.

(3) Proaktiivne teenus on avalik teenus, mida asutus osutab oma initsiatiivil, isiku eeldataval tahtel ja riigi infosüsteemi kuuluvate andmekogude andmete alusel. Proaktiivne teenus osutatakse automaatselt või küsitakse selle osutamiseks isiku nõusolekut.

(4) Sündmusteenus on avalik teenus, mida mitu asutust osutab ühiselt, et isik saaks mugavalt täita kõik kohustused ja kasutada kõiki õigusi, mis talle tekivad seoses ühe sündmuse või olukorraga tema elujärgus. Sündmusteenus koondab mitu sama elu- või ärisündmusega seotud teenust (edaspidi *osateenus*) nii, et näib selle kasutajale üheainsa sujuva teenusena.

(5) Tugiteenust osutab asutus ametnikele või töötajatele, et toetada asutuste ülesannete täitmist.

(6) Protsess määruse tähenduses on asutuse põhi- või tugiülesande täitmisele või asutuste ühise teenuse osutamisele suunatud tegevuste korrastatud kogum. Protsess hõlmab ühte või mitut teenust.

(7) Omanik määruse tähenduses on asutus või asutuse struktuuriüksus ja selle määratud ametnik või töötaja, kes vastutab protsessi, teenuse või teenuste osutamise kanali haldamise ja arendamise eest.

§ 3. Teabehaldus ja dokumendihaldus

(1) Teabehaldus on tegevus, mis toetab asutuse ja avaliku sektori eesmärkide saavutamist teabe planeerimise, haldamise ja jagamise kaudu. Teabehaldus tagab teenustega seotud teabe kvaliteedi ja kättesaadavuse ning vähendab teabe loomise, hoiu ja kasutamisega seotud riske ja kulusid.

(2) Teabena käsitatakse määruses mis tahes viisil ja mis tahes teabekandjale jäädvustatud avalikku teavet, mis on saadud või loodud asutuse või avalikke ülesandeid täitva isiku tegevuse käigus. Teabena käsitatakse ka arhiiviseaduse § 2 lõigetes 1 ja 2 nimetatud teavet.

(3) Dokumendina käsitatakse määruses arhiiviseaduse § 2 lõigetes 1 ja 2 nimetatud teavet, mis on jäädvustatud paberkandjale, ametliku e-kirja sõnumisse või kontoritarkvara abil loodud faili.

(4) Dokumendihaldus on teabehalduse alategevus, mis korraldab asutuse dokumentide haldamist, menetlemist, vahetamist ja juurdepääsu dokumendihaldussüsteemi abil. Dokumendihaldussüsteem on standardlahendusena loodud infosüsteem, mis kasutab dokumentide liigitamiseks hierarhilist liigitusskeemi ja mille osaks on dokumendiregister.

2. peatükk
VASTUTUS TEENUSTE KORRALDAMISE JA ARENGU EEST

§ 4. Vastutus asutuse teenuste korraldamise ja kvaliteedi eest

(1) Asutuse teenuste ühtse korraldamise ja kvaliteedi eest vastutab asutuse juht, kui seaduses või asutuse põhimääruses ei ole sätestatud teisiti.

(2) Seaduses, asutuse põhimääruses või muus asutuse sisemist töökorraldust reguleerivas aktis määratakse ameti- või töökohad, millel töötavad isikud tagavad asutuse:
1) avalike teenuste korraldamise ja kvaliteedi;
2) protsesside korraldamise ja kvaliteedi;
3) teabehalduse korraldamise ja kvaliteedi;
4) teabele juurdepääsu korraldamise ja selle kvaliteedi;
5) dokumendihalduse korraldamise ja kvaliteedi.

(3) Lõikes 2 nimetatud ameti- või töökohtadel töötavad isikud teevad lõikes 1 nimetatud isiku juhtimisel koostööd, et tagada asutuse teenuste ühtlane kvaliteet.

(4) Asutus määrab igale protsessile, teenusele ja teenuste osutamise kanalile omaniku ning annab omanikule tema tegevuseks vajaliku volituse ja ressursid.

