Analüüs

Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile

Monika Mikiver

Justiitsministeerium

2021

Sisukord

Sisukord

Sissejuhatus

Eesti esimese isikuandmete kaitse seaduse eelnõu menetlemisel Riigikogus 1995.aastal selgitas P.Aimla, et „Me elame tehnika järsu, kiire murrangu ajastul, meie andmeid on mitte ainult rätsepal ja Magdaleena haiglas, vaid Tolliametis ja ka Passiametis ja jumal teab missuguses SIA-s[1] veel. Inimene vajab oma põhiseaduslike õiguste kaitsmiseks lihtsalt täpsemat süsteemi, mis aitaks tema isiklikke andmeid ja tema au ning väärikust puudutavaid teateid, olgu siis arvulisi või verbaalseid, hoida teiste jaoks varjatult. Seda seadus tahabki teha. /---/ see on vajalik iga Eesti inimese andmete kaitseks, st põhiseaduslike õiguste kaitsmiseks /---/.“[2]

Aastal 2021 räägime samuti tehnika kiire murrangu ajastust, pidades silmas uute tehnoloogiate, tehisintellekti arengut. Kunstmõistus on võimeline märkama suurtest andmehulkadest mustreid ning prognoosima inimeste edasisi samme, ka ohtlikke tegevusi. Et andmetest rohkem informatsiooni kätte saada, on tekkinud kiusatus koondada neid suurtesse andmeladudesse. Konkreetse inimese kohta käivad andmed puudutavad selle inimese põhiõigusi. Lisaks sellele, et andmed oleks kaitstud, peab olema tagatud ka andmete töötlemise läbipaistvus.

Andmekaitse Inspektsioon (AKI) on märkinud juba aastate eest, et seadusandja ei ole andmekogudega seonduvat põhiõiguste riivet vajalikul määral teadvustanud, sest „väga tihti sisaldubki seaduses vaid üks säte, mis delegeerib andmekogu asutamise koos sinna kantavate andmete koosseisu loetelu kehtestamise ja andmekogu pidamise korra kehtestamisega täitevvõimule“.[3] AKI tõdes, et „[k]ahjuks on see väga levinud praktika, et seaduses küll nimetatakse ära, et andmekogu asutatakse, kuid andmekogusse kantavate andmete koosseisu kindlaks määramine on jäetud täitevvõimu pädevusse. Oleme nõus, et seaduse tasandil ei pea üksikasjalikult ära loetlema kõiki andmeid, kuid **inimesel peaks olema võimalik seadust lugedes aru saada, mis liiki andmeid ja milleks tema kohta kogutakse, kaua neid säilitatakse ning milleks veel võidakse kasutada“.**

2005.a rõhutas toonane õiguskantsler, et „[t]undub iseenesestmõistetav, et inimese iga kokkupuude riigiga tuleks jäädvustada, salvestada andmed andmekogudesse, et oleks hea mitu aastat hiljemgi neid andmeid kasutada, võrrelda andmeid teistes andmekogudes hoitavatega jne.“.[4] Õiguskantsler tõdes, et „ulatuslikud andmekogud ning moodsad infotöötlemise vahendid muudavad ametnike ja poliitikute töö märksa hõlpsamaks. Seejuures ei teadvustata aga kahjuks, et isikuandmete töötlemisega riivatakse inimeste põhiõigusi, milleks on meie põhiseadusest tulenevalt vaja seadusandjalt väga **selgeid volitusi**.“.[5]

On tõsi, et Eesti e-riigi edukusele on olulisel määral kaasa aidanud andmekogudes olevate andmete ulatuslik ristkasutus. Erinevate andmekogude andmete koondamisel on võimalik luua suuremas või väiksemas ulatuses isiksuse profiile, ilma, et puudutatud isik andmete õigsust ja nende edasist kasutamist piisaval määral kontrollida saaks. Inimene, kes enam ei tea, milliseid tema andmeid salvestatakse ja millistel eesmärkidel neid (veel) kasutatakse, võib hakata oma

[1] SIA all on silmas peetud 1995.aastal toimunud nn lindiskandaali.

[2] [2] VIII Riigikogu, II Istungjärk, täiskogu korraline istung
, 08.11.1995, stenogramm 5. Isikuandmete kaitse seaduse eelnõu teine lugemine: https://stenogrammid.riigikogu.ee/et/199511081400?phrase=%22isikuandmete%20kaitse%20seadus&type=ALL&fbclid=IwAR3mfYwf-Qri1sxzle2OJmquxQmRVL0DF0LYcp4GWeKNuexSRtIdCasgFo0

[3] Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2011. Tallinn: Andmekaitse Inspektsioon 2012, lk 61. Arvutivõrgus: http://www.aki.ee/et/inspektsioon/aastaettekanded.

[4] Õiguskantsleri 2005. aasta tegevuseülevaade. Tallinn 2006, lk 87. Arvutivõrgus: http://oiguskantsler.ee/sites/default/files/6iguskantsleri_2005._aasta_tegevuse_ylevaade.pdf

[5] Samas, lk 88.

vabadusi ise piirama, proovides mitte üldisest normist erinevalt silma paista ja loobuda ka mõnede teiste põhiõiguste ja -vabaduste teostamisest. Inimeste kaitse nende teadmata toimuva andmetöötluse eest on seetõttu nii eraelu puutumatuse (sh informatsioonilise enesemääramisõiguse) kui ka inimväärikuse küsimus. Seetõttu on oluline, et inimeste jaoks oleks selge, kes ja milleks tema andmeid riigis töötleb.

25.05.2018 jõustunud isikuandmete kaitse üldmäärus (IKÜM) soovis EL seadusandja anda inimestele tagasi kontrolli oma andmete üle, pidades oluliseks isikuandmete töötlemise läbipaistvuse põhimõtet (vrd IKÜM art 5 lg 1 p a, art-d 12 jj). Ka Eestis kehtestati isikuandmete kaitse rakendamise seaduse vastuvõtmisega mitmeid EL andmekaitseõiguse reformi eesmärke teenivaid sätteid eriseadustes, ent toona ei analüüsitud põhjalikumalt isikuandmete töötlemisega andmekogudes seonduvaid küsimusi. Et Eesti e-riik põhineb oluliselt andmekogudel ja ka andmete ulatusliku ristkasutamise põhimõttel, otsustas Justiitsministeerium põhjalikumalt analüüsida IKÜM-st tulenevaid põhimõtteid just andmekogude kontekstis. Vähetähtis ei ole seejuures, et isikuandmete töötlemisel tuleb tagada inimeste põhiõiguste kaitse. Informatsioonilise enesemääramise põhiõigus eeldab õigusselguse põhimõttele vastavaid regulatsioone, mis austavad ka inimväärikust ja lähtuvad proportsionaalsuse põhimõttest. Analüüsi eesmärk on veenduda, et innovaatilisi digilahendusi ei rakendataks põhiõiguste arvelt ning esitada vajadusel soovitused ja ettepanekud. Põhiseadusest lähtuvalt saame rääkida ühiskondlikkust kokkuleppest meie isikuandmete kasutamiseks riigi poolt[6] vaid tinglikult, pigem tuleb sõnastada kriteeriumid, mille olemasolu korral on isikuandmete salvestamine andmekogudes ja nende edasine kasutamine põhiseaduspärane.

1. Ülevaade andmekoguõiguse ajaloolisest kujunemisest

1.1. 1990.a Eesti NSV riiklike registrite seadus

1990 võeti vastu esimese andmekogude regulatsioonina „Eesti Nõukogude Sotsialistliku Vabariigi riiklike registrite seadus“.[7] Riikliku registrina käsitleti andmekogumit, mis sisaldab reglementeeritud andmeid kõikide objektide kohta täpselt määratletud kategooria piires.[8] Riikliku registri asutamise ja pidamise eesmärk oli koguda ja säilitada usaldusväärset teavet teatud kategooria objektide täieliku hulga kohta, et seda saaks kasutada riigivõimu- ja -valitsemisorganite tegevuses ja muudel käesolevas seaduses ettenähtud juhtudel.[9] Registrid jagunesid territoriaalsust silmas pidades vabariiklikeks ja kohalikeks registriteks.[10]

Vabariikliku registri asutamiseks tuli esitada taotlus Eesti NSV Ülemnõukogu Presiidiumile või Eesti NSV Valitsusele, lisades registri põhimääruse projekti; Eesti Informatsiooninõukogu arvamus registri andmete koosseisu, nende kogumise ja kasutamise aluste otstarbekuse kohta ja registri eelarve projekti.[11] **Kui registrisse kavandati koguda isikuandmeid, anti asutamisluba**

[6] https://www.err.ee/1608337208/kersti-kaljulaid-eestile-on-vaja-riigikogu-kui-teenaitajat
[7] ÜVT 1990, 3, 61. Kehtetu alates 19.04.1997.
[8] Riiklike registrite seaduse art 1 lg 2.
[9] Art 2.
[10] Art 3 lg 1.
[11] Art 5 lg 1.

Eesti NSV seadusega, muudel juhtudel Eesti NSV Valitsuse määrusega. Registri põhimääruses tuli sätestada andmete koosseis, nende kogumise ja kasutamise alused, andmete uuendamise kord ja sagedus, registri pidamise finantseerimise kord ning muud registriga seotud küsimused. Kui tekkis vajadus hakata registrisse koguma täiendavaid andmeid, tuli selleks saada luba samas korras kui registri asutamise puhul.[12] Andmetöötluse läbipaistvust teenis registripidaja kohustus teha riikliku registri andmete koosseis ja kasutamisviis avalikkusele ajakirjanduse kaudu teatavaks.[13]

On tähelepanuväärne, et ajal, mil Eestis polnud veel isikuandmete kaitse seadust, oli riiklike registrite seaduses arvestatud mitmete **andmekaitse üldtunnustatud põhimõtetega**. Nii nägi seadus ette kohustuse kaitsta andmeid volitamata juurdepääsu, kavatsematu või muu seadusevastase töötluse, kasutamise, muutmise või hävitamise eest.[14] Isikuandmete eesmärgipiirangu põhimõte väljendus sättes, mis keelas kasutada riiklikus registris sisalduvaid andmeid eesmärkidel, mis on vastuolus Eesti NSV konstitutsiooni, Eesti NSV muu seadusandluse ning registri põhimäärusega.[15] Andmeid võidi põhimääruses sätestatud juhtudel anda üle tööalaseks kasutamiseks, kuid sel juhul oli lubatud neid andmed kasutada ainult eesmärkidel, mis määrati kindlaks andmete üleandmisel.[16]

Andmete kasutamise logimisena võib käsitleda sätet, mis nägi ette, et andmed kõikide isikute kohta, kellele on riikliku registri andmeid antud, säilitatakse registri arhiivis.[17]

1.2. 1997.a andmekogude seadus

1.2.1. Ülevaade

1997.a võeti vastu andmekogude seadus[18] (AKS), mis asendas senise 1990.a Eesti NSV riiklike registrite seaduse. Uue seaduse vastuvõtmist põhjendati praktilise vajadusega võtta kasutusele uus, Eesti Vabariigi riigivalitsemise struktuuril põhinev regulatsioon, mis arvestaks infotöötluse tehnoloogia arengust tulenevaid nõudeid.[19] AKS defineeris andmekoguna riigi, kohaliku omavalitsuse, avalik-õigusliku või eraõigusliku isiku peetava korrastatud andmete kogumi, mille pidamisel kasutatakse automatiseeritud andmetöötlust või mida peetakse käsitsi ja korrastatud vormidel, mis võimaldavad andmetega lihtsat tutvumist või nende mehhaanilist töötlemist.[20]

Riigi andmekogude liigid olid:

1) riigi põhiregister;
2) riiklik register;
3) riigiasutuste peetavad muud andmekogud.[21]

---

[12] Art 5 lg 2 ja 3.
[13] Art 7.
[14] Art 12 lg 2.
[15] Art 13 lg 2.
[16] Art 14 lg 2.
[17] Art 14 lg 3.
[18] RT I 1997, 28, 423; RT I 2007, 12, 66. Kehtetu alates 01.01.2008.
[19] Andmekogude seadus 79 SE. Seletuskiri Riiklike registrite seaduse eelnõu juurde, lk 1.
[20] AKS § 2 lg 1. AKS §-d 18 ja 19 sätestasid järgmised riigi andmekogude liigid: riigi põhiregister; riiklik register; riigiasutuste peetavad muud andmekogud ning kohalike andmekogudena kohaliku omavalitsuse registrid ja kohaliku omavalitsuse muud andmekogud.
[21] AKS § 18 lg 2.

Kohaliku omavalitsuse andmekogud jagunesid kohaliku omavalitsuse registriteks ja kohaliku omavalitsuse muudeks andmekogudeks.[22]

Riigi põhiregister oli seadusega asutatud avalikuks kasutamiseks määratud andmekogu, mida peeti üldistes huvides riigi kõige olulisemate ülesannete täitmiseks (näiteks riigi rahvastiku, riigis registreeritud juriidiliste isikute, kinnisvara, riigivara ja muude oluliste objektide kohta).[23] Riigi põhiregister asutati tema kohta käiva seadusega või anti mõne muu seadusega loodud registrile riigi põhiregistri staatus.[24] **Riiklik register** oli Vabariigi Valitsuse poolt seaduse või välislepingu alusel asutatud ühe või mitme ministeeriumi seaduse kohaste ülesannete täitmiseks vajalik andmekogu. Riikliku registri asutas Vabariigi Valitsus määrusega,[25] asutamise kohta andis arvamuse ka andmekaitse järelevalveasutus.[26] **Riigiasutuse andmekogu** oli riigiasutusele seaduse või muu õigusaktiga pandud ülesannete täitmiseks või riigiasutuse töö korraldamise tagamiseks vajalik andmekogu. Riigiasutusele seaduse või muu õigusaktiga täitmiseks vajaliku andmekogu asutamise otsustab riigiasutuse juht. Riigiasutuse andmekogu asutab riigiasutuse juht või tema poolt volitatud ametiisik.[27] Sellest tuli teavitada ka Andmekaitse Inspektsiooni ning vajadusel (nt delikaatsete isikuandmete töötlemisel) saada luba selleks.[28]

1.2.2. Ristkasutuse regulatsioon ja dubleerivate andmekogude keeld

Andmete ristkasutust defineeriti §-s 2 järgmiselt:

(7) Andmete ristkasutus on andmete ülekandmine ühest andmekogust teise või mitmes andmekogus sisalduvate andmete ühine infotehnoloogiline töötlemine.

Ristkasutus oli lubatav ainult seaduses või määruses selgelt ette nähtu juhul, lisaks vajas see AKI luba ning kaaluda tuli ka eraelu puutumatuse põhiõigust:

§ 12. Andmete ristkasutus

(1) Riigi või kohaliku omavalitsuse eri andmekogudes säilitatavate andmete ristkasutus on lubatud ainult seaduses või seaduse alusel vastuvõetud õigusaktis sätestatud juhtudel ja ainult riigile või kohalikule omavalitsusüksusele seadusega pandud ülesannete täitmiseks.

(2) Isikuandmete ristkasutus on lubatud ainult andmekaitse järelevalveasutuse loal ja juhul, kui see ei riku isiku perekonna- ja eraelu puutumatust.

Eelnõu algses Riigikogule esitatud versioonis sisaldus regulatsioon, milles eristati andmekogu andmete väljastamist püsiva vajaduse olemasolul olukorrast, kus andmeid vajati pigem erijuhtumil. Vastu võetud seaduses seda sätet enam ei olnud.

§ 17. Andmete väljastamise kord

[22] AKS § 19 lg 2.
[23] AKS § 25 lg 1.
[24] AKS § 26 lg 1.
[25] AKS § 31, 32 lg 1.
[26] AKS § 32 lg 5.
[27] AKS § 38, 39 lg 1. Riigi ja kohaliku omavalitsuse andmekogudes peetavad andmed on avalikud ning igal Eesti kodanikul on õigus nendega seaduses sätestatud korras tutvuda ja neist ärakirju saada, välja arvatud juhul, kui seadusega on andmetega tutvumine võiandmete väljastamine keelatud või need on ette nähtud ainult ametialaseks kasutamiseks. Kui seadus ei sätesta teisiti, siison käesolevas lõikes nimetatud õigus võrdselt Eesti kodanikugaka Eestis viibival välisriigi kodanikul ja kodakondsusetaisikul. AKS § 10 lg 2.
[28] AKS § 40 lg 2.

(1) Andmeid väljastatakse registrist andmekandjal või andmesidevahenditega registri põhimäärusega kehtestatud korras ja selles nimetatud andmesaajatele.

(2) Registri põhimääruses nimetamata andmesaaja peab registrist andmete saamiseks esitama registri haldajale taotluse, milles on märgitud, milliseid andmeid ja milleks soovitakse saada ja kuidas on korraldatud andmekaitse.

Andmekogude seadusega **keelati riigiasutustel pidada sarnaseid ja teineteist sisuliselt kordavaid andmekogusid**.[29] Seletuskirjas põhjendati seda asjaoluga, et „[m]ajanduslikel kaalutlustel on vaja ka sätestada, et ei asutataks riiklikke registreid kordavaid riigiasutuste registreid ja andmebaase.“[30] Seejuures lisati, et „[o]luline on see ka andmekaitse seisukohalt“[31], kuid rohkem seda ei põhjendatud.

Üks eelnõu aluspõhimõtteid oli muuhulgas, et „andmed, s.o. informatsioon on üks riigivaradest“.[32] Andmekogude seaduse esialgses Riigikogule esitatud eelnõus oli sätestatud, et „[r]egistriobjekti kohta registris peetavad andmed on riigi omand.“[33] Eelnõu menetlemisel Riigikogus soovis J.Adams saada rohkem selgust, mida selle all on silmas peetud, küsides: „Kas näiteks andmed Eestis kehtivate õigusaktide kohta saaksid olla riigi omand? Või andmed näiteks kõrgetasemelise patendivoliniku kohta, alates tema nimest ja lõpetades tema ülikooli lõpetamise kraadiga? Kuidas saab seda kuulutada riigi omandiks?“.[34] Küsimusele vastas R.Kasemaa:[35] „Tõepoolest, õigusakt on objekt ja ka isik on nendel juhtudel objekt. Andmetega on asi keerulisem. Kas need on riigi omand? Ma ütleksin niimoodi, et pigem on riigi omand see informatsioon, mis sinna registrisse on salvestatud. Isiku nimi ei muutu sellepärast riigi omandiks, vaid see informatsioon on riigi omand. Vähemalt mina mõtlen nii ja nii mõtleb ka selle seaduse esitaja.“.[36]

Asjaolu, et registrites olev informatsioon oli plaanis kuulutada riigi omandiks, võib tõlgendada mitmeti. Ühelt poolt võis seda mõista selliselt, et sel viisil on riigil õigus andmekogusid omavahel tõhusamalt integreerida. Ka eelnõu seletuskirjas selgitati: „Rahvastikuregister on isikukeskne, kuid hõlmab informatsiooni peale tema enda andmete veel perekonnaseisu andmeid, elukoha andmeid, ehitus- ja hoone andmeid, kinnistuandmeid, jne. Võib arvata, et ka meil pärast seda, kui on andmetega täidetud ja kasutusele võetud rahvastikuregister, ehitusregister, hooneregister ja kinnisturegister, moodustub nendest integreeritud infosüsteem.“.[37] Teine võimalus seda mõista on eelnõu esialgses versioonis sisaldanud idee kontekstis, mille kohaselt oleks andmekogust andmete väljastamine olnud tasuline.[38] See idee leidis Riigikogu menetluse

[29] AKS § 20 lg 4.