(5) Asutus sätestab oma sisemist töökorraldust reguleerivates aktides teenusega seotud tegevuste, teabe ja vastutuse üleandmise ametniku või töötaja teenistus- või töösuhte lõppemisel, ametniku avaliku võimu teostamise õiguse või töötaja teenistussuhte peatumisel või asutuse töökorralduse muutmisel.

§ 5. Asutuste ülene teenuste arengu koordineerimine

(1) Asutuste ülest teenuste arengut koordineerivad asutused (edaspidi *koordineerijad)* on:
1) avalike teenuste korraldamisel Majandus- ja Kommunikatsiooniministeerium;
2) teabele juurdepääsu korraldamisel avaliku teabe seaduse rakendamisel Andmekaitse Inspektsioon;
3) dokumendihalduse korraldamisel Majandus- ja Kommunikatsiooniministeerium;
4) riigi infosüsteemi arhitektuuri, sh kesksete komponentide, nõuete rakendamisel Riigi Infosüsteemi Amet.

(2) Koordineerija täidab järgmisi ülesandeid:
1) kavandab arengu põhisuunad ja arengut toetavad tegevused;
2) annab juhiseid ja soovitusi;
3) jälgib kavandatud tegevuste elluviimist ja juhiste rakendamist;
4) korraldab teavitustööd;
5) teeb koostööd teiste koordineerijatega;
6) kaasab vastavalt vajadusele muid osapooli.

(3) Ministeeriumi valitsemisala teenuste terviklikku arengut korraldab ministeeriumi kantsler või asjaomane asekantsler.

(4) Lõike 2 punktides 1, 2 ja 3 sätestatud ülesannete täitmise toetamiseks tegutseb koordineerija juures nõukogu, kuhu kuuluvad ministeeriumite ja Riigikantselei nimetatud esindajad ning vajadusel teised koordineerija nimetatud isikud. Nõukogu koosolekute materjalid avaldatakse koordineerija veebilehel ja vajadusel lisaks muul viisil.

(5) Nõukogu liige teavitab nõukogu tegevusest enda esindatava asutuse ja selle hallatavate asutuste asjaomaseid isikuid ning kaasab neid oma seisukohtade ja ettepanekute kujundamisel.

(6) Asutus arvestab koordineerija juhiseid ja soovitusi ning tagab nendega arvestamise oma hallatavates asutustes.

3. peatükk
TEENUSTE KORRALDAMINE

§ 6. Üldised nõuded

Asutuse teenuste korraldamine peab tagama:
1) mõõdetava või tajutava väärtuse tekkimise iga teenuse sihtrühmale;
2) väärtust mitteloovate teenuste lõpetamise või ümberkorraldamise;
3) isikute optimaalse halduskoormuse ja teenuste kasutajate rahulolu;
4) asutuse ülesannete täitmise ja teenuste osutamise dokumenteerimise optimaalses mahus;
5) teabe säilimise, kasutatavuse, kiire leidmise ja kaitse kuni teabe hävitamiseni või avalikku arhiivi üleandmiseni;
6) koostöö teiste asutuste ja muude osapooltega, mis aitab kaasa avaliku sektori kui terviku tõhususele;
7) teenuste osutamise, teabehalduse ja koostöö järjepidevuse ametniku või töötaja teenistus- või töösuhte lõppemisel, ametniku avaliku võimu teostamise õiguse või töötaja teenistussuhte peatumisel ja asutuse töökorralduse muutmisel.

§ 7. Teenuste korraldamine ja arendamine

(1) Asutusel peab oma teenuste korraldamiseks olema ajakohane ülevaade asutuse põhiülesannete täitmise protsessidest ja nendega seotud teenustest. Ülevaade koostatakse viisil, mis võimaldab seda lihtsasti ajakohastada.

(2) Kui ühe või mitme põhiülesande kohta puudub lõikes 1 nimetatud ülevaade või kui see on aegunud, määrab asutus kindlaks ja kirjeldab:
1) põhiülesande täitmise protsessi;
2) protsessiga seotud teenused;
3) teenuste osutamise kanalid;
4) teenuseid reguleerivate õigusaktide nõuded;
5) teenuste osutamiseks vajaliku ja selle käigus tekkiva teabe;
6) iga teenuse sihtrühma või sihtrühmad ning teenuse osutamisega neile tekkiva väärtuse.

(3) Asutus hindab vähemalt kord aastas asutuse teenuste kvaliteeti ja maksumust. Teenuste kvaliteedi hindamisel analüüsitakse muu hulgas teenuse töökindlust, kasutajate rahulolu ja oodatud väärtuse tekkimist.

(4) Hindamise käigus määrab asutus kindlaks protsesside, teenuste ja kanalite arendusvajadused ja arendusvajaduste prioriteedid ning tuvastab arengut takistavad tegurid.

(5) Asutus kavandab ja viib ellu prioriteetidest lähtuvad tegevused, minimeerides arengut takistavate tegurite mõju.

(6) Teenuse parema kvaliteedi huvides võivad asutused teenust korraldada ja osutada ühiselt. Asutused väldivad samade tehniliste võimalustega infosüsteemide loomist sarnaste teenuste osutamiseks. Asutused lepivad kokku ühiselt osutatava teenuse:
1) omaniku;
2) protsessi;
3) osutamise tähtaja;
4) osutamist reguleerivate õigusaktide muutmise, kui see on vajalik;
5) osutamiseks vajalike ressursside jaotuse, kui see on vajalik;
6) muud teenuse väljatöötamise või arendamise ja teenuse osutamise üksikasjad.

(7) Kui avaliku teenuse osutamiseks vajalik teave on riigi infosüsteemi andmekogudes olemas ja võib eeldada isiku tahet teenuse saamiseks, töötab asutus koostöös andmekogusid haldavate asutustega välja proaktiivse teenuse.

(8) Sündmusteenuse kavandamise või arendamise võib algatada koordineerija või mis tahes asutus, kes osutab vähemalt ühte elu- või ärisündmusega seotud avalikku teenust. Lisaks lõikes 6 sätestatule lepivad asutused kokku osateenuste osutamise tähtajad.

(9) Kui asutus haldab infosüsteemi, milles osutavad või kasutavad teenust teised asutused, vastutab ta tehnilise lahenduse ning selle toimimise ja arendamise eest. Infosüsteemi haldaja ja infosüsteemi kasutavate asutuste vahel peab olema kokku lepitud:
1) infosüsteemi võimalused, nende kasutamine ja muutmine;
2) vastutuse jaotus protsesside ja teenuste kvaliteedi eest.

§ 8. Avalike teenuste loetelu

(1) Asutus koostab oma avalike teenuste loetelu. Kui kasutamiseks avatakse uus avalik teenus, lisab asutus selle loetellu.

(2) Avalike teenuste loetelu peab iga avaliku teenuse kohta sisaldama selle:
1) kasutamise mahtu kordades,
2) osutamise kulu asutusele;
3) kasutajate rahulolu näitajat;
4) kasutajatele tekkiva halduskoormuse näitajat.

(3) Lõikes 2 nimetatud andmed esitatakse iga kalendriaasta kohta.

(4) Avalike teenuste loetelu koostamiseks ja haldamiseks töötab koordineerija välja ühtse kirjeldusvormi ja -keele ning annab juhise.

(5) Asutus avaldab avalike teenuste loetelu oma veebilehel ning lisaks neis elektroonilistes kanalites, mida isikud eelistavad teenuseni jõudmiseks kasutada.

§ 9. Avalike teenuste osutamine

(1) Asutus tagab, et avaliku teenuse kasutamiseks vajalik teave on lihtsasti leitav ja avaldatud ka Eesti teabeväravas eesti.ee (edaspidi *eesti.ee teabevärav)*. Teave esitatakse kasutajale kasutajarühma vajadustest lähtuval viisil ja mahus.