[30] Andmekogude seadus 79 SE. Seletuskiri Riiklike registrite seaduse eelnõu juurde, lk 2

[31] Samas.

[32] Samas, lk 1.

[33] Andmekogude seadus 79 SE, algtekst, § 3 lg 3.

[34] VIII Riigikogu, II Istungjärk, täiskogu korraline istung, 08.11.1995, stenogramm 5. Riiklike registrite seaduse eelnõu teine lugemine.

[35] Toonane Riigiarvutuskeskuse direktor Raivo Kasemaa.

[36] VIII Riigikogu, II Istungjärk, täiskogu korraline istung, 08.11.1995, stenogramm 5. Riiklike registrite seaduse eelnõu teine lugemine.

[37] Andmekogude seadus 79 SE. Seletuskiri Riiklike registrite seaduse eelnõu juurde.

[38] Andmekogude seadus 79 SE, algtekst, § 23. Registrist andmete saamise eest tasumine
(1) Andmete saamme registrist on **tasuline**.
(2) Riigiasutused ja kohaliku omavalitsuse organid, kes on registri põhimääruses tähendatud andmesaajad, tasuvad registripidajale ainult nende teenindamisega seotud kulud, mille katteks tuleb ette näha summad oma

käigus teravat kritiseerimist, mh ka põhiseadusest tulenevalt.[39] Riigikogu menetluses jäetigi isikuandmete riigi omandiks lugemise säte seaduse tekstist siiski välja.

Selleks, et paremini tagada andmete dubleeriva kogumise keeldu, nähti ette, et Vabariigi Valitsus asutab riigi ja kohalike omavalitsuste andmekogude ning eraõiguslike isikute peetavate delikaatseid isikuandmeid sisaldavate andmekogude riikliku registri nimetusega "Andmekogude riiklik register". Andmekogude riikliku registri vastutavale töötlejale anti õigus teha Vabariigi Valitsusele ja andmekogude vastutavatele töötlejatele ning riigi infosüsteemide alaseid töid koordineerivale asutusele sarnaste ja teineteist sisuliselt kordavate andmekogude pidamise vältimiseks ettepanekuid andmekogu laiendamiseks, ühendamiseks või likvideerimiseks, andmete ristkasutuseks, andmetöötluse või andmehõive korrastamiseks.[40]

1.2.3. Andmekogude ristkasutus praktikas: probleemid ja lahendused

Riigikontroll avaldas 2001.a põhjaliku auditi, milles tõdeti, et enamik aastatel 1993-1999 loodud andmekogudest olid asutusekesksed ning erinevate andmekogude vahelist andmete ristkasutust Eestis praktiliselt ei toimunud. Selle peamiste põhjustena nägi Riigikontroll andmete halba ühilduvust andmekogude vahel, üheselt lahendamata tehnoloogilisi küsimusi ja ebapiisavatest andmeturbemeetmetest tulenevat kartust andmete terviklikkuse säilimise pärast. Riigikontroll nägi andmekogudevahelises suuremas koostöös nii avaliku halduse otsuste kvaliteedi tõusu kui ka olulist kokkuhoiuvõimalust.[41] Riigikontrolli aruandes on ühe probleemina välja toodud, et puuduvad andmekaitse standardid ristkasutuse jaoks, seda mõtet siiski täpsemalt avamata.[42] Riigikontroll rõhutas, et riigi põhiandmed peavad olema ristkasutatavad ja omavahel ühilduvad ning pani tollal infoühiskonna arendamise eest vastutavale Teede- ja Sideministeeriumil kohustuse „töötada välja programm andmekogude süsteemi optimeerimiseks ja neis olevate andmete kättesaadavuse ja kasutuskõlblikkuse tõstmiseks. Teha vastavad ettepanekud muudatuste tegemiseks andmekogude seadusesse.“.[43]

1999.a infoühiskonna aastaraamatus tõdetakse samas, et “[p]ositiivse poole pealt tuleb veel märkida, et registrite asutajad ning töötlejad on enam ja enam hakanud mõtlema registrite

---

eelarvetes. Kui andmesaajate teenindamise kulud on lülitatud registri pidamise eelarvesse, teenindatakse andmesaajaid nendele summadeie vastavas mahus.
(3) Ülejäänud andmesaajad tasuvad nende teenindamise eest **registri põhimääruses sätestatud korras.**
(4) Füüsilisel isikul on õigus saada registripidajalt tasuta teavet tema kohta peetavatest andmetest üks kord aastas.

[39] E. Nestor: „Teine probleem on seotud nende andmete tasulisusega. /---/ Riikliku registri seadusega ei saa peale panna ega mingisuguse põhimäärusega kohustada kedagi millegi eest maksma. See on põhiseaduse alusel nonsenss. Kui see on äri, siis keegi võib ju pidada registrit selle kohta, kui palju Eestis on blondiine, kui palju brünette ja pärast selle info eest raha võtta. See on riiklik register, see ei saa olla äriobjekt. Kui me neid andmeid kogume ja teame, et meie kohta kogutakse, siis see peab olema ka avalik. **Kõik peavad teadma, et on kogutud selliseid andmeid, nende andmete alusel on tuldud sellistele järeldustele. Mitte nii, et ma maksan ja siis ma saan teada, mis see on**.“. VIII Riigikogu, II Istungjärk, täiskogu korraline istung, 08.11.1995, stenogramm 5. Riiklike registrite seaduse eelnõu teine lugemine.

[40] AKS § 16 lg 4.

[41] Riigikontrolli kontrolliakt infosüsteemide arendusprojektide tulemuslikkuse kohta, 2001, lk 7.

[42] Riigikontroll 2001, lk 18.

[43] Riigikontroll 2001, lk 34.

omavahelisele koostööle e andmete ristkasutusele.".[44] Kõigi andmekogude omavaheliste juurdepääsude kaudu n-ö ühendamise idee käis 2000. aastal välja peaministri nõunik Linnar Viik. Põhjendustena toodi muuhulgas välja, et "suletud ja asutuse-kesksed andmebaasid on vaja **muuta avatuks ja orienteerida teenuseid pakkuvateks**. Infovahetus andmebaaside vahel on keeruline, ebamugav ja kallis. Unikaalsete tarkvaraliste liideste loomine on väga töömahukas. Seetõttu kasutatakse praegu sageli infovahetuseks paberit ja käsitsi tippimist.".[45]

2001.a tõdeti, et riigi registreid ja andmebaase reguleeriv 1997.a jõustunud andmekogude seadus on juba ajale jalgu jäänud, sest"/---/ seadus ei võimalda efektiivselt juurutada uuemaid suundi andmetöötluses /---/.".[46] Ilmselt peeti silmas eeskätt ranget ristkasutuse regulatsiooni, mille kohaselt oli igaks juurdepääsu loomiseks (ristkasutuseks) vajalik eraldi seaduslik alus. Samal aastal nimetati ka ühe tähtsama arendusvaldkonnana riiklike registrite korrastamist ning nende ristkasutuse tagamist.[47] 2003.a sõnastati uue andmekogude regulatsiooni põhipostulaadid. Lähtekohaks oli taas andmekogude ulatuslik ristkasutus: „Peamine eesmärk on luua integreeritud registrite süsteem. Avaliku halduse jaoks oluline info peaks olema kättesaadav kas ühest kohast või ühtsest integreeritud ja andmete ristkasutuses olevast süsteemist. Infosüsteemide integreerimine avaliku halduse piires on aluseks võimalusele pakkuda uusi innovatiivseid avalikke elektroonilisi teenuseid. Integreeritud registrite süsteem võimaldab rakendada uusi halduskorralduse põhimõtteid: kodanikukeskus, paindlikkus, kiirus, väiksem raha- ja ajakulu nii kodanikule kui ka riigile." [48] Taas rõhutati, et ühe ametkonna poolt avalike ülesannete täitmiseks kogutavad andmed kuuluvad riigile tervikuna, mitte sellele ametile.[49]

Norm, mille kohaselt oli andmekogude ristkasutus lubatav ainult siis, kui see oli seaduses eraldi normiga sätestatud, kehtis siiski kuni 2008. aastani.

Praktikas esines sellegipoolest ka olukordi, kus ristkasutus loodi ilma selgesõnalise seadusliku aluseta. Näiteks tuvastas õiguskantsler 2007.a, et piirivalve infosüsteemi koguti alates 2003. aastast teavet järgmistest andmekogudest: sissesõidukeeldude riiklik register, ärandatud sõidukite andmebaas, infosüsteem POLIS ning Kodakondsus- ja Migratsiooniameti (KMA) väljaantavate isikut tõendavate dokumentide andmekogu.[50] Juurdepääsusildade loomine oli toimunud siseministri ja politseipeadirektori käskkirjade ning KMA ja Piirivalveameti vahel allkirjastatud isikuandmete üleandmise akti alusel.[51] Õiguskantsler rõhutas, et põhiseaduse § 3 lõike 1 esimesest lausest tuleneva halduse seaduslikkuse põhimõtte järgi ei saa sellist andmekogude

[44] Kaidi Oone. Õigusloome IT valdkonnas. RISO 1999.a aastaraamat.
[45] Uuno Vallner. Riigi andmekogude keskkiht. RISO 2000.a aastaraamat.
[46] Priit F. Lillemaa. IT-valdkonna õiguse areng 2001. Aastal. RISO 2001.a aastaraamat.
[47] Arvo Ott. Riigisektori IKT valdkonna arengutest 2001. Aastal. RISO 2001.a aastaraamat.
[48] Riina Kivi. Riigi andmekogude hetkeolukord ja Andmekogude seadus.
[49] Samas.
[50] Asi nr 7-4/070255. – Õiguskantsleri 2007. aasta tegevuse ülevaade. Tallinn 2008, lk 207.
[51] Politseiameti vastusest õiguskantslerile selgus, et andmekogust POLIS väljastati andmeid Piirivalveametile vastavalt siseministri 11.12.2003 käskkirjale nr 552 „Teabevahetuse korraldamine Politseiametilt Piirivalveametile". Piirivalveametile edastati tagaotsitavate ja teadmata kadunud isikute ning tagaotsitavate sõidukite andmed. Siseministri 11.12.2003 käskkiri nr 557 „Teabevahetuse korraldamine Kodakondsus- ja Migratsiooniametilt Piirivalveametile" paneb KMA-le kohustuse väljastada andmesidevõrkude vahendusel Piirivalveametile isikut tõendavate dokumentide andmeid. KMA ja Piirivalveameti vahel on 29.04.2004 sõlmitud isikuandmete üleandmise akt, mille järgi edastab KMA isikut tõendavate dokumentide andmekogust andmeid Piirivalveametile. Samas, lk 207–208.

seadusega vastuolus olevat andmete edastamise õigust luua andmekogu põhimääruse, siseministri käskkirja ega isikuandmete üleandmise aktiga, kui andmekogude seadus nõuab ristkasutuseks seaduslikku alust.[52]

1.3. 2000ndate algus, andmevahetuskiht X-tee ja infosüsteemide hajusa arhitektuuri põhimõte

Linnar Viigi poolt 2000.a välja pakutud kõikide andmekogude ühendamise ideest arendati välja tehniline lahendus, mis võimaldas ühel riigiasutusel kasutada teise riigiasutuse andmeid, ainult siis ja sel määral, mis on vajalik teisele riigiasutusele seadusega pandud avalike ülesannete täitmiseks, seejuures kõiki andmeid koondavat superandmebaasi loomata.[53] Sellise tehnilise lahenduse nimeks sai andmevahetuskiht X-tee. Riigi Infosüsteemi Amet tutvustab andmevahetuskihti X-tee järgmiselt: „Teabe vahetamiseks kirjeldab üks X-tee liige jagatavad andmed ning kõik teised liikmed saavad kokkuleppe alusel seda infot kasutada.“.[54] X-tee aluseks on **infosüsteemide hajus infrastruktuur, millest lähtuvalt andmeid ei tsentraliseerita**.[55] Andmed liigu-vad andmevahetuse käigus otse ametiasutuselt teisele ning tehniliselt on see võimalik nii üksnes andmete vaatamise, andmetest koopiate saamise kui ka jah/ei vastusega päringu kujul.[56]

Ka Riigi Infosüsteemi Ameti veebilehel on selgitatud, et riigi infosüsteemi hajus arhitektuur ja andmete ühte süsteemi koondamise vältimine oli teadlik valik: „Üks kõige suuremaid ohtusid riiklusele on andmete kontrollimatu kogunemine ühte keskses andmebaasi. Mainitud oht ilmnes esmakordselt 1930-ndate Saksamaal, kus imporditud kartoteegisüsteemid (sisuliselt infotehnoloogia) leidsid kasutust teatud rahvastikugruppide selekteerimisel ja hävitamisel [---]. Eestis realiseerus keskse andmebaasi oht aastal 1996, kui 26. septembri ETV Aktuaalses Kaameras demonstreeriti häkker Imre Perli loodud superandmebaasi.“.[57] Lisaks sellele, et superandmebaasi häkkimise korral on kahju palju suurem[58], võimaldab see üksnes paari hiireklikiga

[52] Vrd AKS § 33 p 4, § 35 p 8. Seetõttu oleks tulnud niipea, kui otsustati anda Piirivalveametile andmekogust POLIS ja KMA väljaantavate isikut tõendavate dokumentide andmekogust pärit andmetele püsiv juurdepääs, kujundada andmekogu ümber riiklikuks registriks, kust oleks olnud lubatud andmeid edastada ka teistele riigiasutustele, ning sätestada seaduses ka andmete ristkasutus. Õiguskantsleri viidatud puuduste kõrvaldamiseks töötati välja politseiseaduse ja mitmete muude seaduste muutmise seaduse eelnõu, mille Riigikogu võttis vastu 14.11.2007 ja mis jõustus 21.12.2007. Nimetatud seaduses nähti muuhulgas ette volitusnorm, millega antakse Vabariigi Valitsusele õigus asutada isikut tõendavate dokumentide register. Sama seadusega muudeti ka piirivalveseadust. 08.07.2007 jõustus politseiseaduse § 51, mille lg 1 järgi on politseil õigus töödelda oma ülesannete täitmiseks isikuandmeid ja asutada andmekogusid kooskõlas isikuandmete kaitse seadusega. Siseministri 03.10.2007 määrusega nr 66 kinnitati „Politsei andmekogu asutamine ja andmekogu pidamise põhimäärus“. Samas, lk 209–210.

[53] X-tee tehnoloogia võimaldab andmeteenuste pääsuõigusi hallata organisatsiooni ja infosüsteemi tasemel. See tähendab, et teenuse osutaja määrab, milliseid tema andmeteenuseid on teistel asutustel õigus kasutada. Lisapiiranguid ega -nõudeid kasutusõiguste haldusele X-tee ei sea, seega on kasutusõiguste haldus täielikult teenuse omaniku otsustada ning tema infosüsteemiga reguleeritav. Ka andmed, mida andmeteenuse osutaja X-tee kaudu jagab, on täielikult andmeteenuse osutaja kontrolli all. https://www.ria.ee/et/riigi-infosusteem/x-tee/miks-eelistada-x-teed.html.

[54] X-teel on mitmekülgne turvalahendus: autentimine, mitmetasemeline autoriseerimine, kõrgetasemeline logide töötlemise süsteem, krüpteeritud ja allkirjastatud andmeliiklus.

[55] Vt ka Majandus- ja Kommunikatsiooniministeerium. Eesti infoühiskonna arengukava 2020. Lk 7.

[56] https://www.ria.ee/et/riigi-infosusteem/x-tee/miks-eelistada-x-teed.html

[57] A. Veldre. Sissejuhatus X-teesse (osa 1). 28.08.2015.

[58] Samas: „Keskse andmebaasi risk on teada ka muudest riikidest, näiteks nimetame nn Andersoni reeglit – Cambridge’is resideeruv infoturbe professor Ross John Anderson järeldas, et keskne suur andmebaas, mida on

saada inimesest põhjaliku profiili, mis riivab ulatuslikult eraelu puutumatust. RIA blogis tõdetakse: „Ametlikult pole Imre Perli baasiga seotud andmeleket kunagi tunnistatud ega ole ka kedagi selle eest süüdi mõistetud, samas läks piinlik õppetund täie ette ning edaspidi on Eesti riigis üritatud keskseid andmebaase vältida“.[59]. Ka 25 aastat hiljem ei ole andmelekete oht kuskile kadunud.[60]

Kui X-tee idee ja arendusprojekti käivitamise võib dateerida 2000. aastasse, siis õiguslikus mõttes loodi X-tee Vabariigi Valitsuse 19.12.2003 määruse nr 331 „Infosüsteemide andmevahetuskihi rakendamine“,[61] milles sätestati, et infosüsteemide andmevahetuskiht (edaspidi X-tee) on turvalist internetipõhist andmevahetust võimaldav tehniline ja tehnoloogiline keskkond.[62] X-tee haldamist ja arendamist koordineerib ning X-tee tegevuse eest vastutab Majandus- ja Kommunikatsiooniministeerium, kes tagab turvalise andmevahetuse, juurdepääsu vaid autenditud kasutajale ning kasutaja poolt teostatavate toimingute jälgimise ja tuvastamise võimaluse.[63]

Asutustel jäeti esialgu X-teega liitumine vabatahtlikuks. Siiski sätestati kohustus tagada alates 1. märtsist 2004. a X-tee vahendusel juurdepääs vähemalt järgmiste asutuste andmekogudele/infosüsteemidele: Riiklik maanteeregister, Riiklik ehitisregister; Maksukohustuslaste register, piiriületuste andmekogu; Karistusregister, Riigi kohanimeregister, Viisaregister; tolli põhitegevuse infosüsteem ASYCUDA; Tööotsijate ja tööturuteenuste riiklik register; kinnistusraamatu päringusüsteem.[64] Teisi valitsusasutusi kohustati liituma X-teega hiljemalt 1. jaanuaril 2005. a.[65]

1.4. Haldusõigus ja andmete ühekordse kogumise põhimõte

1990ndate lõpus valmistati ette ka haldusõiguse reformi.