(2) Asutus ei pane isikule kohustust esitada uuesti andmeid, mis on juba kantud seaduse alusel asutatud andmekogusse, kuid isikul peab olema võimalus andmete muutumisest andmeallikat teavitada.

(3) Asutus ei pane isikule kohustust kontrollida ja kinnitada asutuste loodud või töödeldud andmete õigsust, kuid isikul peab olema võimalus avastatud veast andmeallikat teavitada.

(4) Asutus annab avaliku teenuse kasutajale teavet teenuse osutamise tähtaja kohta ja optimaalses mahus teavet teenuse kulgemisest. Asutus tagab teenuse osutamise tähtaja jooksul.

(5) Asutus tagab teenuse kasutajale võimaluse saada teenuse kasutamise käigus nõu ja abi, anda teenuse kohta tagasisidet ja teha ettepanekuid.

§ 10. Täiendavate nõuete kehtestamine avalike teenuste korraldamisele ja osutamisele

(1) Käesolevas peatükis sätestatud nõuete täpsustamiseks võib anda juhiseid koordineerija või muu pädev asutus. Kui õigusakti või juhise rakendamise üksikküsimuses on vaja kokku leppida ühetaoline toimimisviis, teeb otsuse § 5 lõike 4 alusel tegutsev nõukogu.

(2) Asutuse avalike teenuste osutamise täpsem korraldus sätestatakse asutuse sisemist töökorraldust reguleerivates aktides. Asutus toetab sätestatud nõuete täitmist infotehnoloogiliste vahenditega.

4. peatükk
TEABEHALDUSE KORRALDAMINE

§ 11. Teabe korrastamine

(1) Asutusel peab oma teabehalduse korraldamiseks olema ajakohane ülevaade protsesside käigus tekkiva teabe, selle allikate ja hoiukohtade kohta. Ülevaade luuakse § 7 lõigetes 1 ja 2 ettenähtud tegevuste käigus ning viisil, mis võimaldab seda lihtsasti ajakohastada.

(2) Kui ühe või mitme protsessi kohta puudub lõikes 1 nimetatud ülevaade või kui see on aegunud, määrab asutus kindlaks ja kirjeldab:
1) mis andmeid ja muud teavet on protsessiga seotud teenuste osutamiseks vaja, lähtudes õigusaktiga sätestatud tingimustest;
2) millist täiendavat teavet protsessi käigus luuakse või saadakse;
3) millised on teabe allikad ja juurdepääsutingimused;
4) millistes vormingutes, millistes infosüsteemides ja teistes hoiukohtades teavet hoitakse;
5) teabe säilitustähtajad, kui need on määratud;
6) kes on teabe kasutajad.

(3) Asutus analüüsib teabe kasutamist ja vajalikkust, tuvastab sama teabe dubleerimise eri vormingutes ja hoiukohtades, määrab teabele säilitustähtajad ja määratleb arhiiviseaduse § 2 lõikes 1 nimetatud teabe.

(4) Asutus lõpetab mittevajaliku teabe kogumise ja loomise ning vähendab vajaliku teabe dubleerimist. Teabe dubleerimise vähendamisel eelistab asutus andmetes hoitavat teavet dokumentides hoitavale teabele.

(5) Asutus selgitab teabe kasutajarühmade vajadused teabe, selle esitamise viisi ja mahu kohta ning arvestab vajadusi teenuste loomisel ja muutmisel.

(6) Lisaks muule teabele korraldab asutus ka ametnike ja töötajate töö käigus saadud teadmiste ja kogemuste talletamise, jagamise ja kasutamise.

§ 12. Teabe haldamine ja teabele juurdepääsu korraldamine

(1) Asutus tagab teabe säilimise ja kasutatavuse kuni üleandmiseni avalikku arhiivi või kuni hävitamiseni. Arhiiviseaduse § 2 lõigetes 1 ja 2 nimetatud teabe hoidmisel, üleandmisel ja hävitamisel lähtub asutus arhiiviseaduse § 13 alusel kehtestatud määrusest (edaspidi *arhiivieeskiri)* ja arvestab arhiiviseaduse § 6 lõike 5 alusel antud Rahvusarhiivi juhiseid.