Andmete ühekordse küsimise põhimõte väljendus haldusmenetluse seaduse koostajate soovis koormata haldusmenetluses isikut võimalikult vähe. HMS § 5 lg 2 sätestab: „**Haldusmenetlus viiakse läbi eesmärgipäraselt ja efektiivselt, samuti võimalikult lihtsalt ja kiirelt, vältides üleliigseid kulutusi ja ebameeldivusi isikutele**.“. Ka „Haldusmenetluse käsiraamatu“ autorid tõdesid HMSi eesmärke selgitades, et „Piiratud on kodanikult nõutavate dokumentide hulka. Kui vähegi võimalik, peab otsuse tegemiseks pädev asutus suhtlema info kogumiseks teiste asutustega, mitte nõudma, et inimene esitaks teise asutuse käes olevate andmete kohta tõendeid. Seni oli tavaline, et kodanikku sunniti lubade ja muude soodustuste taotlemisel tööle riigiasutuste vahelise käskjalana. Tänapäeva infotehnoloogia võimaldab infot nt riigilõivu maksmise või äriregistrisse kantud andmete kohta edastada asutuste vahel ilma eriliste lisakuludeta, mistõttu kodaniku või ettevõtja jooksutamine on tarbetu.“[66]. Samas on tõdetud, et isikuandmete kaitse nõuded võivad omakorda seada piiri tõendite kogumisele uurimispõhimõtte raames.[67]

---

kerge kasutada, on ühtlasi ka kergesti kuritarvitatav. Kui kõrvaldada võimalused kuritarvitusteks, muutub keskne andmebaas paraku kasutamatuks.“.

[59] Samas.

[60] Vt H.Roonemaa. Kurikuulus häkker ähvardab riiki: ID-kaartide fotod lähevad tumeveebi, seniteadmata turvaaukude info häkkerite foorumitesse.Eesti Ekspress, 14-09.2021.

[61] https://www.riigiteataja.ee/akt/688079.

[62] Määruse § 2 lg 1.

[63] Määruse § 3 lg 1.

[64] Määruse § 9 lg 1.

[65] Määruse § 9.

[66] A.Aedmaa jt. Haldusmenetluse käsiraamat, lk 39.

[67] Samas, lk 184.

Seda, millised nõuded isikuandmete kaitse õigusest andmete jagamise suhtes kehtivad, haldusmenetluse käsiraamatus ei käsitletud.

1.4. Andmekogude regulatsiooni reform 2008 – avaliku teabe seadus

1.4.1. Ülevaade

2008. aastal kaotas AKS kehtivuse ning andmekogude täielikult reformitud normistik viidi üle avaliku teabe seadusesse. Reformi põhjendati andmekogude seaduse „paindumatusega" ning asjaoluga, et nii „tehnoloogia kui ühiskonna vajadused" on edasi arenenud.[68] Andmekogusid puudutavad sätted paigutati avaliku teabe seadusesse, sest reformiga sooviti sarnaselt avaliku teabe seaduse eesmärgiga „tagada avalike ülesannete täitmisel saadud ja loodud teabe kättesaadavus.".[69] X-teega liidestamise kohustus kehtestati seaduse tasemel[70], sest jätkuvalt oli suur hulk riigi andmekogusid X-teega ühendamata ning esines andmete dubleerivat kogumist.[71]

Andmekogu definitsioon esitati järgmiselt:

AvTS § 43[1]. Andmekogu

(1) Andmekogu 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.

Andmekaitse Inspektsioon selgitas oma andmekogude juhendis: „Seega andmekogu eristamiseks on formaalne tunnus – asutamine seaduse või selle alusel antud akti alusel. Muul juhul on tegu üldise avaliku sektori andmetöötlusega ehk täpsemalt avaliku teabe töötlemisega.".[72]

X-tee võimaluste paremaks ärakasutamiseks loodi reformiga ka riigi infosüsteemi haldussüsteem (RIHA). Nii oli reformi eesmärgiks arendada riigi infosüsteem **ühtseks teenusepõhiseks andmeruumiks**, eesmärgiga luua senise killustatud ja liigselt detsentraliseeritud riigi infosüsteemi asemel **terviklik koostoimeline riigi infosüsteem**.[73] Andmete ristkasutamist seadus otsesõnu enam ei reguleerinud, kuivõrd uus normistik põhines riigi andmeteenuse osutamise ja kasutamise kontseptsioonil.[74] Loobuti ka senistest andmekogude erinevatest liikidest. Sarnaselt 1997.a andmekogude seadusega sätestati, et keelatud on asutada ühtede ja samade andmete kogumiseks eraldi andmekogusid.[75] Kasutusele võeti põhiandmete kontseptsioon, millest tulenevalt tuleb andmekogu asutamisel või andmekoosseisude täiendamisel alati enne

[68] Avaliku teabe seaduse ja sellega seonduvate seaduste muutmise seaduse 1027 SE seletuskiri, lk 18.
[69] Samas.
[70] AvTS § 43[2], 43[3].
[71] Avaliku teabe seaduse ja sellega seonduvate seaduste muutmise seaduse 1027 SE seletuskiri, lk 18.
[72] Andmekaitse Inspektsioon. Andmekogude juhend. Tallinn, 14.08.2013, lk 3.
[73] Avaliku teabe seaduse ja sellega seonduvate seaduste muutmise seaduse 1027 SE seletuskiri, lk 18.
[74] Seletuskirjas selgitatakse, et "Andmete kasutamine avalike ülesannete täitmiseks eeldab õigusliku reguleerimise praktikas loobumist valitsemis- ja haldusalade kesksest lähenemisest ning üleminekut protsessikesksele ehk valitsusalasid integreerivale lähenemisele.".
[75] AvTS § 43[3] lg 2. Sellega seondub ka põhiandmete kontseptsioon: AvTS § 43[6]. Põhiandmed ja andmete tähendus
(1) Põhiandmed on riigi infosüsteemi kuuluvasse andmekogusse kogutavad andmekogu unikaalsed andmed, mis tekivad andmekogu haldaja avalike ülesannete täitmise käigus.
(2) Andmete töötlemisel, mida kogub põhiandmetena teine riigi infosüsteemi kuuluv andmekogu, tuleb aluseks võtta vastava teise andmekogu põhiandmed.

kontrollida, kas andmed, mida plaanitakse hakata koguma, on juba mõne olemasoleva andmekogu põhiandmed. Sel juhul tuleks kasutada olemasolevaid andmeid.[76]

§ 43[3]. Andmekogu asutamine

(2) Keelatud on asutada ühtede ja samade andmete kogumiseks eraldi andmekogusid.

§ 43[6]. Põhiandmed ja andmete tähendus

(1) Põhiandmed on riigi infosüsteemi kuuluvasse andmekogusse kogutavad andmekogu unikaalsed andmed, mis tekivad andmekogu haldaja avalike ülesannete täitmise käigus.

(2) Andmete töötlemisel, mida kogub põhiandmetena teine riigi infosüsteemi kuuluv andmekogu, tuleb aluseks võtta vastava teise andmekogu põhiandmed.

(3) Andmete põhiandmeteks olek määratakse kindlaks käesoleva seaduse § 43[3] lõike 3 kohaselt kooskõlastatud tehnilise dokumentatsiooni alusel riigi infosüsteemi haldussüsteemis. Põhiandmete kindlaksmääramisel lähtutakse andmekogu asutamise eesmärgist.

1.4.2. Eesmärgipiirangu regulatsioon (kuni IKÜM jõustumiseni 2018)

Isikuandmete kaitse õiguse üheks nurgakiviks peetakse eesmärgipiirangu põhimõtet, mille kohaselt **isikuandmeid tohib koguda üksnes täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei tohi töödelda hiljem viisil, mis on vastuolus kõnealuste eesmärkidega** (andmekaitsedirektiivi art 6(1)b).

Eesmärgipiirangu põhimõte oli sätestatud ka Eesti esimeses, 1996.a isikuandmete kaitse seaduses, kus isikuandmete esialgse eesmärgiga ühildamatu teisane kasutamine oli lubatav üksnes andmesubjekti nõusolekul,[77] ning 2003.a isikuandmete kaitse seaduses, mille kohaselt võis isikuandmeid muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks

(3) Andmete põhiandmeteks olek määratakse kindlaks käesoleva seaduse § 43[3] lõike 3 kohaselt kooskõlastatud tehnilise dokumentatsiooni alusel riigi infosüsteemi haldussüsteemis. Põhiandmete kindlaksmääramisel lähtutakse andmekogu asutamise eesmärgist. Seletuskiri: „Põhiandmete regulatsioon on suunatud andmete dubleeriva kogumise vältimisele ja riigi infosüsteemis sisalduvate andmete ühtlustamisele ning omavahelisele andmevahetusele. Põhiandmed on riigi infosüsteemi kuuluvas andmekogus seaduse või selle alusel antud õigusakti alusel kogutavad andmekogu unikaalsed andmed, mida teistes andmekogudes ei koguta ja mis tekivad andmekogu haldaja avalike ülesannete täitmise käigus. Andmete töötlemisel, mida andmekogu ise põhiandmetena ei kogu, tuleb aluseks võtta vastava teise andmekogu põhiandmed.“.

[76] Vabariigi Valitsuse 28.02.2008 määrusega nr 58 kehtestatud Riigi infosüsteemi haldussüsteem, § 5 lg 1 p 3, § 6.

[77] 1996.a IKS § 8 Mittedelikaatsete isikuandmete töötlemise lubatavus
(1) Mittedelikaatsete isikuandmete töötlemine on lubatud ilma isiku nõusolekuta, kui töötlemise eesmärk on:
1) isikuga sõlmitud lepingu täitmine või tööde teostamine, mis toimub isiku tellimisel;
2) isiku elu, tervise või vabaduse kaitse;
3) seaduse või välislepinguga ettenähtud kohustuste täitmine;
4) avalikku huvi silmas pidava ülesande täitmine, mis on seaduse või selle alusel kehtestatud õigusaktiga pandud vastutavale töötlejale või kolmandale isikule, kellele andmed üle antakse;
5) üldiste huvide või vastutava töötleja õigustatud huvide või kolmanda isiku, kellele andmed üle antakse, õigustatud huvide arvestamine, kui isiku huvid ei ole olulisemad.
(2) Käesoleva paragrahvi lõikes 1 loetletud eesmärkidel töödeldavate mittedelikaatsete isikuandmete üleandmine kolmandale isikule on lubatud, kui nende töötlemine, sealhulgas kasutamine kolmanda isiku poolt, toimub samadel eesmärkidel. Kui mittedelikaatsete isikuandmete töötlemine, sealhulgas nende kasutamine kolmanda isiku poolt, ei toimu samadel eesmärkidel, on nende üleandmine lubatud ainult isiku nõusolekul.

pädeva organi loal.[78] Nii reguleeriti see ka 2008.a jõustunud uues isikuandmete kaitse seaduses. Andmekogudes säilitatavate isikuandmete teisel eesmärgil kasutamise puhul tuli kuni 2008.a alguseni kehtinud andmekogude seaduse §-s 12 sisalduvat ristkasutuse regulatsiooni käsitleda erinormina, mis reguleeris andmekogu andmete (sh isikuandmete) kasutamist teistel eesmärkidel. Et 2008 kaotas AKS kehtivuse, tuli 2008-2018 juhinduda IKS-s sätestatud eesmärgipiirangu reeglitest.

§ 6. Isikuandmete töötlemise põhimõtted

Isikuandmete töötleja on kohustatud isikuandmete töötlemisel järgima järgmisi põhimõtteid:

2) eesmärgikohasuse põhimõte – isikuandmeid võib koguda üksnes määratletud ja õiguspäraste eesmärkide saavutamiseks ning neid ei või töödelda viisil, mis ei ole andmetöötluse eesmärkidega kooskõlas;

4) kasutuse piiramise põhimõte – isikuandmeid võib muudel eesmärkidel kasutada üksnes andmesubjekti nõusolekul või selleks pädeva organi loal;

1.4.3. Pädeva organi luba muudel eesmärkidel kasutamiseks

Ainuüksi seaduse ka teiste sätete pinnalt jääb selgusetuks, kuidas mõista „pädeva organi loa" tingimust[79] isikuandmete kasutamise eesmärgi muutumisel – kas pädev organ on konkreetse juhtumi vastutav töötleja või hoopis andmekaitse järelevalveasutus?

Segadusse heidab olulisel määral valgust 2003.a IKSi eelnõu algtekstiga tutvumine. Eelnõu Riigikogule esitatud tekstis oli ettenähtud isikuandmete ristkasutuse põhjalik regulatsioon, mis nõudis isikuandmete ristkasutamise eelnevat registreerimist AKI-s[80]. Isikuandmete ristkasutus oleks olnud lubatav Andmekaitse Inspektsiooni tähtajalisel loal[81] ja juhul, kui see ei riku isiku perekonna- ja eraelu puutumatust ning on tagatud isikuandmete töötlemise nõuete täitmine. Isikuandmete ristkasutuseks oleksid ristkasutuse pooleks olevad vastutavad töötlejad pidanud taotlema Andmekaitse Inspektsioonilt vastava loa.[82] Erandina poleks AKI luba olnud nõutav juhul, kui isikuandmete ristkasutuse kohustus on töötlejale pandud seadusega ning kui isikuandmete ristkasutus toimub Andmekaitse Inspektsiooni poolt eelnevalt heakskiidetud tehnilises keskkonnas ning on tagatud isikuandmete töötlemise nõuete täitmine.[83] Registreerimise taotluses tulnuks esitada põhjalik ülevaade kavandatava ristkasutuse detailidest: isikuandmete töötlemise eesmärgid; isikuandmete koosseis; isikute kategooriad, kelle andmeid töödeldakse; isikuandmete allikad; isikud või nende kategooriad, kellele isikuandmete edastamine on lubatud jt.[84] Algteksti seletuskirjas põhjendati ristkasutuse reguleerimist isikuandmete kaitse seaduse eelnõus vajadusega tagada õigusliku regulatsiooni selgus ning

[78] Samasuguses sõnastuses kehtis eesmärgiga seotuse põhimõte ka järgmises, 1.1.2008 jõustunud IKS-s.

[79] Ka Euroopa Nõukogu soovitus Resolution 74(29) on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector nägi ette teisel eesmärgil kasutamise pädeva organi loal.

[80] Eelnõu algteksti § 27 lg 2: Isikuandmete ristkasutuse poolteks olevad vastutavad töötlejad on kohustatud isikuandmete ristkasutuse registreerima Andmekaitse Inspektsioonis.

[81] (4) Isikuandmeteristkasutus registreeritakse viieksaastaks. Vastutav töötleja on kohustatud vähemalt kolmkuud ennetähtaja möödumistesitama uue § 25 nõuetele vastavaregistreerimistaotluse. Tähtaja möödumisel kaotab vastutav töötlejaisikuandmeteristkasutamise õiguse.

[82] Eelnõu algteksti § 27 lg 3.

[83] Eelnõu algteksti § 27 lg 5.

[84] Eelnõu algteksti § 27 lg 6, § 25 lg 2.

koondada isikuandmete töötlemist puudutavad olulisemad normid ühte seadusesse. Riigi või kohaliku omavalitsuse eri andmekogudes säilitatavate andmete ristkasutuse lubatavuse kriteeriumid tulenevad andmekogude seadusest kui vastavate andmekogude pidamist reguleerivast üldseadusest.[85] Seletuskirjas toodud põhjendused ja selgitused on napisõnalised, ent regulatsioonist aimdub eelnõu koostajate soov luua mehhanism andmesubjektide põhiõiguste kaitseks, arvestades üha massilisemaks muutuvat ristkasutust, millega paratamatult kaasneb isikuandmete töötlemine teisel eesmärgil.

2002.a pidas riigi infosüsteemide osakonna nõunik P. F. Lillemaa kõnealust eelnõu ülemääraselt bürokraatlikuks, leides samuti, et andmete ristkasutus ei kujuta endast täiendavat ohtu isiku privaatsusele: „Kui seadusandja on kooskõlas põhiseadusega piiranud isiku õigust eraelu puutumatusele, pannes mingile asutusele kohustuse, mille täitmiseks on vajalik isikuandmete töötlemine, siis pole ju enam oluline, kas andmeid töötlev asutus kogub neid otse allikmaterjalidest või kantakse need andmed ristkasutuse korras üle teisest andmekogust. Tähtis on, milliseid andmeid ja mis alusel töödeldakse, mitte aga see, kust need andmed võetakse.“.[86] Eelnõus väljapakutud ristkasutuse detailsemat loamenetlust nimetab ta „mõttetuks bürokraatiaks, mis indiviidi sisuliselt ei kaitse, kuid raskendab märgatavalt mitmete asutuste tööd“.[87] Oma kriitikas Lillemaa ei puuduta ristkasutusega kaasneva eesmärgi muutumise problemaatikat, kuid selgitab, seadusandja mure mitmete andmebaaside põhjal isiku kohta profiilide loomisega pärast on alusetu, kuivõrd 2002.a tehnoloogia võimaldas juba lubada juurdepääsu info saajale vaid registri valitud kirjetele, jäädvustada logifailis päringu tegemise aja, isiku ja päringu sisu kohta.[88]

Eelnõu menetlemisel Riigikogus jäeti kogu eelnevalt kirjeldatud ristkasutuse reguleerimine seaduse tekstist välja.[89] Lisaks tunnistati rakendussätetega andmekogude seaduse ristkasutuse regulatsiooni sättest kehtetuks see osa, mille kohaselt isikuandmete ristkasutus on lubatud ainult andmekaitse järelevalveasutuse loal ja juhul, kui see ei riku isiku perekonna- ja eraelu puutumatust.[90] Norm, mille kohaselt oli andmekogude ristkasutus lubatav ainult siis, kui see oli seaduses sätestatud, kehtis siiski kuni 2008. aastani.