(2) Teavet võib infosüsteemis sisestada, kasutada või muul viisil töödelda isik, kellel on asjakohased õigused ja kelle isikusamasus on tuvastatud. Teabe loomine ja haldamine peab olema kirjeldatud ja auditeeritav ning tagama teabe kvaliteedi.

(3) Enne teabe ülekandmist uude infosüsteemi vaatab asutus üle teabe säilitustähtajad. Üle ei kanta teavet, mille säilitustähtaeg on möödunud ja teavet, mida asutused enam ei vaja. Aegunud ja mittevajalik teave hävitatakse. Üle kantavale teabele määratakse säilitustähtajad.

(4) Infosüsteemi väljatöötamisel või arendamisel luuakse tehnoloogilised ja organisatoorsed tingimused, mis võimaldavad isikule ülevaate sellest, kes ja millal tema isikuandmeid infosüsteemis kasutab.

(5) Teabele juurdepääsu võimaldamisel ning isikuandmete ja muu teabe kaitse korraldamisel lähtub asutus avaliku teabe seadusest ja isikuandmete kaitse seadusest ning arvestab avaliku teabe seaduse § 45 lõike 4 ja isikuandmete kaitse seaduse § 35 lg 1 punkti 5 alusel antud Andmekaitse Inspektsiooni juhiseid. Dokumendile juurdepääsupiirangu kehtestamisel arvestab asutus ka riigi infosüsteemi haldussüsteemis (edaspidi *RIHA*) registreeritud juurdepääsupiirangu aluste klassifikaatorit.

(6) Asutus avalikustab oma veebilehel kasutajasõbraliku teabe:
1) isikuandmete töötlemise kohta asutuses;

2) juurdepääsu kohta asutuse taaskasutamiseks antud teabele ja teabe taaskasutamise eest võetava tasu kohta.

(7) Asutus avalikustab eesti.ee teabeväravas oma tegevusvaldkonda ja avalikke teenuseid kirjeldava teabe kooskõlas avaliku teabe seaduse § 32^1 lõike 1 alusel kehtestatud määrusega.

(8) Kui asutus haldab infosüsteemi, milles loovad teavet teised asutused, vastutab ta teabe säilimise, kasutatavuse ja kaitse, teabe avalikku arhiivi üleandmise või hävitamise ning teabele juurdepääsu võimaldamise eest.

§ 13. Teabe jagamine ja vahetamine

(1) Asutus tagab, et tööülesande täitmiseks vajalik teave on ametnikule või töötajale lihtsasti leitav. Teave esitatakse kasutajarühma vajadustest lähtuval viisil ja mahus.

(2) Asutused teevad koostööd, et teavet jagada ja kasutada kvaliteetsete teenuste osutamiseks.

(3) Dokumentide vahetamine asendatakse võimalusel dokumentides sisalduvate andmete vahetamisega.

(4) Asutused vahetavad omavahel dokumente elektrooniliselt, välja arvatud juhul, kui edastamisele kuulub enne määruse jõustumist loodud mahukas paberdokument või -toimik.

(5) Põhiseaduslikud institutsioonid, valitsusasutused ja kohaliku omavalitsuse asutused ning võimalusel teised avalikke ülesandeid täitvad asutused ja isikud vahetavad elektroonilisi dokumente X-teel asuva asutustevahelise dokumendivahetussüsteemi (*edaspidi* DVK) kaudu. Koos dokumendiga edastatakse dokumendi metaandmed, mis vastavad RIHA XML varade registris registreeritud dokumendivahetuse metaandmete loendile.

(6) DVK haldamise ja arendamise korraldab ning ja DVK häireteta töö tagab Riigi Infosüsteemi Amet. DVK asendamisel alternatiivse X-tee dokumendivahetuslahendusega töötab lahenduse välja ja korraldab selle juurutamise Riigi Infosüsteemi Amet. Dokumendivahetuse järjepidevuse tagamiseks vajalikud ressursid näeb ette Majandus- ja Kommunikatsiooniministeerium.