Vahekokkuvõttena võib järeldada, et õigusnormide tekkelugu arvestades võis isikuandmete muul eesmärgil kasutamiseks „selleks pädeva organi loal“ pidada silmas andmekaitse järelevalveasutust. Pädeva organi luba väljendus Andmekaitse Inspektsiooni pädevuses hinnata ja kontrollida dokumentatsiooni kooskõlastamisel andmekogu korralduslike ja infotehnoloogiliste nõuete, sealhulgas kogutavate andmete koosseisu ja allikate vastavust Avaliku teabe seaduse nõuetele, eelkõige andmekogu andmetele juurdepääsupiirangute kehtestamise vajadust või andmekogu andmete võimaliku avalikustamise kohustuse täitmist, ning isikuandmete kaitse seaduse nõuetele, eelkõige vastavust isikuandmete töötlemise põhimõtetele ning andmekogu turvaklasside ja -meetmete piisavust.[91]

[85] Eelnõu algteksti seletuskiri, p 3.1.4.
[86] P. F. Lillemaa. Märkusi IKS eelnõu kohta. Juridica VII/2002, lk 450-451.
[87] P. F. Lillemaa, lk 451.
[88] P. F. Lillemaa, lk 451.
[89] 1196E II MUUDATUSETTEPANEKUTE LOETELU ISIKUANDMETE KAITSE SEADUSE eelnõule. Muudatusettepanek nr 12.
[90] IKS 2003 § 43.
[91] Vt RIHA määruse § 7.

1.4.4. Pärast 2008.a reformi kujunenud praktika

2008.aastast kehtima hakanud andmekogude regulatsioon ei sisaldanud enam seni kehtinud AKS-le sarnast ristkasutuse regulatsiooni. Avaliku teabe seadus ei käsitle küsimust, kus ja kuidas reguleeritakse, millised haldusorganid ja millistel eesmärkidel püsivalt teise andmekogu andmeid saama hakkavad. Küll aga nähti ette kohustus reguleerida põhimääruses andmekogu andmeandjad.

§ 43[5]. Andmekogu põhimäärus

(1) Andmekogu põhimääruses sätestatakse andmekogu pidamise kord, sealhulgas andmekogu vastutav töötleja (haldaja) ja vajaduse korral volitatud töötleja, andmekogusse kogutavate andmete koosseis, andmeandjad ja vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused.

(2) Andmeandjaks on riigi- või kohaliku omavalitsuse asutused või muud avalik-õiguslikud või eraõiguslikud isikud, kui neil on seadusega või selle alusel antud õigusaktiga sätestatud kohustus andmekogusse andmeid esitada või kui nad teevad seda vabatahtlikult.

AKI 2013.a koostatud ja 2016.a viimati täiendatud andmekogude juhendis, selgitatakse, et mõnel juhul on seadusandja täpselt määratlenud, kes veel ja milliste ülesannete täitmiseks vastavast andmekogust andmeid püsivalt saavad[92] (vt näiteks MKS § 29).

Kui seda eraldi reguleeritud ei ole, siis kehtivad üldsätted, mille kohaselt tuleb kontrollida, kas teisel asutusel on neid andmeid püsivalt vaja mingi avaliku ülesande täitmiseks. Seejuures on AKI andnud järgmise soovituse (silmas on peetud 2008- 2019 kehtinud IKSi):

„IKS § 10 lg 2 ja § 14 lg 2 mõttes seadusest tulenev õiguslik alus peaks koosnema kolmest komponendist:

- seaduse norm, mis sätestab avaliku ülesande,

- pädevusnormi (et see ülesanne on just sellele asutusele pandud) ning

- menetlusnorm, milles väljendub andmete saamise õigus ja tingimused (nt „kogub tõendeid“, „on õigus saada teise asutuse andmekogust andmeid“ vms).“[93]

Kui asutuse hinnangul on need soovituslikud kriteeriumid täidetud, reguleeritakse juurdepääsu täpsem korraldus kahe asutuse vahelises lepingus; ka X-tee määrus nõuab liitumiskokkulepet.[94]

Selgesõnaliste erandite (nagu näiteks MKS § 29) kõrval lähtutigi otsejuurdepääsude andmisel IKS-st tulenevast üldvolitusest (IKS § 10 lg 2 koostoimes § 14 lg 2). Põhimäärustes ei ole seetõttu enamasti sätestatud, kes ja millise ülesande (eesmärgi) täitmiseks otsejuurdepääsu saab, vaid määrusega on antud otsustusõigus asutuse juhile.

Selliselt on juurdepääsu korraldus reguleeritud piiriületuse ootejärjekorra andmekogu põhimääruses, aga ka mitmetes teistes põhimäärustes:[95]

Vastutava ja volitatud töötlejate ülesanded

[92] Vt Andmekogude juhendis „Juurdepääsu õiguslik reguleerimine“ lk 17.
[93] Samas, lk 19.
[94] Vabariigi Valitsuse 23.09.2016 määrus nr 105 „Infosüsteemide andmevahetuskiht“, § 5.
[95] Aga ka piiriületuse ootejärjekorra andmekogu, broneeringuinfo andmekogu põhimäärus, samuti tsiviiltoetuse registri põhimääruse § 34, mobilisatsiooniregistri põhimääruse § 16.

§ 2[1]. Vastutav töötleja:

3) otsustab kolmandatele isikutele andmekogu andmetele juurdepääsu andmise;

§ 18. Andmete väljastamine andmekogust

(4) Andmekogu vastutav töötleja otsustab kolmandatele isikutele andmetele juurdepääsu andmise andmesideühenduse kaudu neile seadusega pandud ülesannete täitmiseks. Vajadusel sõlmitakse andmesaajaga väljastatavate andmete kaitse leping, kus sätestatakse väljastatavate andmete koosseis, andmete väljastamise **eesmärk,** tingimused, kord ja viis.

Mõnes õigusaktis, näiteks liiklusseaduse § 184 lg 5, on sätestatud üldsõnaliselt, et riigi- ja kohaliku omavalitsuse asutusel on õigus juurde pääseda seaduses sätestatud ülesannete täitmiseks vajalikele andmetele. Transpordiameti dokumendiregistrist nähtuvalt on liiklusregistri andmete saamise leping sõlmitud muuhulgas Sotsiaalkindlustusametiga.[96] Alles järelepärimise vastusest selgub, millise konkreetse eesmärgi täitmiseks ja õiguslikule alusele tuginedes liiklusregistri andmeid kasutatakse (toimetulekutoetuse määramisel isiku varalise seisu kontrollimiseks ning võlanõustamise või majandusliku toimetuleku nõustamise korral (SHS § 132. lõige 6, SHS § 15)).

Enamasti seega andmesubjektide jaoks ei ole üheselt selge, millised asutused veel nende andmeid töötlevad. See, kes ja milleks veel otsejuurdepääsu kaudu ühel eesmärgil kogutud andmeid kasutab, ei ole sätestatud enamasti isegi mitte põhimääruses.

Toonane õiguskantsleri nõunik T. Ilus oli juba 2002.a juhtinud Juridica veergudel tähelepanu ka asjaolule, et isikuandmete ristkasutamisel andmekogudes võib samuti kaduda üksikisiku kontroll oma andmete üle: „/m/ida rohkem töödeldakse isikuandmeid ning mida rohkem eri andmebaase ristkasutatakse, seda vähem omab andmesubjekt selle üle kontrolli ning väheneb isikuandmete töötlemise **läbipaistvus**. Et sellises olukorras andmetöötluse läbipaistvus ning selgus siiski võimalikult suures ulatuses tagada, peab isikuandmete ristkasutamine tuginema selgele seaduslikule alusele, et andmesubjektidele oleks õigusaktidest üheselt selge, millised asutused milliseid isikuandmeid töötlevad.“.[97]

Ka AKI on näinud murekohana asjaolu, et „Kui andmete algse kogumise eesmärk on seaduses kirjas, siis see, milleks neid veel võidakse kasutada, tuleneb teistest seadustest. **Nii ei tekigi inimesel andmekogu asutamist ette nägevat seadust lugedes terviklikku ülevaadet sellest, kes ja milleks tema andmeid veel kasutab**.“[98] Näitena tõi AKI välja, et ka kohtuekspertiisi seaduse eelnõu reguleerib vaid sõrmejälgede ja DNA riiklikes registrites andmete säilitamist. Andmete sinna kandmise näevad ette teised seadused; samuti määravad teised seadused kindlaks selle, milleks sõrmejälgede ja DNA riiklikesse registritesse kantud andmeid kasutada võib. [99]

Andmekaitsereformiga kaasnevaid vajalikke muudatusi analüüsinud kontseptsioonidokumendis tõdetakse, et „[ü]ldises plaanis püütakse isikuandmete reformi raames säilitada Eestile

[96] Maanteeameti ja Sotsiaalkindlustusameti vahel 25.03.2020 sõlmitud leping nr 1-13/20/0641-1.
[97] Ilus, Isikuandmete kaitse olemus ja arengusuunad. Juridica 2002/7, lk 523.
[98] Samas.
[99] Andmekaitse Inspektsioon. AVALIKU TEABE SEADUSE JA ISIKUANDMETE KAITSE SEADUSE TÄITMISEST AASTAL 2011, Tallinn, 2012, lk 31-32.

omane avaliku sektori kättesaadavus ja andmekogude ristkasutus läbi X-tee, sh once-only põhimõte ehk andmete ühekordse küsimise põhimõte.“.[100] Nagu käesoleva analüüsi sissejuhatuses mainiti, siis seda, kas andmekogudega seonduv õigusloome vastab IKÜM-st tulenevatele nõuetele, eraldi ei analüüsitud.

[100] Justiitsministeerium. ISIKUANDMETE KAITSE UUE ÕIGUSLIKU RAAMISTIKU KONTSEPTSIOON. 18.04.2017, lk 33.

2. Andmekogude regulatsiooniga seonduvad õiguslikud probleemid ja lahendused

2.1. Isikuandmete töötlemine andmekogudes kui põhiõiguste riive

2005.a märkis toonane õiguskantsler tabavalt, et „/s/ageli on isikuandmete töötlemine (sh nende kogumine) riigi tegevuse nii loomulik osa, et seda ei märgatagi. Tundub iseenesestmõistetav, et inimese iga kokkupuude riigiga tuleks jäädvustada, salvestada andmed andmekogudesse, et oleks hea mitu aastat hiljemgi neid andmeid kasutada, võrrelda andmeid teistes andmekogudes hoitavatega jne.“.[101] Õiguskantsler tõdes, et „ulatuslikud andmekogud ning moodsad infotöötlemise vahendid muudavad ametnike ja poliitikute töö märksa hõlpsamaks. Seejuures ei teadvustata aga kahjuks, et isikuandmete töötlemisega riivatakse inimeste põhiõigusi, milleks on meie põhiseadusest tulenevalt vaja seadusandjalt väga **selgeid volitusi**.“.[102]

PS § 26 kaitseb igaühe perekonna- ja eraelu puutumatust. Euroopa Inimõiguste Kohus on rõhutanud, et eraelu mõiste ammendava definitsiooni andmine ei ole võimalik.[103] Euroopa Nõukogu Parlamentaarse Assamblee resolutsioonis nr 428 (1970) määratletakse eraelu kui õigust elada omaenda elu minimaalse sekkumisega. Sellele lisati resolutsiooniga nr 1165 (1998) õigus kontrollida enda kohta käivat informatsiooni.[104] Eraelu ei piirdu Euroopa Inimõiguste Kohtu praktika järgi üksnes isiku sisemise sfääriga, vaid see hõlmab ka võimude poolt isiku kohta käiva informatsiooni kogumise ja talletamise.[105] Eraelu puutumatust riivab järelikult ka isikuandmete kogumine, säilitamine ja juurdepääsu võimaldamine kolmandatele isikutele[106].

Eraelu puutumatusest tuletatakse ka informatsiooniline enesemääramisõigus, mille tähendus on selgitatud kui iga isiku võimalust ise otsustada, kas ja millises ulatuses tema enda kohta käivaid andmeid kogutakse ja salvestatakse.[107]

Informatsioonilise enesemääramisõiguse lõi ja sisustas Saksamaa Liidukonstitutsioonikohus 1984 aastal kaitseks moodsa infotehnoloogiaga seotud ohtude vastu. Informatsioonilise enesemääramisõiguse tagamiseks tuleb just automatiseeritud andmetöötluse puhul seada varasemast enam organisatoorseid ja menetluslikke kaitsemeetmeid, mis aitaks tasakaalustada selle põhiõiguse rikkumise ohtu.[108] Erinevate andmekogude ristkasutusest tulenevat inimese enda kontrolli kaotust oma andmete üle tasakaalustas kohus eesmärgipiirangu põhimõtte rõhutamisega, mille kohaselt tohib avalik võim isikuandmeid koguda üksnes konkreetselt määratletud eesmärkide saavutamiseks ega tohi koguda andmeid igaks juhuks – eelnevalt määratlemata eesmärkidel.[109] Selleks, et tagada inimeste kontrolli oma andmete üle moodsa andmetöötlusega kaasneva esialgsest eesmärgist erineva töötlemisega seoses rõhutas kohus, et isikuandmete töötluse eesmärgid peavad olema alati

[101] Õiguskantsleri 2005. aasta tegevuseülevaade. Tallinn 2006, lk 87.
[102] Samas, lk 88.
[103] Euroopa Inimõiguste Kohtu 16.12.1992 otsus asjas nr 13710/88, Niemietz *vs*. Saksamaa.
[104] "In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition." Euroopa Nõukogu Parlamentaarse Assamblee resolutsioon nr 1165 (1998) "Right to privacy" p 5.
[105] Euroopa Inimõiguste Kohtu 04.05.2000 otsus asjas nr 28341/95, Rotaru *vs.* Rumeenia.
[106] U.Lõhmus. Kommentaarid §-le 26. - Justiitsministeerium. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Tallinn 2002, § 26 komm 8.3.
[107] M.Ernits. Kommentaarid §-le 19. - Justiitsministeerium. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Tallinn 2002, § 19 komm 4.1.
[108] BVerfG, 15.12.1983 - 1 BvR 209/83 -, Rn. 1-215, p 149.
[109] Samas, p 153.

seadusandja poolt määratletud.[110] Informatsioonilise enesemääramisõiguse piirangud vajavad (põhiseadusest tulenevatele nõuetele vastavat) õiguslikku alust, millest nähtuvad piirangute eeldused ja ulatus inimeste jaoks selgel ja arusaadaval viisil ning mis seega vastab ka õigusriigi põhimõttest tulenevale õigusselguse nõudele.[111]

On leitud, et EL Põhiõiguste Harta põhiõiguse isikuandmete kaitsele sätestamisel tugineti olulisel määral just Saksamaa Liidukonstitutsioonikohtu loodud informatsioonilisele enesemääramisõigusele.[112]

Alates otsekohalduva isikuandmete kaitse üldmääruse (IKÜM) jõustumisega 2018.aastal tuleb IKÜM rakendamisel liikmesriikide poolt kohaldada põhiõiguste hartat, kuivõrd tegemist on EL õiguse kohaldamisega.[113] Kui riik reguleerib isikuandmete töötlemise õiguslikke aluseid ulatuses, mis on IKÜM kohaselt lubatav,[114] viitab ka üldmäärus ise liikmesriigi põhiseaduse (paralleelsele) kohaldamisele: „[k]ui käesolevas määruses osutatakse õiguslikule alusele või seadusandlikule meetmele, ei pea selleks tingimata olema parlamendi poolt vastu võetud seadusandlik akt, ilma et see piiraks asjaomase liikmesriigi põhiseaduslikust korrast tulenevate nõuete kohaldamist.“.[115]

EL Põhiõiguste Harta

Artikkel 8

Isikuandmete kaitse

1. Igaühel on õigus oma isikuandmete kaitsele.

2. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist.

3. Nende sätete täitmist kontrollib sõltumatu asutus.

Euroopa Kohus on seoses EL põhiõiguste hartaga kaitstavate eraelu ja isikuandmete kaitse põhiõiguste riivega rõhutanud, et

“[m]is puudutab põhiõiguste ja -vabaduste kaitse taset, mis on tagatud liidus, siis peab liidu õigusakt, millega kaasneb sekkumine harta artiklitega 7 ja 8 tagatud põhiõigustesse, Euroopa Kohtu väljakujunenud praktika kohaselt sisaldama **selgeid ja täpseid õigusnorme, mis reguleerivad meetme ulatust ja kohaldamist** ning millega on kehtestatud miinimumnõuded, nii et isikutel, kelle isikuandmed on asjassepuutuvad, on piisavad tagatised, mis võimaldavad nende andmeid tõhusalt kaitsta kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest. Niisuguste tagatiste olemasolu on veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt ja kui esineb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult”.[116]

[110] Samas, p 154.
[111] Samas, p 149.
[112] P.K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. Juridica 2016, nr 4, lk 234-235, edasiste viidetega.
[113] ELPH Art 51 lg 1 lause 1.
[114] IKÜM art 6 lg 2 ja 3.
[115] IKÜM pp 41.
[116] EKo 6.10.2015, C-362/14, p 91.

Lisaks tuleneb Euroopa Kohtu praktikast, et isikuandmete kaitsega seondub riive piirduks rangelt vajalikuga. [117] Vastav piirang peab kujutama endast põhiõigusi vähimal määral riivavat meedet, et saavutada taotletud eesmärgi saavutamist.[118] Ka näiteks avaliku halduse rahastamise läbipaistvuse eesmärk ei kaalu isikuandmete kaitse õigust automaatselt üle.[119]

Selleks, et isikuandmete avalikustamine kujutaks endast tema eraelu riivet, ei pea tegemist olema eriti tundlike andmetega, samuti ei pea tõendama ka seda, et inimesele ka tegelikult tekiks sellest mingid negatiivsed tagajärjed. Euroopa Kohus on selgitanud, et isikuandmete edastamine kolmandale isikule riivab asjassepuutuvate isikute õigust eraelu puutumatusele hoolimata sellest, milleks edastatud teavet edaspidi kasutatakse. Samas asjas rõhutas EK: „Sellise sekkumise tõendamisel ei ole oluline, kas edastatud isikuandmed on delikaatsed või mitte või kas asjassepuutuvad isikud on selle sekkumise tõttu pidanud taluma mingeid ebamugavusi".[120]

Asjakohaste põhiõiguste käsitlemisel ei tohi unustada ka põhiseadusest tulenevat inimväärikuse põhimõtet, mille kohta Riigikohus on märkinud, et inimväärikus „on kõigi isiku põhiõiguste alus ning põhiõiguste ja vabaduste kaitse eesmärk".[121] Inimväärikuse põhimõte keelab inimese kohtlemise võimu objektina. Riigikohtu praktikas on selles kontekstis käsitletud haldusmenetluses kehtivat menetlusosalise teavitamise ja vastuväidete esitamise õigust: „Puudutatud isiku ärakuulamisel on ka iseseisev protseduuriline väärtus, sest tagaselja otsuseid tegev asutus käsitab isikut kui vaid menetluse objekti ja mitte kui õigusvõimelist kodanikku."[122] Ka IKÜM-st tuleneb andmesubjekti teavitamise kohustused ja teatud juhtudel ka vastuväidete esitamise õigus. Inimväärikuse küsimus võib tõusetuda ka inimeste profileerimisel, inimeste eeldataval tahtel baseeruvas andmetöötlusel, aga ka isikuandmetele ulatuslike juurdepääsude võimaldamisel olukordades, millest isik ei ole teadlik ega saagi teadlikuks.

---

[117] Vt nt EK C-203/15 ja C-698/15, p. 96 – Tele 2 Sverige AB ja Secretary of State for the Home Department: „Proportsionaalsuse põhimõtte järgimine tuleneb samuti Euroopa Kohtu väljakujunenud praktikast, mille kohaselt nõuab eraelu puutumatuse põhiõiguse kaitsmine liidu tasandil, et isikuandmete kaitse erandid ja piirangud piirduksid rangelt vajalikuga (kohtuotsused, 16.12.2008, Satakunnan Markkinapörssi ja Satamedia, C-73/07, EU:C:2008:727, punkt 56; 9.11.2010, Volker und Markus Schecke ja Eifert, C-92/09 ja C-93/09, EU:C:2010:662, punkt 77; Digital Rights, punkt 52, ja 6.10.2015, Schrems, C-362/14, EU:C:2015:650, punkt 92)." Vt ka Eur Kohus 06.10.2020, nr C-511/18, C-512/18 ja C-520/18, p 210: „Seega ei saa määruse 2016/679 artikli 23 lõikeid 1 ja 2 tõlgendada nii, et need võivad liikmesriikidele anda õiguse kahjustada eraelu puutumatust, rikkudes harta artiklit 7, või muid hartas ette nähtud tagatisi (vt analoogia alusel direktiivi 95/46 kohta 20. mai 2003. aasta kohtuotsus Österreichischer Rundfunk jt, C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, punkt 91). Täpsemalt saab sarnaselt sellega, mis kehtib direktiivi 2002/58 artikli 15 lõike 1 puhul, liikmesriikidele määruse 2016/679 artikli 23 lõikega 1 antud pädevust teostada üksnes nii, et järgitakse proportsionaalsuse nõuet, mille kohaselt isikuandmete kaitse erandid ja piirangud peavad jääma selle piiresse, mis on tingimata vajalik (vt analoogia alusel direktiivi 95/46 kohta 7. novembri 2013. aasta kohtuotsus IPI, C-473/12, EU:C:2013:715, punkt 39 ja seal viidatud kohtupraktika).".

[118] Vt nt EK C-92/09 ja 93/09, p 81 – Schecke ja Eifert: „Miski ei viita sellele, et nõukogu ja komisjon oleks määruse nr 1290/2005 artikli 44a ja määruse nr 259/2008 vastuvõtmisel vaaginud toetusesaajaid puudutavate andmete avaldamise viisi, mis vastaks avaldamise eesmärgile, kuid riivaks vähem toetusesaajate eraelu puutumatuse õigust üldiselt ja konkreetsemalt õigust isikuandmete kaitsele, näiteks toetusesaajaid puudutavate isikuandmete avaldamise piiramine sõltuvalt toetuse saamise ajavahemikust, toetuse sagedusest või liigist ja tähtsusest."

[119] EKo C-92/09 ja C-93/09, p 85.

[120] EKo C-465/00, C-138/01 ja C-139/01.

[121] RKHKo 22.03.2006, 3-3-1-2-06, p 10; RKHKo 3-3-1-14-06, p 11.

[122] RKHKm 08.10.2002, 3-3-1-56-02, p 9.

Eesti Vabariigi põhiseadusest ja selle kohtupraktikast tuleneb põhiõiguste riive puhul **seadusliku aluse nõue.** PS § 11 kohaselt tohib õigusi ja vabadusi piirata ainult kooskõlas põhiseadusega. See tähendab, et niisugune piirang peab olema kooskõlas ka PS § 3 esimese lausega, mille kohaselt teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. PS § 3 lõike 1 esimese lause kohaselt teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. Selles sättes väljendatud üldise seadusereservatsiooni põhimõtte järgi peab **põhiõigusi puudutavates küsimustes kõik olulised otsused langetama seadusandja.**[123] Sama on rõhutatud ka AKI andmekogude juhendis – see, **mil määral peab andmekogu eesmärk, andmekoosseisud ja muud andmekogu olulised küsimused olema reguleeritud seaduse või määruse tasandil, sõltub kaasneva riive intensiivsusest**.[124] Riigikohus on rõhutanud, et intensiivse riive korral ei ole piisav üldsõnaline riivet lubav seadusenorm, vaid olulisuse põhimõttest tulenevalt peab seadusandja otsustama lubatava haldustegevuse sisu, ulatuse ja mahu. Mida intensiivsemalt isiku põhiõigust riivatakse, seda täpsem peab olema selliseks riiveks alust andev regulatsioon. Riivet lubavad seadused peavad olema avalikult kättesaadavad ja inimestel peab olema võimalik mõista, millistel tingimustel võib nende õigusi piirata ja millist käitumist avalik võim neilt ootab.[125]

Riigikohus on siiski märkinud, et „Riigikohtu senise praktika kohaselt ei ole põhiõiguste piirangute kehtestamine määrusega välistatud, kui nende aluseks on täpne, selge ja piirangu intensiivsusega vastavuses olev volitusnorm".[126] Määrust kehtestades (sh määrusega põhiõigusi piirates) ei või minister minna vastuollu seadustes sätestatuga.[127]

Vahekokkuvõte

- Isikuandmete salvestamine andmekogus on põhiõiguste riive
- Sellest, milliseid isikuandmeid salvestatakse, sõltub, kas riive on intensiivne
- Põhiõiguste riive on mistahes edasine toiming nendega, sh isikuandmete kasutamine teiste ametkondade poolt.
- Läbipaistvuse tagamiseks peab regulatsioon olema õigusselge.
- Olulisuse põhimõttest lähtuvalt peavad olulised küsimused olema reguleeritud seaduse tasandil.

,

2.2. IKÜM-st tulenevad nõuded andmekogude reguleerimiseks

2.2.1. Nõuded isikuandmete töötlemise õiguslikule alusele

Õiguspärane isikuandmete töötlemine eeldab, et selleks on IKÜM-st tulenev õiguslik alus (art 6) ning töötlemine vastab IKÜM-s sätestatud töötlemise põhimõtetele (art 5).

[123] RKPJKo 17.12.2019, nr 5-19-40, p 36.
[124] AKI andmekogude juhend, lk 6 jj koos viidetega asjakohasele Riigikohtu praktikale.
[125] RKHKo 18.05.2021, nr 3-19-549/98, p 18 koos viidetega varasemale kohtupraktikale.
[126] RKPJKo 17.12.2019, nr 5-19-40, p 50.
[127] RKPJKo 18.12.2019, nr 5-19-41/9, p 18.

Kui haldusorgan talletab teatud isikuandmeid andmekogus, tuleneb õiguslik alus isikuandmete töötlemiseks GDPR art 6 lg 1 punktist e, mille kohaselt on isikuandmete töötlemine vajalik **avalikes huvides oleva ülesande täitmiseks** või vastutava töötleja avaliku võimu teostamiseks. Teatud juhtudel võib arvesse tulla ka punkt c, mille kohaselt on isikuandmete töötlemine on vajalik vastutava töötleja **juriidilise kohustuse täitmiseks**.[128]

Andmekogudes isikuandmete töötlemise reguleerimisel tuleb arvestada ka art 6 lõikega 3:

> 3. Lõike 1 punktides c ja e osutatud isikuandmete töötlemise alus kehtestatakse:
>
> a) liidu õigusega või
>
> b) vastutava töötleja suhtes kohaldatava liikmesriigi õigusega
>
> Isikuandmete töötlemise **eesmärk** määratakse kindlaks selles õiguslikus aluses või see on lõike 1 punktis e osutatud isikuandmete töötlemise osas vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks. See õiguslik alus võib sisaldada erisätteid, et kohandada käesoleva määruse sätete kohaldamist, sealhulgas üldtingimusi, mis reguleerivad vastutava töötleja poolt isikuandmete töötlemise seaduslikkust, **töötlemisele kuuluvate andmete liiki, asjaomaseid andmesubjekte, üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid, eesmärgi piirangut, säilitamise aega ning isikuandmete töötlemise toiminguid ja -menetlusi, sealhulgas meetmeid seadusliku ja õiglase töötlemise tagamiseks**, nagu näiteks meetmed teiste andmetöötluse eriolukordade jaoks, nagu need on sätestatud IX peatükis. Liidu või liikmesriigi õigus vastab avaliku huvi eesmärgile ning on proportsionaalne taotletava õiguspärase eesmärgiga.

Kui andmekogus töödeldakse **eriliiki isikuandmeid** – s.o. isikuandmeid, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta – sätestatakse juhud, mis tingimustel liikmesriik tohib eriliiki isikuandmete töötlemist reguleerida, IKÜM art 9 lg-s 2.

Seejuures nõuab IKÜM, et liikmesriigi seadusandja kehtestaks **sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks** (IKÜM art 9 lg 2 p-d b, g, h, i, j). IKÜM ei sätesta, millised konkreetsed tagatised tuleb sätestada, sest seadusandja peabki arvestama iga juhtumi eripärasid ja konteksti, millist kaitset andmesubjekt vajab.[129] Kaitsemeetmete nõuet tuleb käsitleda seadusandja täiendava kaalumisvajadusena, millega tehakse seadusandjale ülesandeks võtta arvesse eriliiki isikuandmete spetsiifilist tundlikkust ning näha ette täiendavaid materiaalseid, menetluslikke, organisatoorseid ja/või tehnilisi meetmeid.[130] Materiaalse kaitsemeetmena võib käsitleda näiteks teisel eesmärgil töötlemise keeldu.[131] Euroopa

[128] Vt selle kohta põhjalikumalt näiteks: Arvamus 06/2014 andmete vastutava töötleja õigustatud huvide mõiste kohta direktiivi 95/46/EÜ artikli 7 tähenduses lk 18-19.

[129] BeckOK DatenschutzR/Albers/Veit, 35. Ed. 1.5.2020, DS-GVO Art. 9 äärenr 93

[130] BeckOK DatenschutzR/Albers/Veit, 35. Ed. 1.5.2020, DS-GVO Art. 9 äärenr 94; Kühling/Buchner/Weichert äärenr 132 jj. Vt ka IKÜM nii pp-d 71, aga ka 78, 81, 87 jne. Asjakohane on ka IKÜM art 32, 89.

[131] Näiteks IGUS § 16. Geenivaramu kasutamise lubatavus
(1) Geenivaramut võib kasutada üksnes teaduslikuks uurimistööks, geenidoonori haiguste uurimiseks ja raviks, rahva tervise uurimiseks ja statistilistel eesmärkidel. Geenivaramu kasutamine muul otstarbel, eriti tsiviil- või kriminaalprotsessis tõendite kogumiseks või jälitustegevuseks, on keelatud.

Inimõiguste Kohus on pidanud oluliseks ka säilitustähtaegade olemasolu, nõudes teatud juhtudel ka diferentseeritud säilitamistähtaegu.[132]

EL seadusandja on pidanud oluliseks ka õigusselguse põhimõtet – IKÜM põhjenduspunktis 41 selgitatakse, et „kui IKÜM-s osutatakse õiguslikule alusele või seadusandlikule meetmele, ei pea selleks tingimata olema parlamendi poolt vastu võetud seadusandlik akt, ilma et see piiraks asjaomase liikmesriigi põhiseaduslikust korrast tulenevate nõuete kohaldamist. Selline õiguslik alus või seadusandlik meede peaks siiski olema **selge ja täpne** ning **selle kohaldamine peaks olema eeldatav isikute jaoks, kelle suhtes seda kohaldatakse** vastavalt Euroopa Liidu Kohtu („Euroopa Kohus“) ja Euroopa Inimõiguste Kohtu praktikale.“.

2.2.2. Nõuded isikuandmete töötlemise eesmärgipiirangule

Isikuandmete eesmärgipärasuse põhimõtte on üldmääruses sätestatud sarnaselt eelneva andmekaitsedirektiiviga[133]:

IKÜM artikkel 5

Isikuandmete töötlemise põhimõtted

1. Isikuandmete töötlemisel tagatakse, et

b) isikuandmeid **kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel** ning neid ei töödelda hiljem viisil, mis on nende eesmärkidega vastuolus; isikuandmete edasist töötlemist avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil ei loeta artikli 89 lõike 1 kohaselt algsete eesmärkidega vastuolus olevaks („eesmärgi piirang“).[134]

Isikuandmete töötlemine andmekogus toimub IKÜM art 6 lg 1 punkti e alusel, mille alla kuuluvad olukorrad, mil isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, samuti võib see toimuda punkti c alusel, mille kohaselt on isikuandmete töötlemine on vajalik vastutava töötleja juriidilise kohustuse täitmiseks.[135].

[132] EIK 22.06.2017, Aycaguer v. France (The Court noted that, to date, no appropriate action had been taken on that reservation and that **there was currently no provision for differentiating the period of storage depending on the natuure and gravity of the offences committed**. The Court also ruled that the regulations on the storage of DNA profiles in the FNAEG did not provide the data subjects with sufficient protection, owing to its duration and the fact that the data could not be deleted).

[133] Direktiivi 95/46/EÜ art 6 lg 1 punkti b kohaselt liikmesriigid sätestavad selle, et isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ega töödelda hiljem viisil, mis on vastuolus kõnealuste eesmärkidega. Täiendavat töötlemist ajaloo, statistika või teadusega seotud eesmärkidel ei peeta vastuolus olevaks tingimusel, et liikmesriigid kannavad hoolt vajalike tagatiste eest.

[134] Õiguskaitseasutuste osas vt ka IKS § 16.

[135] Artikli 29 alusel asutatud andmekaitse töörühm on direktiiviga seoses selgitanud punktide c ja e vahetegu järgmiselt: „Tegu võib olla ka avaliku sektori asutuse kohustusega, kuna artikli 7 punkti c kohaldamine ei ole mingil viisil piiratud avaliku või erasektoriga. Seda saab kohaldada näiteks selliste andmete suhtes, mida kogub kohalik asutus vales kohas parkimise eest määratud trahvide haldamiseks./---/ Vastutaval töötlejal ei tohi olla valikut, kas täita kohustust või mitte./---/ Lisaks peab seadusjärgne kohustus olema isikuandmete töötlemise nõudmise küsimuses piisavalt selge. Seega kohaldatakse artikli 7 punkti c selliste õiguslike sätete alusel, milles osutatakse sõnaselgelt töötlemise liigile ja objektile. Vastutaval töötlejal ei tohi olla põhjendamatul määral otsustusõigust küsimuses, kuidas seadusjärgset kohustust täita./---/ Õigusaktides võib mõnel juhul olla kindlaks määratud vaid üldine eesmärk, kusjuures konkreetsemad kohustused on kehtestatud muudel tasanditel, näiteks

IKÜM art 6 lõikes 3 täpsustatakse, et punktides c ja e osutatud isikuandmete töötlemise alus kehtestatakse kas liidu või vastutava töötleja suhtes kohaldatava liikmesriigi õigusega ning et „Isikuandmete töötlemise eesmärk määratakse kindlaks selles õiguslikus aluses või see on lõike 1 punktis e osutatud isikuandmete töötlemise osas vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks.“. Isikuandmete töötlemise eesmärgi määratlemist nõuab ka EL põhiõiguste harta art 8 lg 2, mille kohaselt tuleb isikuandmeid töödelda asjakohaselt ning **kindlaksmääratud eesmärkidel** ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel.

Eesmärgi piirangu põhimõte, mille kohaselt tohib isikuandmeid töödelda **vaid sel eesmärgil, milleks neid koguti**, näib olevat vastuolus andmekogude ulatusliku ristkasutuse ja andmete ühekordse küsimise põhimõttega, millel Eesti e-riik rajaneb.

Näiteks rahvastikuregistri andmeid tohib rahvastikuregistri seadusest tulenevalt kasutada Eesti rahvastiku üle arvestuse pidamise kõrval ka „riigi ja kohaliku omavalitsuse asutustele ning muudele füüsilistele ja juriidilistele isikutele neile seadusega või seaduse alusel pandud avalik-õigusliku ülesande (edaspidi avalik ülesanne) täitmiseks“.[136]

Liiklusregistri eesmärk on aga sätestatud järgmiselt: „Liiklusregister on Vabariigi Valitsuse poolt asutatud andmekogu, mille eesmärk on pidada arvestust sõidukite, väikelaevade, alla 12-meetrise kogupikkusega laevade ja jettide, juhilubade ja muude juhtimisõigust tõendavate dokumentide, digitaalse sõidumeeriku kaartide, juhtide ametikoolituse ja registerpantide üle.“. Seega kujutab endast teisel eesmärgil töötlemist näiteks liiklusregistri andmete kasutamine liiklusjärelevalve teostamisel, inimese toimetuleku hindamisel või maksupettuste tuvastamiseks.

Kui ei ole täidetud IKÜM-st tuleneva teisel eesmärgil töötlemise tingimused, siis esialgse kogumisega eesmärgiga vastuolus oleval eesmärgil isikuandmeid töödelda ei tohi (IKÜM art 5 lg 1 p b), kusjuures isikuandmete edasist töötlemist avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil ei loeta artikli 89 lõike 1 kohaselt algsete eesmärkidega vastuolus olevaks.

IKÜM reguleerib eesmärgi muutust vastuoluliselt. Ühelt poolt deklareeritakse, et liikmesriik võib säilitada avaliku halduse andmetöötluse osas oma senise süsteemi (vrd art 6 lg 2) ja reguleerida avaliku halduse puhul ka eraldi oma seadustes täpsemalt eesmärgipiirangut just isikuandmete töötlemisel avalike ülesannete täitmisel, reguleerides „üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid, eesmärgi piirangut“ (art 6 lg 3).[137] Teiselt poolt reguleerib eraldi muul eesmärgil töötlemist ka art 6 lg 4, milles on üsna ranged tingimused eesmärgimuutuseks.