§ 14. Teabe või dokumendi saatmine isiku ametliku e-posti aadressi kaudu

(1) Kui asutusest väljasaadetava ametliku teabe või dokumendi adressaadiks on isik, kes on aktiveerinud oma ametliku e-posti aadressi eesti.ee teabeväravas ja ei ole konkreetse menetlusega seotud teabevahetuseks esitanud teisi kontaktandmeid, saadab asutus isiku ametlikule e-posti aadressile teate teabe või dokumendi edastamise kohta. Teade peab sisaldama linki, mille kaudu isik saab sisse logida veebikeskkonda ja seal pärast autentimist ja autoriseerimist teavet või dokumenti lugeda.

(2) Kui asutusel puudub lõikes 1 nimetatud teabe või dokumendi kättetoimetamiseks turvaline veebikeskkond, edastab ta dokumendi eesti.ee teabevärava ametlike dokumentide infrastruktuuri teenuse (edaspidi *isiku ametlik postkast)* kaudu. Teade dokumendi isiku ametlikku postkasti edastamise kohta saadetakse isikule eesti.ee teabeväravast.

(3) Asutus võib isiku ametliku e-posti aadressile saata saata ka meeldetuletusi ja muid teateid, mis tulenevad asutusele pandud avaliku ülesande täitmisest. Avaliku ülesande täitmisega mitte seotud teateid, eriti reklaami, asutus isiku ametliku e-posti aadressile ei saada.

(4) Ametliku e-posti aadresside aktiveerimise toimimise ning isiku ametliku postkasti haldamise ja arendamise korraldab ja häireteta töö tagab Riigi Infosüsteemi Amet. Selleks vajalikud ressursid näeb ette Majandus- ja Kommunikatsiooniministeerium.

§ 15. Nõuded dokumentidele

(1) Dokumendil on kohustuslikud elemendid ja lisaks nendele dokumendi liigile omased elemendid. Dokumendi kohustuslikud elemendid on:
1) autor;
2) kuupäev;
3) sisu;
4) allkirjastaja või sisu kinnitaja või märge asutuse automaatse kinnituse kohta.

(2) Dokumendi elementide koosseis lähtub vastava dokumendiliigi andmekirjeldusest, kui see on RIHA XML varade registris registreeritud. Sellist liiki dokumendi ja selle veebivormide koostamisel võetakse aluseks andmekirjeldus.

(3) Dokumendi tekst peab olema üheselt arusaadav ja võimalikult lühike ning vastama eesti kirjakeele normile.

(4) Dokument võib olla allkirjata, kui allkirja nõue ei tulene õigusaktist ning dokumendi autentsus, usaldusväärsus ja terviklus on tagatud.

§ 16. Dokumendihalduse korraldamine

(1) Dokumentide haldamisele ja neile juurdepääsu korraldamisele kehtivad §-s 12 teabele sätestatud nõuded, arvestades käesoleva paragrahvi erisusi.

(2) Dokumentide jagamisele, vahetamisele ja isiku ametliku e-posti aadressile saatmisele kehtivad §-des 13 ja 14 sätestatud nõuded, arvestades käesoleva paragrahvi erisusi.

(3) Asutus loob, kooskõlastab ja menetleb dokumente elektrooniliselt. Kui dokument on vaja väljastada paberkandjal ja kui õigusaktiga ei ole sätestatud teisiti, võib asutus väljastada elektroonilise dokumendi paberkandjal koopia.

(4) Asutus skaneerib saadud paberdokumendi. Dokumendi originaal tagastatakse selle esitajale või saatjale või hävitatakse, kui õigusaktiga ei ole sätestatud teisiti ja kui teabe ülekandmine elektroonilisele teabekandjale toimus arhiivieeskirjas sätestatud korras.

(5) Asutus talletab rohkem kui 10-aastase säilitustähtajaga ja võimalusel ka teised elektroonilised dokumendid arhiivivormingus. Menetlemise tagamiseks või muu vajaduse korral hoiab asutus lisaks alal muus vormingus versiooni.