EL seadusandja sõnum avalikus sektoris toimuva andmete ristkasutuse reguleerimiseks ja seega ka andmete ühekordse küsimise põhimõtte juurutamisel on olnud vastuoluline. Erinevates IKÜMi kommentaarides on leitud näiteks nii seda, et art 6 lg 2 on üksnes deklaratiivse

---

kas teiseste õigusaktidega või avaliku sektori asutuse siduva otsusega konkreetse juhtumi kohta. See võib samuti tekitada artikli 7 punkti c kohase seadusjärgse kohustuse, eeldusel et töötlemise liik jaobjekt on täpselt kindlaks määratud ja töötlemisel on piisav õiguslik alus.“. Vt põhjalikumalt art 29 arvamust õigustatud huvi kohta, lk 18jj.

[136] RRS § 4 p 1.

[137] Ka pp 45: „Samuti peaks töötlemise eesmärk olema kindlaks määratud liidu või liikmesriigi õigusaktis. Lisaks võiks nimetatud õigusaktis olla sätestatud käesoleva määruse üldtingimused, millega reguleeritakse isikuandmete töötlemise seaduslikkust, kehtestatakse tingimused vastutava töötleja kindlaksmääramiseks, töötlemisele kuuluvate isikuandmete liik, asjaomased andmesubjektid, **üksused, kellele võib andmeid avaldada, eesmärgi piirangud,** säilitamise aeg ja muud meetmed seadusliku ja õiglase töötlemise tagamiseks.“.

tähendusega ja tegelikult ebavajalik[138], kui ka seda, et see moodustab koostoimes lõikega 3 volitusnormi liikmesriigi jaoks[139], aga ka seda, et lõige 2 ja lõige 3 on mõlemad täiesti eraldi volitusnormid, kusjuures lg 2 annab õiguse arvata avaliku halduse andmetöötlus, millel puudub mõju EL ühisturule, IKÜMi kohaldamisalast üldse välja[140]. Art 6 lõiget 4 on peetud eraldiseisvaks volitusnormiks, mille alusel liikmesriik saab reguleerida teisel eesmärgil töötlemist[141], aga ka üldse mitte volitusnormiks, kuivõrd volitusnorm tuleneb üksnes lg 4 koostoimes lõigetega 2 ja 3[142]. Leitakse samuti, et lõiget 4 tuleb pidada sätteks, mis reguleerib eesmärgi muutmise lubatavust, samal ajal kui üksnes lõike 3 alusel saab liikmesriik reguleerida uue eesmärgi esialgse eesmärgiga ühildumise teatavaid üksikasju.[143] Samuti on leitud, et art 6 lg 4 toodud eesmärgi ühilduvuse hindamise kriteeriumid markeerivad liikmesriigi seadusandja kaalutlusruumi välimise piiri.[144] Segadusse ei heida erilisel määral valgust ka üldmääruse põhjenduspunktid, milles on selgitatud näiteks, et „Kui töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, võib liidu või liikmesriigi õiguses kindlaks määrata ja täpsustada need ülesanded ja eesmärgid, mille puhul tuleks pidada edasist töötlemist eesmärkidele vastavaks ja seaduslikuks.“ ja „Liidu või liikmesriigis õiguses sätestatud õiguslik alus isikuandmete töötlemiseks võib olla ka edasise töötlemise õiguslikuks aluseks.“. Analüüsi koostamisel kasutatud kommentaaridest nähtub ka, et eriarvamused ei esine üksnes õigusteadlaste käsitlustes, vaid näiteks Saksamaal on erinevates seaduste seletuskirjades tuginetud teatud juhtudel art 6 lõikele 4, teatud juhtudel aga lõigetele 2 ja 3, eriliiki isikuandmete puhul aga hoopis artiklile 9.[145]

Käesoleva analüüsi koostajate hinnangul tuleks IKÜM mõista selliselt, et liikmesriik tohib art 6 lg 2 ja 3 alusel reguleerida täpsemalt andmetöötlust, mis toimub art 6 lg 1 p-de c ja e alusel (avalike ülesannete täitmine ja juriidiline kohustus), ja selles osas tohib liikmesriik reguleerida ka eesmärgi piirangut, lähtudes seejuures art 6 lg 4.

Seejuures tuleb lähtuda nii sellest, et andmetele juurdepääsu avamine teisele ametiasutusele kasutamiseks on eraldi põhiõiguste riive; samuti seda, et reguleerides lõike 3 alusel „üksuseid, kellele võib isikuandmeid avaldada, ja avaldamise põhjuseid, eesmärgi piirangut“ tuleb tagada pp 41 viidatud õigusselgus ja proportsionaalsus:

---

[138] ZB Kühling/Martini et al., lk 28jj.; Paal/Pauly/Frenzel Art. 6 äärenr. 32, 40; Ehmann/Selmayr/Heberlein Art. 6 äärenr 2, 30; Schaffland/Wiltfang/Schaffland/Holthaus DSGVO Art. 6 äärenr 300ff. Alexander Roßnagel, Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, Rn.

[139] Schantz NJW 2016, 1841 (1842); Gola/Schulz Art. 6 äärenr 172.

[140] Alexander Roßnagel, Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, Rn.

[141] DSGVO Art. 6 Abs. 4 Zweckvereinbarkeit, Alexander Roßnagel, Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, äärenr 18. , samuti Kühling/Martini et al., lk 38.

[142] Kühling/Buchner/Buchner/Petri, 3. Aufl. 2020, DS-GVO Art. 6 Rn. 200, *Albers/Veit* in BeckOK DatenschutzR Art. 6 äärenr 71.

[143] DSGVO Art. 6 Abs. 4 Zweckvereinbarkeit, Alexander Roßnagel, Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, Rn 28.

[144] Martini/Wenzel: „Die Mitgliedstaaten dürfen dadurch den Zweckbindungsgrundsatz jedoch nicht ad absurdum führen. Die Kompatibilitätskriterien des Art. 6 Abs. 4 DSGVO bilden deshalb die äußerste Grenze für die gesetzgeberische Beurteilung, welche weiteren Verarbeitungszwecke noch im Rahmen des Zulässigen liegen.“. „Once only“ versus „only once“: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit. DVBl 2017, S. 749-758.

[145] DSGVO Art. 6 Abs. 4 Zweckvereinbarkeit, Alexander Roßnagel, Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, Rn. 29jj

(41) Kui käesolevas määruses osutatakse õiguslikule alusele või seadusandlikule meetmele, ei pea selleks tingimata olema parlamendi poolt vastu võetud seadusandlik akt, ilma et see piiraks asjaomase liikmesriigi põhiseaduslikust korrast tulenevate nõuete kohaldamist. Selline õiguslik alus või seadusandlik meede peaks siiski olema **selge ja täpne ning selle kohaldamine peaks olema eeldatav isikute jaoks**, kelle suhtes seda kohaldatakse vastavalt Euroopa Liidu Kohtu („Euroopa Kohus“) ja Euroopa Inimõiguste Kohtu praktikale.

Andmetöötlus peab olema inimeste jaoks läbipaistev. EL järjepideva kohtupraktika on ka rõhutanud, et andmekaitseliste normide puhul olema tagatud **„põhiõiguste ja -vabaduste kaitse kõrge tase“**.[146]

2.2.3. Täiendavad nõuded läbipaistvuse tagamiseks

Läbipaistev andmetöötlus ja kontroll oma isikuandmete üle on osaks põhiõigusest eraelu puutumatusele: „Lisaks on Euroopa Kohus harta artikli 7 kohta juba leidnud, et selles artiklis tunnustatud põhiõigus eraelu puutumatusele eeldab, et andmesubjekt saab veenduda, et tema isikuandmeid töödeldakse õigesti ja seaduslikult. Vajaliku kontrolli teostamiseks peab sellel isikul olema õigus tutvuda teda käsitlevate töödeldavate andmetega/---/.“.[147] Selleks, et tagada isikuandmete töötlemise läbipaistvus, nähakse üldmääruses ette rida andmesubjekti õigusi ja vastutava töötleja teavitamiskohustusi (art 12jj). Ainult siis, kui andmesubjekt on teadlik, kes ja milleks tema andmeid töötleb, saab ta kasutada õigust tutvuda oma andmetega ja nõuda ebaõigete andmete parandamist. Tegemist ei ole uudishimu rahuldamise võimaldamisega, vaid informatsioonilise enesemääramisõiguse ja inimväärikuse põhimõtte tagamisega.

Nii tuleneb üldmäärusest kohustus avaldada veebis andmekaitsetingimused, milles „kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt“ (art 12 lg 1). Põhjenduspunktis 63 selgitatakse, et „Igal andmesubjektil peaks seega olema õigus teada eelkõige isikuandmete töötlemise eesmärke, võimaluse korral isikuandmete töötlemise ajavahemikku, isikuandmete vastuvõtjaid, isikuandmete automaatse töötlemise loogikat ja sellise töötlemise võimalikke tagajärgi (vähemalt juhul kui töötlemine põhineb profiilianalüüsil) ning saada eelneva kohta teate. Võimaluse korral peaks vastutav töötleja saama anda kaugjuurdepääsu turvalisele süsteemile, kus andmesubjekt saab otse tutvuda oma isikuandmetega.“ (vt ka art 13). Käesoleva analüüsi raames kontrollitud haldusorganite veebilehtedel avaldatud andmekaitsetingimustes ei ole avaldatud andmekogudes salvestatud isikuandmete kohta infot, samuti ka mitte seda, millistele teistele haldusorganitele on loodud juurdepääsud või kelle päringute puhul isikuandmeid väljastatakse. IKÜMi koostamisel peeti

[146] Vrd nt: „Direktiivi 95/46 artiklist 1 ning põhjendustest 2 ja 10 nähtub, et direktiivi eesmärk on tagada mitte ainult füüsiliste isikute põhiõiguste ja -vabaduste ning eelkõige nende õiguse eraelu puutumatusele tõhus ja täielik kaitse isikuandmete töötlemisel, vaid ka põhiõiguste ja -vabaduste kaitse kõrge tase. Seda, et nii harta artikliga 7 tagatud põhiõigus eraelu puutumatusele kui ka artikliga 8 tagatud põhiõigus isikuandmete kaitsele on olulised, on lisaks rõhutatud ka Euroopa Kohtu praktikas (vt kohtuotsused Rijkeboer, C-553/07, EU:C:2009:293, punkt 47; Digital Rights Ireland jt, C-293/12 ja C-594/12, EU:C:2014:238, punkt 53, ning Google Spain ja Google, C-131/12, EU:C:2014:317, punktid 53, 66 ja 74 ning seal viidatud kohtupraktika).“. Schrems, 6.10.2015, EK C-362/14, p 39.

[147] Viitega EKo, 7.5.2009, Rijkeboer, C-553/07, EU:C:2009:293, punkt 49, Euroopa Kohtu (suurkoda) arvamuse projekt. Kanada ja Euroopa Liidu vahelise lepingu projekt – Lennureisijate broneeringuinfo edastamine liidust Kanadasse nr 1/15, 26. juuli 2017, P 219.

andmesubjekti õigustest teavitamise kohustusi sedavõrd olulisteks[148], et kohustuste rikkumise eest on võimalik kohaldada ka haldustrahvi[149] ja seda on teistes liikmesriikides ka tehtud.[150]

Kui teine haldusorgan saab isikuandmed mitte inimeselt endalt, vaid teiselt haldusorganilt, tuleb vastavalt IKÜM art 14 tagada inimese teavitamine sellest. Teavitamise kohustust ei ole, kui „isikuandmete saamine või avaldamine on selgesõnaliselt sätestatud vastutava töötleja suhtes kohaldatavas liidu või liikmesriigi õiguses, milles nähakse ette asjakohased meetmed andmesubjekti õigustatud huvide kaitsmiseks“ (art 14 lg 5 c). **Seega, kui teiste asutuste juurdepääs ei ole andmekogu regulatsioonis selgesõnaliselt sätestatud, nõuab IKÜM art 14 puudutatud inimeste personaalset teavitamist**, et nende andmed saadi mujalt kui inimeselt endalt.

Teavitamine annab andmesubjektile õiguse esitada vastuväide IKÜM art 21 lg 1 kohaselt, mis näeb ette, et andmesubjektil on õigus oma konkreetsest olukorrast lähtudes esitada igal ajal vastuväiteid teda puudutavate isikuandmete töötlemise suhtes, mis toimub **artikli 6 lõike 1 punkti e (isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks)**, sealhulgas nendele sätetele tugineva profiilianalüüsi suhtes. Vastutav töötleja ei töötle isikuandmeid edasi, välja arvatud juhul, kui vastutav töötleja tõendab, et töödeldakse mõjuval õiguspärasel põhjusel, mis kaalub üles andmesubjekti huvid, õigused ja vabadused, või õigusnõuete koostamise, esitamise või kaitsmise eesmärgil.

IKÜM art 23 kohaselt on liikmesriigil võimalik küll andmesubjekti õigusi ja teavitamiskohustusi piirata, kuid seejuures austades põhiõiguste olemust ning tagades proportsionaalsuse põhimõtted, lisaks ka muud art 23 lõigetest 1 ja 2 tulenevad nõuded.

2.3. Eesti andmekogude regulatsiooni vastavus nõuetele

2.3.1. Olulisuse põhimõte: seaduse või määruse tasand?

Andmekogude asutamist reguleerib AvTS järgmiselt:

AvTS § 43[3]. Andmekogu asutamine

(1) Andmekogu asutatakse seadusega või selle alusel antud õigusaktiga.

Nii AKI kui ka õiguskantsler on juba aastaid tagasi toonud välja probleemi, et andmekogu asutamist reguleerivates seadustes on andmekogu regulatsioon on liiga napp. Nii on AKI juba aastate eest tõdenud, et „[k]ahjuks on see väga levinud praktika, et seaduses küll nimetatakse ära, et andmekogu asutatakse, kuid andmekogusse kantavate andmete koosseisu kindlaks määramine on jäetud täitevvõimu pädevusse. Oleme nõus, et **seaduse tasandil ei pea üksikasjalikult ära loetlema kõiki andmeid, kuid inimesel peaks olema võimalik seadust lugedes aru saada,**

[148] Vt lisaks EDPB soovitus läbipaistvuse kohta.
[149] Art 83 lg 5 punkt c: „Kooskõlas lõikega 2 võib järgmiste sätete rikkumise eest määrata trahvi, mille suurus on kuni 20 000 000 eurot või ettevõtja puhul kuni 4 % tema eelneva majandusaasta ülemaailmsest aastasest kogukäibest, olenevalt sellest, kumb summa on suurem: andmesubjektide õigused artiklite 12–22 alusel“.
[150] Veebilehel https://www.enforcementtracker.com/ on võimalik vaadata IKÜM konkreetsete artiklite alusel kohaldatud haldustrahve.

mis liiki andmeid ja milleks tema kohta kogutakse, kaua neid säilitatakse ning milleks veel võidakse kasutada.“.[151]

Sama on täheldatud õiguskantsleri 2005.a ülevaates, milles on analüüsitud mitmeid erinevaid andmekogusid, kus seadusandja ei olnud täpsustanud andmekoosseisusid ega registri eesmärki.[152] Näitena tuuakse välja, et kaitseväekohustuslaste registri puhul tulenes seadusest lakooniline volitus „pidada arvestust“ kaitseväekohustuslike Eesti kodanike üle, ent register, mis selle sätte alusel loodi, sisaldas detailset ülevaadet iga kaitseväekohustuslase kohta. Muuhulgas kajastas register andmeid perekonnaseisu, laste, elukoha, hariduse, töökoha, oskuste jms kohta. Registrisse salvestati ka hulk isikuandmeid terviseseisundi kohta.[153] Toonane õiguskantsler juhtis tähelepanu, et kui isikuandmete töötlemise eesmärk jääb seaduse tasemel piisavalt määratlemata, „riskime olukorraga, kus üksikisikutel kaob igasugune kontroll selle üle, millistes asutustes tema kohta milliseid andmeid kogutakse ning täitevvõim saab vabad käed üha üksikasjalikumaks inimeste jälgimiseks“.[154]

Tuleb tõdeda, et regulatsioon kehtib samal kujul tänase päevani: kaitseväeteenistuse seaduse § 11 kõlab järgmiselt:

§ 11. Kaitseväekohustuslaste register
(1) Kaitseväekohustuslaste register on andmekogu, mille eesmärk on pidada arvestust kaitseväekohustuslaste, kaitseväekohustust võtta soovivate isikute, kaitseväekohustuse täitmise ning seaduses ettenähtud toimingute ja otsuste tegemise üle ning tegevteenistusse asumise nõuetele vastavuse kohta.
(11) Kaitseväekohustuslaste registris **töödeldakse isikuandmeid, sealhulgas eriliiki isikuandmeid.**
(2) Kaitseväekohustuslaste registri asutab ja selle põhimääruse kehtestab Vabariigi Valitsus määrusega.
(3) Kaitseväekohustuslaste registri vastutav töötleja on Kaitseministeerium.
(4) Kaitseväekohustuslaste registri volitatud töötleja on Kaitseressursside Amet.
(5) Kaitseväekohustuslase andmed kantakse kaitseväekohustuslaste registrisse. Esmakordsest kandest teavitab kaitseväekohustuslast Kaitseressursside Amet.