(6) Dokument hoitakse alal koos dokumenti, selle seoseid ja haldamise ajalugu kirjeldavate metaandmetega. Dokumendi metaandmed peavad olema kooskõlas RIHA XML varade registris registreeritud dokumendihalduse metaandmeloendi ja dokumendi liigi andmekirjeldusega.

(7) Asutus avalikustab juurdepääsupiiranguta elektroonilised tekstidokumendid ja paberdokumentide skaneeritud koopiad dokumendiregistri kaudu PDF vormingus või muus rakendustarkvarast sõltumatus vormingus inimloetaval kujul.

(8) Riigiasutused võivad anda rohkem kui 10-aastase säilitustähtajaga elektroonilised dokumendid, mis arhiiviväärtust ei oma, säilitamiseks Rahvusarhiivi. Rahvusarhiiv tagab üleandnud asutuse juurdepääsu dokumentidele. Dokumentide üleandmise ja säilitamisega seotud

kulud katab dokumente üle andev asutus kulunormide alusel, mille kehtestab arhiivinduse valdkonna eest vastutav minister.

(9) Asutus tagab, et RIHAs on ajakohased ja tõesed andmed selle kohta, millist dokumendihaldussüsteemi või -süsteeme ta oma dokumentide haldamisel või hoidmisel kasutab.

§ 17. Täiendavate nõuete kehtestamine teabehaldusele

(1) Käesolevas peatükis sätestatu täpsustamiseks võib anda juhiseid koordineerija või muu pädev asutus. Kui õigusakti või juhise rakendamise üksikküsimuses on vaja kokku leppida ühetaoline toimimisviis, teeb otsuse § 5 lõike 4 alusel tegutsev nõukogu.

(2) Asutus kehtestab ja hoiab ajakohasena korrad, milles sätestatakse nõuded teabe kvaliteedi tagamise, teabe hoidmise, jagamise ja kaitse, teabele juurdepääsu võimaldamise ning teabe hävitamise ja avalikku arhiivi või teenusepakkujale üleandmise kohta. Asutus toetab kordade täitmist infotehnoloogiliste vahendite abil.

5. peatükk
RAKENDUSSÄTTED

§ 18. Määruse rakendamine

(1) Asutus määrab § 4 lõigetes 2 ja 3 sätestatud ameti- või töökohad ja vastutavad isikud hiljemalt 1. jaanuariks 2017. a.

(2) Asutus koostab § 7 lõikes 1 sätestatud ülevaate ja korrastab oma teabe §-s 11 kirjeldatud viisil hiljemalt 1. juuliks 2017. a.

(3) Asutus koostab ja avalikustab §-s 8 sätestatud avalike teenuste loetelu:
1) elektrooniliste kanalite kaudu osutatavate avalike teenuste osas hiljemalt 1. märtsiks 2016;
2) kõigi avalike teenuste osas hiljemalt 1. juuliks 2017. a.

(4) Asutus avalikustab juurdepääsupiiranguta elektroonilised tekstidokumendid § 16 lõikes 7 nimetatud vormingutes hiljemalt alates 1. juulist 2017. a.

(5) Asutus viib oma sisemist töökorraldust reguleerivad aktid määruse nõuetega vastavusse ja kehtestab § 17 lõikes 2 nimetatud korrad hiljemalt 1. juuliks 2017. a.

(6) Asutus edastab isikutele teavet ja dokumente § 14 lõigetes 1 ja 2 sätestatud viisil hiljemalt alates 1. juulist 2017. a.

(7) Asutus tagab § 9 lõigetes 2 ja 3 sätestatud nõuete täitmise hiljemalt 1. jaanuariks 2019. a.

(8) Vabariigi Valitsuse 26. veebruari 2001. a määruse nr 80 „Asjaajamiskorra ühtsed alused“ § 54^2 lõike 1 alusel antud juhiseid järgitakse kuni juhiste uuendamise või kehtetuks tunnistamiseni.

(9) Majandus- ja Kommunikatsiooniministeerium vaatab käesoleva paragrahvi lõikes 6 nimetatud juhised läbi hiljemalt 1. juuliks 2017. a ja vajadusel uuendab need või tunnistab kehtetuks.

(10) Vabariigi Valitsuse 26. veebruari 2001. a määruse nr 80 „Asjaajamiskorra ühtsed alused“ § 54^2 lõike 1^1 alusel moodustatud dokumendihaldusnõukogu jätkab tegevust dokumendihalduse arengut toetava nõukoguna käesoleva määruse §-s 5 sätestatud korras.

§ 19. Vabariigi Valitsuse 22. detsembri 2011. a määruse nr 181 „Arhiivieeskiri“ muutmine

Vabariigi Valitsuse 22. detsembri 2011. a määruse nr 181 „Arhiivieeskiri“ § 39 tekst muudetakse ja sõnastatakse järgmiselt:

„Avalikud arhiivid rakendavad käesoleva määruse §-de 32–36 nõudeid kõigile avalikku arhiivi üleantud dokumentidele juurdepääsu tagamisel, välja arvatud arhiiviseaduse § 6 lg 2 alusel antud Vabariigi Valitsuse määruse § 16 lõikes 8 nimetatud dokumentidele juurdepääsu korraldamisel.“.

§ 20. Vabariigi Valitsuse 19. detsembri 2001. a määruse nr 417 „Eesti Töötukassa põhikiri“ muutmine

Vabariigi Valitsuse 19. detsembri 2001. a määruse nr 417 „Eesti Töötukassa põhikiri“ § 5 lõige 1 muudetakse ja sõnastatakse järgmiselt:

„(1) Töötukassa dokumente hallatakse kooskõlas arhiiviseaduse ja selle alusel kehtestatud õigusaktidega.“.

§ 21. Vabariigi Valitsuse 25. juuni 2002. a määruse nr 204 „Tagatisfondi põhikiri“ muutmine

Vabariigi Valitsuse 25. juuni 2002. a määruse nr 204 „Tagatisfondi põhikiri“ § 3 lõige 1 muudetakse ja sõnastatakse järgmiselt:

„(1) Fondi dokumente hallatakse kooskõlas arhiiviseaduse ja selle alusel kehtestatud õigusaktidega.“.

§ 22. Määruse kehtetuks tunnistamine

Vabariigi Valitsuse 26. veebruari 2001. a määrus nr 80 „Asjaajamiskorra ühtsed alused“ tunnistatakse kehtetuks.

§ 23. Määruse jõustumine

Määrus jõustub 1. veebruaril 2016.

Taavi Rõivas
peaminister

Kristen Michal
majandus- ja taristuminister

Heiki Loot
riigisekretär

LISA 2 Vabariigi Valitsuse määruse „Teenuste korraldamise ja teabehalduse alused“ eelnõu seletuskiri. Väljavõte paragrahvist 12

Vabariigi Valitsuse määruse „Teenuste korraldamise ja teabehalduse alused“ eelnõu seletuskiri

Paragrahvis 12 on teabe haldamise ja teabele juurdepääsu korraldamise nõuded. Need keskenduvad peamiselt teabe kvaliteedile, säilimisele ja kasutatavusele, selle kaitsele volitamata kasutamise eest ja selle avalikustamisele.

Lõikes 4 on veel üks nõue, millega uute infosüsteemide loomisel ja olemasolevate arendamisel arvestada. Nõue on seotud infoühiskonna arengukava 2020 meetme 5.3.1 „Paremate avalike teenuste arendamine IKT abil“ tegevusega 2b, mis näeb ette, et inimestele luuakse lihtsad võimalused jälgida, kas, kes ja milleks on nende isikuandmeid riigi infosüsteemis kasutanud. Et isikule saaks sellist teavet anda kogu riigi infosüsteemi ulatuses, on vaja, et iga üksik infosüsteem seda toetaks. Sealjuures tähendab sättes nimetatud organisatoorsete tingimuste loomine, et asutus peab olema valmis vastama päringutele selle kohta, mis eesmärgil isikuandmeid on vaadatud või muul moel kasutatud.