Andmekoosseisud on põhimääruses kehtestatud järgmiselt:

§ 8. Digitaalsesse registrisse kantavad andmed (1) Kaitseväekohustuslase ja kaitseväekohustust võtta sooviva isiku (edaspidi koos andmesubjekt) andmetena kantakse digitaalsesse registrisse: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) isikuandmed; 2) haridusandmed; 3) andmed oskuste ja usutunnistuse kohta; 4) andmed terviseseisundi hindamise kohta;	(5) Andmesubjekti **terviseseisundi andmed** on: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) teave arstlikku komisjoni kutsumise ja komisjoni viibimise kohta; 2) teave arstliku komisjoni otsuse kohta; 3) diagnoosid ja RHK-10 kood; 4) veregrupp ja reesusfaktor; 5) antropomeetrilised andmed; 6) teave arstlikus komisjonis tehtud arstliku läbivaatuse ja terviseuuringute tulemuste kohta.	(8) Andmesubjekti **kaitseväeteenistuse kohta** kantakse registrisse järgmised andmed: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) teave kaitseväelase tõotuse andmise kohta; 2) teave ajateenistusse asumise ja ajateenistuse lõpetamise kohta; 3) teave asendusteenistusse asumise ja asendusteenistuse lõpetamise kohta; 4) teave naissoost isiku ajateenistusest loobumise kohta;

[151] AKI 2011.a tegevusülevaade, lk 31.
[152] Õiguskantsleri 2005. aasta tegevuse ülevaade. Tallinn 2006, lk 89 „Kriminaalmenetlusregistri puhul on huvitav märkida, et enne kavandatavaid muudatusi oli tegemist vaid abistava iseloomuga menetlusregistriga, kuhu kanti põhiliselt menetlustoimingutega seotud faktoloogia. Parandusi ette näinud eelnõuga seotud dokumentidest oli võimalik välja lugeda, et andmekoosseisu on vaja täiendada statistika tegemise eesmärgiga. Eelnõu ettevalmistanud Justiitsministeeriumi esindajate kinnitusel oli aga andmekoosseisu laiendamise taga veel teinegi plaan – laiendada järk-järgult registri mahtu, et lõppeesmärgina muutuks register kriminaalmenetluse toimiku elektrooniliseks variandiks. See eesmärk ei kajastunud aga isegi vastava määruse eelnõuga seotud dokumentides. Registri pidamise eesmärk sõltus täielikult täitevvõimu soovidest. Seadusandja ei pruukinud sellisest põhiõiguste riive ulatuse laiendamisest teadagi.“.
[153] Samas, lk 89-90.
[154] Samas, lk 88.

5) andmed kutsesobivuse kohta; 6) andmed kaitseväekohustuse täitmise kohta; 7) andmed kaitseväeteenistuse kohta; 8) andmed kaitseväeteenistuse käigu kohta; 9) andmed kohaldatavate piirangute kohta; 10) andmed kirjavahetuse ja haldusotsuste kohta. [RT I, 14.04.2020, 5 - jõust. 17.04.2020] (2) Andmesubjekti **isikuandmed** on: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) isikukood; 2) ees- ja perekonnanimi või -nimed; 3) sünnikoha riik; 4) kodakondsus; 5) alaealiste laste arv; 6) elukoht rahvastikuregistri järgi; 7) kontaktaadress, kui see erineb rahvastikuregistrisse kantud elukohast; 8) kontakttelefon ja e-posti aadress; 9) arvelduskonto andmed. [RT I, 14.04.2020, 5 - jõust. 17.04.2020] (3) **Andmesubjekti haridusandmed** on: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) teave omandatud või omandatava haridustaseme kohta; 2) teave õppeasutuse kohta; 3) teave õpingute alguse ja lõpu kohta; 4) õppekava kood; 5) õppekava nimetus; 6) teave õppetöö õppevormi kohta. (4) **Andmesubjekti oskuste ja usulise veendumuse kohta** kantakse registrisse andmed: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) mootorsõiduki juhtimisõiguse kohta; 2) vaba tahte alusel antud teave usutunnistuse kohta.	[RT I, 14.04.2020, 5 - jõust. 17.04.2020] (6) Andmesubjekti **kutsesobivuse andmeteks** on kutsealuse kutsesobivuse hindamise aeg ja hindamise tulemus. [RT I, 14.04.2020, 5 - jõust. 17.04.2020] (7) Andmesubjekti **kaitseväekohustuse täitmise kohta** kantakse registrisse järgmised andmed: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) teave arvestuskategooria kohta; 2) teave ajateenistusse kutsumise kohta; 3) teave ajapikenduse andmise kohta; 4) teave andmesubjekti suhtes teostatava kriminaalmenetluse kohta; [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 5) teave karistatuse kohta; 6) teave kaitseväekohustuse võtmise taotluse või sõjaväelise auastmega sõjaaja ametikohale nimetamise nõusoleku esitamise kohta; [RT I, 29.12.2015, 11 - jõust. 01.01.2016] 7) teave kaitseväekohustuslaseks tunnistamise kohta; 8) teave naissoost isiku ajateenistusse asumise taotlemise kohta; 9) teave Kaitseressursside Ameti otsuse tegemiseks vajalike toimingute kohta; 10) identifitseerimiskoodi moodustamise ja väljastamise kohta.	5) teave tegevteenistusse asumise ja tegevteenistuse lõpetamise kohta; 6) teave õppekogunemise ja lisaõppekogunemise kohta; 7) teave reservis olemise kohta; 8) teave sõjaväelise auastmega ametikohale nimetamise kohta; 9) teave sõjaväelise väljaõppe ja väljaõppe astme kohta; 10) teave mobilisatsioonikäsu kohta. [RT I, 14.04.2020, 5 - jõust. 17.04.2020] (9) Andmesubjekti **kaitseväeteenistuse käigu kohta** kantakse registrisse järgmised andmed: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) teave viimasele rahuaja ametikohale nimetamise kohta; 2) teave viimasele sõjaaja ametikohale nimetamise kohta; 3) teave sõjaväelise auastme andmise kohta; 4) kaitseväekohustuslase sõjaväearvestuse eriala kood; 5) teave sõjaväelise väljaõppe ja väljaõppe astme kohta. (10) Andmesubjekti suhtes kohaldatavate **piirangute kohta** kantakse registrisse järgmised andmed: [RT I, 14.04.2020, 5 - jõust. 17.04.2020] 1) teave Eestist lahkumise keelu kohta; 2) teave piirangute kohta õppekogunemisele või lisaõppekogunemisele kutsumisel või mobiliseerimisel; 3) teave piirangutest seoses kaitseväeteenistuskohustuse täitmisega. [RT I, 28.06.2018, 7 - jõust. 01.07.2018] (11) **Kirjavahetuse ja haldusotsuste kohta** kantakse registrisse järgmised andmesubjekti ja Kaitseressursside Ameti vahel kaitseväekohustuse täitmisega seotud kirjavahetuse ning Kaitseressursside Ameti ja arstlike komisjonide tehtud haldusotsuste andmed: 1) dokumendi saaja ja saatja nimi ja isikukood või registrikood; 2) dokumendi saabumise või väljastamise kuupäev; 3) dokumendi vastuvõtmise või edastamise viis; 4) dokumendi elemendid; 5) dokumendi liik; 6) dokumendi kohta kehtivad juurdepääsupiirangud.

Sarnaselt ei sätestata riigikaitseseaduses väga palju mobilisatsiooniregistri kohta:

RiKS § 25. Mobilisatsiooniregister
(1) Mobilisatsiooniregister on andmekogu, mille eesmärk on pidada arvestust sõjaaja ametikohtade täitmise ja riigi sõjaliseks kaitseks kasutatavate materiaalsete vahendite üle.
(2) Andmekogu sisaldab:
1) sõjaaja üksuse andmeid;
2) sõjaaja ametikoha andmeid;
3) sõjaaja üksuse varustatuse andmeid.
(3) Mobilisatsiooniregistri põhimääruse kehtestab Vabariigi Valitsus määrusega.
(4) Mobilisatsiooniregistri vastutav töötleja on Kaitseministeerium.
(5) Mobilisatsiooniregistris töödeldakse isikuandmeid, sealhulgas eriliiki isikuandmeid.

Mobilisatsiooniregistri põhimääruses on aga sätestatud, et sõjaaja ametikohale nimetatud isiku kohta kantakse registrisse mh omandatud või omandatav haridustase; mootorsõiduki juhtimisõigus; töö- või ametikoht; veregrupp ja reesusfaktor; vastavus tervisenõuetele; antropomeetrilised andmed (§ 5 lg 3).

Tsiviiltoetuste registri kohta on seaduse tasandil reguleeritud järgnevalt:

RKSKS § 4^2. Tsiviiltoetuse register
(1) Tsiviiltoetuse register on andmekogu, milles peetakse arvestust riigikaitseks, vastuvõtva riigi toetuse osutamiseks ja tsiviil-sõjaliseks koostööks vajalike vahendite üle, elutähtsa teenuse osutajate, riigikaitselisi ameti- ja töökohti omavate tööandjate ning sundkoormise määramise ja täitmise üle. Tsiviiltoetuse registris töödeldakse isikuandmeid.
(2) Tsiviiltoetuse registri vastutav ja volitatud töötleja on Kaitseressursside Amet.
(2^1) Elutähtsa teenuse osutaja arvestuse puhul on volitatud töötleja elutähtsa teenuse toimepidevust korraldav asutus.
(3) Tsiviiltoetuse registri põhimääruse kehtestab Vabariigi Valitsus määrusega.

Tsiviiltoetuste registri põhimääruse kohaselt kantakse registrisse erinevate liiklusvahendite, õhu- ja veesõidukite omanike, vastutavate kasutajate, tegelike kasutajate andmeid, samuti muude objektide valdajate andmeid.

Ka politsei andmekogu POLIS puhul ei ole seaduse ja määruse tasakaal paigas. PPVS § 8 lg 1 sätestab: „Politsei andmekogu on andmekogu, kus töödeldakse korrakaitse ja süüteomenetlusega seotud andmeid avaliku korra ja siseturvalisuse tagamise eesmärgil.“.

PPVS § 10. Politsei andmekogu ülesehitus ja andmekogusse kantavad andmed
(1) Politsei andmekogu koosneb järgmistest andmestikest:
1) ühiste infoobjektide andmestik;
2) süüteomenetluse andmestik;
3) korrakaitseliste ülesannetega seotud haldustegevuse andmestik;
4) ennetava tegevuse andmestik;
5) reageeriva tegevuse andmestik;
6) arestimajade tegevuse andmestik;
7) otsimise andmestik;
8) jälitusmenetluse andmestik.

Andmekogu alamandmekogude eesmärgid on seaduse tasemel määratlemata. Ennetava tegevuse andmestikku salvestab politsei muuhulgas tähelepanekuid tõenäoliselt tulevikus toimepandava õiguserikkumise kohta ja sellega seotud isikute, ettevõtjate, sõidukite kohta; samuti hinnangulisi ohumärkeid piirkonnas tegutsevate isikute, kes on toime pannud või tõenäoliselt tulevikus paneb toime õiguserikkumise, kohta.[155] Vahemärkusena olgu tõdetud, et

[155] Politsei andmekogu põhimääruse § 10 lg 2.

süütegude ennetamise ja menetlemise eesmärgil isikuandmete töötlemist reguleeriv direktiiv peab isikute, kes politsei hinnangul tulevikus võivad toime panna õiguserikkumise, töötlemist andekogus võimalikuks,[156] ent olulisuse põhimõttest lähtuvalt peab see olema sätestatud seaduse tasemel.

AKI-le teadaolevalt oli POLISe ennetava tegevuse andmestikus 2011.aastal 55 miljonit kirjet.[157] Andmekogude juhendis on AKI kritiseerinud, et seaduse tasandil on täielikult lahtiseks jäetud politseiväliste andmeandjate loetelu, samuti andmesaajate loetelu. Nende oluliste küsimuste asemel on seadusse toodud aga ebaolulisi tehnilisi asjaolusid – nii sätestab seadus, et andmekogu pidamiseks tuleb kasutada tarkvara:[158]

PPVS § 12. Politsei andmekogusse kande tegemine

(1) Andmed kantakse politsei andmekogusse selle kasutamiseks loodud tarkvara abil.

Et isikuandmete töötlemisel tuleb arvestada põhiõiguste riivega, ei ole andmekogude puhul, mis sisaldavad isikuandmeid, põhiseaduspärane tugineda ka üldvolitusele, näiteks:

Välissuhtlemisseaduse § 9

(14) Käesoleva paragrahviga Välisministeeriumile pandud ülesannete täitmiseks ja töö korraldamise tagamiseks vajalike andmekogude asutamise otsustab ja selliste andmekogude põhimäärused kehtestab valdkonna eest vastutav minister.

Sellise üldvolituse alusel on antud rida erinevate andmekogude põhimäärusi, seejuures näiteks Eeltäidetud viisataotluse andmekogu asutamine ja andmekogu põhimääruse § 6 p 33 reguleerib biomeetriliste andmete (sõrmejäljed) säilitamist.

---

[156] Direktiiv 2016/680 artikkel 6
Andmesubjektide eri kategooriate eristamine
Liikmesriigid näevad ette, et asjakohasel juhul võimaluste piires eristab vastutav töötleja isikuandmeid selgelt andmesubjektide eri kategooriate kaupa, nimelt:
a) **isikud, kelle puhul on tõsine alus arvata, et nad on toime pannud või panevad varsti toime süüteo**;
b) isikud, kes on süüteos süüdi mõistetud;
c) süüteoohvrid ja isikud, kelle puhul teatavad asjaolud annavad alust arvata, et nad võivad olla süüteo ohvrid, ning
d) süüteoga seotud muud isikud, näiteks isikud, keda süüteo uurimise või sellele järgneva kriminaalmenetluse käigus võidakse kutsuda tunnistusi andma, isikud, kellelt võib saada teavet süüteo kohta, ning punktides a ja b osutatud isikute kontaktisikud ja kaasosalised.

[157] AKI 2011.a tegevuse ülevaade, lk 58. Politsei andmekogu põhimääruse § 24 lg 3 sätestab, et politsei ennetava tegevuse andmestiku andmeid säilitatakse alljärgnevalt:
1) piirkondlikke infoteateid 3 aastat andmete infosüsteemi kandmisest arvates;
2) õigusevastase teo toime pannud alaealise kohta kuni tema täisealiseks saamiseni;
3) numbrituvastuskaamera teadet, mis ei ole seotud infosüsteemi teise andmestikuga, kuni 3 kuud teate saabumisest arvates;
(8) Käesoleva paragrahvis sätestatud säilitustähtaegade möödumisel kantakse andmed arhiivi, välja arvatud lõike 3 punktis 2 nimetatud andmed, mis säilitustähtaja möödumisel kustutatakse.
§ 25. Infosüsteemi arhiiv
(1) Arhiveeritud andmeid säilitatakse digitaalselt.
(2) Arhiivist on õigus saada andmeid:
1) politseiametnikul ja muul isikul põhjendatud teadmisvajadusel;
2) andmesubjektil tema kohta käivaid andmeid.

[158] AKI andmekogude juhend, lk 9.

Samas leidub kehtivas õiguses regulatsioone, nagu näiteks haigekassa andmekogu regulatsioon haigekassa seaduse §46[1] jj, milles on lisaks eesmärgile seaduse tasemel sätestatud säilitustähtajad ja andmekoosseisud konkreetsemalt; samuti töövõimetoetuse seaduse §-s 22 töövõime hindamise ja töövõimetoetuse andmekogu.

§ 22. Töövõime hindamise ja töövõimetoetuse andmekogu
(1) Töövõime hindamise ja töövõimetoetuse andmekogu (edaspidi andmekogu) peetakse töövõime hindamiseks, töövõimetoetuse maksmiseks, osalise või puuduva töövõimega töötaja eest sotsiaalmaksu erijuhtudel maksmiseks ning statistika ja analüüside tegemiseks vajalike andmete tagamiseks.
(2) Andmekogu vastutav töötleja on töötukassa.
(3) Andmekogu sisaldab ja selles töödeldakse **järgmisi andmeid**:
1) töövõime hindamist ja töövõimetoetust taotleva isiku andmed – nimi, sünniaeg ja sugu või isikukood, kontaktandmed, kodakondsus, elamisloa või elamisõiguse kehtivusaeg ning rahvusvahelise kaitse saaja või varjupaiga taotleja seisund;
2) töövõime hindamise andmed;
3) töövõimetoetuse andmed;
4) sotsiaalmaksu maksmise erijuhtude üle arvestuse pidamise andmed;
5) andmeandjate loetelu ja nendelt saadavad andmed.
(4) Andmekogu asutab ja selle põhimääruse kehtestab valdkonna eest vastutav minister määrusega.
(5) Andmekogusse kantud andmeid **säilitatakse järgmiselt**:
1) töövõime hindamise andmeid nende andmekogusse kandmisest kuni kümme aastat pärast isiku surma;
2) töövõimetoetuse ja erijuhtudel sotsiaalmaksu maksmise andmeid nende andmekogusse kandmisest kuni kümme aastat pärast isiku suhtes alustatud käesolevas seaduses sätestatud menetluse lõppemist või isiku surma;
3) andmekogusse kantud andmed pseudonüümitakse kord aastas säilitustähtaja möödumise kalendriaasta lõpus.
(6) Andmekogusse kantud pseudonüümitud andmed säilitatakse 65 aastat, mille möödumisel andmed anonüümitakse kord aastas säilitustähtaja möödumise kalendriaasta lõpus.
(7) Täpsemad säilitustähtajad ja säilitamise tingimused ning kord sätestatakse andmekogu põhimääruses.

Seega seaduses tuleb sätestada isikuandmete üldised grupid (nt isiku kontaktandmed, isiku haridust ja tööd puudutavad andmed, terviseandmed), **mis annab määrusandjale raamid volituse ulatuse ja piiride osas**; ehk teisisõnu, määruses saab täpsustada, et milliseid nendesse gruppidesse kuuluvaid andmeid kogutakse (nt töökoht, tööle asumise aeg ja lahkumise aeg jne).

Vahejäreldus:

Kui andmekogu sisaldab isikuandmeid, peab seaduse tasemel olema sätestatud:

- **milliseid isikuandmeid andmekogusse kogutakse**
- **mis eesmärgil neid andmeid kogutakse ja veel kasutatakse selle sama haldusorgani poolt**
- **kui kaua neid säilitatakse.**

Üksikasjade täpsustamiseks võib volitada määrusandjat (PS § 87, 94).

2.3.2. Teiste asutuste otsejuurdepääsud kui põhiõiguste riive

Andmekogude regulatsioon AvTS-is ei nõua, et konkreetse andmekogu regulatsioon peaks sisaldama seda, milline haldusorgan ja milliseks konkreetseks eesmärgiks ja ülesandeks teise

andmekogu andmeid ristkasutab. 2008.a andmekoguõiguse reformi idee oligi luua ühtne andmeruum. Kujunes tänaseni kehtiv praktika, kus andmete ristkasutusel lähtutakse teise haldusorgani pädevusnormidest ning paljudel juhtudel ei reguleeri ristkasutust isegi mitte põhimäärus, vaid otsejuurdepääs luuakse asutuste omavahelise lepingu alusel (põhjalikumalt ülal).

AvTS-s nähti siiski ette kohustus sätestada üksnes andmeandjad.

AvTS § 43[5]. Andmekogu põhimäärus

(1) Andmekogu põhimääruses sätestatakse andmekogu pidamise kord, sealhulgas andmekogu vastutav töötleja (haldaja) ja vajaduse korral volitatud töötleja, andmekogusse kogutavate andmete koosseis, **andmeandjad** ja vajaduse korral muud andmekogu pidamisega seotud korralduslikud küsimused.

IKÜM art 5 lg 1 p b nõuab, et isikuandmeid kogutaks täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel. Kui riik lubab ühel konkreetsel eesmärgil kogutud isikuandmeid töödelda ka teiste asutuste poolt teistel eesmärkidel, vajab ka see põhiseadusele (ja hartale) vastavat reguleerimist – ka teiste asutuste päringud või andmete laadimine juba uutesse andmekogudesse kujutab endast põhiõiguste riivet. Ka ELPH-st tulenev põhiõigus isikuandmete kaitsele nõuab, et isikuandmeid töödeldaks vaid „kindlaksmääratud eesmärkidel".

Seetõttu on küsitav, kas see, kui juurdepääsusid hakatakse reguleerima määruse tasandil, kuid volitusnorm lubab üksnes andmekogu asutada, on üldse volitusnormiga hõlmatud.

Näiteks kui PPVS § 8 lg 4 sätestab: „Politsei andmekogu põhimääruses sätestatakse politsei andmekogu pidamise kord, politsei andmekogusse kogutavate andmete täpsem koosseis, andmeandjad, andmete säilitamise tähtajad ja vajaduse korral muud politsei andmekogu pidamisega seotud korralduslikud küsimused". Seetõttu tekib küsimus, kas see, kui siseministri määrusega kehtestatud POLISe põhimääruse §-s 19 on antud juurdepääsud ka teistele asutustele, on kaetud volitusnormiga. Riigikohus on rõhutanud: „Põhiseaduse § 3 kohaselt teostatakse riigivõimu üksnes põhiseaduse ja sellega kooskõlas olevate seaduste alusel. Määrusandluse puhul tähendab nimetatud säte täitevvõimu jaoks kohustust järgida talle delegatsiooninormiga antud volitusi ja neid mitte ületada. HMS § 90 lg 1 kohaselt võib määruse anda ainult seaduses sisalduva volitusnormi olemasolul ja kooskõlas volitusnormi piiride, mõtte ja eesmärgiga. Kohtupraktikas on rõhutatud, et volitusnormis sätestatakse määrusandliku volituse selge eesmärk, sisu ja ulatus (põhiseaduslikkuse järelevalve kolleegiumi 20. detsembri 1996. a otsus asjas nr 3-4-1-3-96).".[159]

Justiitsministeeriumile on tehtud ettepanek lisada avaliku teabe seadusesse üldvolitus, mis võimaldaks avaliku ülesande täitmise käigus andmekogusse kogutud andmeid kasutada teiste asutuste andmekogude poolt avaliku ülesande täitmiseks üle x-tee, kui nende andmete kasutamist pole seadusega piiratud (maksusaladus, ärisaladus jne.). Kui sätestada põhimääruses, milliste teiste andmekogude andmetele antakse otsejuurdepääs, kirjutatakse MKM hinnangul paindliku teenuste arendamise võimalused põhimäärustega lukku, mis raskendaks tehisintellekti kasutuselevõttu ning andmete „avastamisest" tulenevat uute kasutusjuhtude ja kasu leidmist, kuivõrd kõiki rakendusvõimalusi ei ole võimalik ette teada.[160]

[159] RKHK 19.01.2009, 3-3-1-85-08, p 18.

[160] Majandus- ja kommunikatsiooniministeeriumi 30.09.2020 kiri nr 2-15/2020/5111-2 „Vastus Justiitsministeeriumi algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsusele („krati VTK")", lk 10-11. Kättesaadav eelnõude infosüsteemis.

Põhiõiguste seisukohast lähtuvalt ei saa siiski toetada ettepanekut luua AvTS-i üldvolitust andmete ristkasutamiseks. [161]

Isikuandmete töötlemise eesmärgimääratlus ei ole tülikas bürokraatlik nõue, vaid teenib otseselt põhiõigust isikuandmete kaitsele (vt EL põhiõiguste harta art 8 lg 2) ja informatsioonilisele enesemääramisele (PS § 26 ja 19), kaudselt ka inimväärikuse põhimõtet. Informatsioonilise enesemääramise põhiõigus ei ole tagatud, kui inimene ei tea, millistel eesmärkidel veel tema isikuandmeid töödeldakse, millega neid kombineeritakse, mis järeldusi ja kelle poolt nende pinnalt tehakse ja kuidas see teda mõjutada võib. See võib omakorda mõjutada inimest loobuma ka teiste põhiõiguste teostamisest, mis võib omakorda ohustada lausa demokraatlikku riigikorda kui sellist.

Kui seda, kes ja millisel uuel eesmärgil asub otsejuurdepääsu kaudu isikuandmeid töötlema, ei sätestata seaduses ega määruses, toob see kaasa olukorra, kus andmetöötlus on täiesti läbipaistmatu ning sõltub ainuüksi täidesaatva võimu otsustest.

Seetõttu on küsitav ka, kas andmekogule teisele asutusele otsejuurdepääsu andmisel saaks tugineda näiteks HMS § 7 lõikele 5, mis sätestab isikuandmete töötlemise üldvolituse haldusmenetluses: „haldusorgan võib haldusmenetluses haldusakti andmise, toimingu tegemise või halduslepingu sõlmimise eesmärgil töödelda isikuandmeid menetletavas asjas vajalike asjaolude kohta, kui seadusega või selle alusel antud õigusaktidega ei ole ette nähtud teisiti“. EL seadusandja on siiski eeldanud, et isikuandmete väljastamine või juurdepääsu võimaldamine teisele haldusorganile tuleb sätestada õigusselgel viisil. Vastasel korral tuleb puudutatud isikuid iga kord, kui nende andmeid töödeldakse teise asutuse poolt, sellest teavitada.[162]

Eesmärgipärasust ja töötlemise läbipaistvust on rõhutanud ka Eesti informaatikateadlane Dan Bogdanov, kelle sõnul: „Eestis juurutatud *once only* põhimõtte valguses peaks olema avalikkusele läbipaistev, millistel teisese kasutuse eesmärkidel ühtesid ja samu isikuandmeid töödeldakse. /---/ Kodaniku vaatest on oluline jälgida, et andmetele juurdepääs oleks eesmärgipärane ja piisavalt kontrollitud ega väljuks põhiseadusega kehtestatud raamidest.“[163]

Vahejäreldused:

- Eriliiki isikuandmete puhul, samuti muude tundlikemate andmekogude puhul (näiteks POLIS) tuleb sätestada seaduse tasandil, milline haldusorgan ja millisteks ülesanneteks neid andmeid veel otsejuurdepääsu kaudu kasutab.
- Vähemtundlikemate isikuandmete puhul võib seadusandja volitada selle otsuse ka määrusandjale. Sel juhul sätestatakse andmekogu põhimääruses, milline haldusorgan ja millisteks ülesanneteks isikuandmeid veel otsejuurdepääsu kaudu kasutab.
- Määrusest allapoole teiste haldusorganite otsejuurdepääsude otsustamist delegeerida ei saa. Andmekogud, mille puhul on seda tehtud, tuleb põhiseaduse nõuetega kooskõlla viia.

[161] Üldsäte, mis võimaldaks avaliku ülesande täitmise käigus andmekogusse kogutud andmeid kasutada teiste asutuste andmekogude poolt avaliku ülesande täitmiseks üle x-tee, kui nende andmete kasutamist pole seadusega piiratud (maksusaladus, ärisaladus jne.).

[162] Vt IKÜM art 14 lg 5 p c.

[163] D. Bogdanov, T. Siil. Infotehnoloogilised võimalused põhiõiguste kaitsel. Juridica 2020, nr 6, lk 480.

2.3.3. Andmekogu isikuandmete väljastamine teise haldusorgani põhjendatud taotluse alusel

Kui andmekogu andmete ristkasutus andmevahetuskihi kaudu toimub juhul, kui teisel haldusorganil on **püsiv vajadus** neid andmeid kasutada (näiteks liikluspolitsei ja liiklusregistri andmed), siis küsitav on, kas juhul, kui teisel haldusorganil tekib pigem erandjuhul vajadus oma menetluses kasutada muu haldusorgani andmekogus olevaid isikuandeid, tuleks talle seda võimaldada, hoolimata sellest, et andmekogu regulatsioon sellist isikuandmete töötlemist ette ei näe. Sellist üksikjuhtumil esitatavat päringut mainitakse eraldi ka üldmääruses:

„Avaliku sektori asutusi, kellele avaldatakse isikuandmeid vastavalt juriidilisele kohustusele täita oma ametiülesandeid, näiteks maksu- ja tolliasutused, finantsuurimisüksused, sõltumatud haldusasutused või finantsturuasutused, kes vastutavad väärtpaberiturgude reguleerimise ja järelevalve eest, ei peaks pidama vastuvõtjateks, **kui nad saavad isikuandmeid, mida vajatakse üldistes huvides konkreetse päringu tegemiseks kooskõlas liidu või liikmesriigi õigusega.** Avaliku sektori asutuste saadetavad andmete avaldamise taotlused **peaksid olema alati kirjalikud, põhjendatud ja juhtumipõhised** ning **need ei tohiks puudutada kogu andmete kogumit** või **põhjustada andmete kogumite omavahelist ühendamist**.“.

On kaheldav, kas teise haldusorgani taotlus isikuandmete saamiseks saaks tugineda halduskoostöö seaduses (HKTS) sätestatud ametiabi regulatsioonile, mille § 18 lg 1 p 2 kohaselt võib haldusorgan taotleda teiselt haldusorganilt ametiabi, „kui haldusülesande täitmiseks on vaja andmeid, mis haldusorganil puuduvad või mida haldusorgan ei ole võimeline välja selgitama“ ning p 3 kohaselt „kui haldusülesande täitmiseks on vaja teise haldusorgani valduses olevaid dokumente või muid tõendeid“.

Ametiabi õiguslikke küsimusi analüüsinud I.Pilvingu peab isikuandmete edastamist ametiabi korras problemaatiliseks just eesmärgikohasuse ja minimaalsuse põhimõtte valguses. Pilvingu hinnangul võis aluse isikuandmete edastamiseks ametiabi raames tuletada IKS (2008-2019) § 14 lõike 2 punktist 1, kuid Pilvingu hinnangul tuleks tundlikemate andmete puhul (eeskätt eriliiki isikuandmed) niisugune kohustus täpsemalt sätestada. Pilving rõhutas ka, et IKS (2008-2019) § 15 lõikest 1 tulenevalt tuleb üldjuhul andmesubjekti andmete edastamisest teavitada, sellest kohustusest ei ole ametiabi andmisel erandit kehtestatud.[164] IKS (2008-2019) § 14 lg 2 p 1 kohaselt oli isikuandmete edastamine või nendele juurdepääsu võimaldamine andmete töötlemiseks kolmandale isikule on lubatud andmesubjekti nõusolekuta, kui kolmas isik, kellele andmed edastatakse, töötleb isikuandmeid seaduse, välislepingu või Euroopa Liidu Nõukogu või Euroopa Komisjoni otsekohalduva õigusaktiga ettenähtud ülesande täitmiseks.

Sarnane üldvolitus on sätestatud HMS § 7 lg 5, mille kohaselt haldusorgan võib haldusmenetluses haldusakti andmise, toimingu tegemise või halduslepingu sõlmimise eesmärgil töödelda isikuandmeid menetletavas asjas vajalike asjaolude kohta, kui seadusega või selle alusel antud õigusaktidega ei ole ette nähtud teisiti. Üldvolituse alusel ei saa siiski küsida välja eriliiki isikuandmeid vmt tundlikke isikuandmeid, mille puhul on seadusandja ammendavalt sätestanud andmetele juurdepääsu eesmärgid.

Vahejäreldused:

[164] I. Pilving. Ametiabi. Juridica 2015, nr 3, lk 182.

- Asutus saab teiselt asutuselt oma menetluse jaoks välja küsida, kui selleks on õiguslik alus (näiteks politsei süüteomenetluses, kohus), millest nähtub, et sel asutusel on õigus küsida andmeid teiste asutuste isikuandmeid. Haldusmenetluse puhul peaks õigusnormid reguleerima ka, milliste konkreetsete asjaolude kohta tõendeid kogutakse.

2.3.4. Andmekogu isikuandmete juurdepääsupiirangud ja avalikustamine

Avaliku teabe seaduse koostamisel lähtuti põhimõttest, et avalik teave AvTS § 3 lg 1 tähenduses jaguneb kolmeks:

1) teave, mis tuleb seaduse kohaselt aktiivselt (veebis) avalikustada;
2) teave, mille suhtes kehtib juurdepääsupiirang („AK-teave“);
3) teave, mis ei ole avalikustatud, kuid mis väljastatakse teabenõude korras.

AvTSi seletuskirjas selgitatakse, et „[k]ui teabenõude täitmise puhul on tegemist nn passiivse-teabele juurdepääsu võimaldamisega, siis teabe avalikustamine eeldab teabe aktiivset pakkumist teabevaldaja poolt“.[165]

2.3.4.1. Andmekogu andmete juurdepääsupiirangu alus

AvTS § 43[8] lg 1 sätestab, et andmekogus töödeldavad andmed peavad olema avalikult kättesaadavad, kui neile ei ole seadusega või selle alusel kehtestatud juurdepääsupiirangut. Ka AvTS § 3 lg 2 näeb ette, et teabele juurdepääsu võib piirata seaduses sätestatud korras.

Mõnel juhul on juurdepääsupiirang kehtestatud andmekogu põhimääruses, samal ajal, kui andmekogu asutamist reguleeriv seadus seda küsimust ei reguleeri. Näiteks POLISe põhimääruse art 3 lg 2 sätestab:

„Infosüsteem on piiratud juurdepääsuga ja infosüsteemi andmed on ainult ametialaseks kasutamiseks, kui käesolevas määruses ei ole sätestatud teisiti.“.[166]

AvTS § 43[8] lg 1 ei anna aga määrusandjale õigust otsustada juurdepääsupiirangute kehtestamise üle. Andmekogude juhendis selgitatakse seda järgnevalt: „AvTS võimaldab teabele, sh andmekogudele, juurdepääsupiirangu seada **kas AvTS § 35 alustel või eriseaduse alusel.** Seega peabki eriseaduses vajadusel sätestama erinormina AvTS-ist andmete juurdepääsupiirangu. Juurdepääsupiirangu norm peab olema **konkreetne ja selge ning sellest peab selguma, miks juurdepääsupiirang kehtestatakse.**“.

Kui andmekogu asutamist reguleerivas seaduses ei ole andmekogus olevate andmete avalikkust või piiranguid eraldi reguleeritud, kehtivad andmekogus sisalduvate andmete suhtes AvTS § 35 sätestatud juurdepääsupiirangud, samuti AvTS §-d 36 - 43.

[165] Avaliku teabe seadus 462 SE seletuskiri, lk 19.
[166] Vrd ka tsiviiltoetuse registri põhimääruse § 34 lg 1.

Seega on eksitav, kui andmekogu põhimääruses sätestada üldsõnaliselt, et andmekogu andmed on juurdepääsupiiranguga. See tuleb ette näha seaduse tasemel või kehtestab teabevaldaja juht andmekogus sisalduvale teabele juurdepääsud AvTS § 41 kohaselt.

2.3.4.2. Andmekogu isikuandmete aktiivne avalikustamine

AvTS § 28 lg 1 p 30 ja § 29 lg 1 tuleneb, et teabevaldaja on kohustatud avalikustama veebilehel andmekogudes sisalduvad andmed, millele ei ole kehtestatud juurdepääsupiirangut.

Seletuskirja kohaselt lähtub säte avaliku teabe seaduse üldisest põhimõttest, mille kohaselt kogu avalik teave (st avalike ülesandeid täites saadud või loodud teave), mis ei ole juurdepääsupiiranguga teave, on avalik.[167] Sellest sättest ei saa siiski tuletada teabevaldaja kohustust avaldada aktiivselt mistahes isikuandmed, millel puudub juurdepääsupiirang. Teabele juurdepääsu võimaldamisel peab olema tagatud isiku eraelu puutumatus (AvTS § 4 lg 3). Isikuandmed on eraelu puutumatuse kaitsealas (vt põhjalikumalt ülal p 2.1). Nii näiteks on AvTS §-s 36 kehtestatud ka loetelu andmetest, millele on keelatud juurdepääsupiirangut kehtestada (sh näiteks ettekirjutused). Ent juba AvTSi seletuskirjas on selgitatud, et kui näiteks tekib vastuolu juurdepääsupiirangu ja AvTS § 36 vahel, „siis eraldatakse ja tagatakse juurdepääs ainult nendele andmetele [---], millele juurdepääsupiirangud ei kehti“.[168] Ka Riigikohus on leidnud, et teabe aktiivsel avalikustamisel tuleb eelistada tõlgendust, mille puhul ei esineks eraelu riivet ja avaldada teave mitteisikustatud kujul.[169] **Isikuandmete aktiivne avalikustamine on lubatav üldjuhul vaid siis, kui see on seadusandja poolt selge sõnaga ette nähtud.**

Riigikohus on sellega seoses möönnud, et teabe passiivne avalikustamine ei vaja sama selget alusnormi: „Asjaolu, et ATS § 65 ja AvTS § 28 lg 1 p 25 näevad 1. aprillist 2013 ette ametniku palga aktiivse avalikustamise, võimaldab vaid järeldada, et töötaja töötasu ei tule aktiivselt avalikustada veebilehel. See tõdemus ei anna vastust passiivse avaldamise, s.o teabenõude vastusena teabe väljastamise kohta.“.[170]

Siinkohal tuleb samuti meeles pidada, et isikuandmeteks loetakse mitte üksnes otseselt (ees- ja perekonnanime kaudu) tuvastatava inimese andmed, vaid ka kaudsete tunnuste alusel tuvastatavad andmed.[171] Euroopa Kohus on selgitanud, et „Liidu seadusandja poolt sõna „kaudselt“ kasutamisega soovitakse näidata, et isikuandmeteks määratlemiseks ei pea need andmed ise võimaldama kõnealust isikut tuvastada.“.[172] IKÜM põhjenduspunktis 26 on täpsustatud, et „Füüsilise isiku tuvastatavuse kindlakstegemisel tuleks arvesse võtta kõiki vahendeid, mida vastutav töötleja või keegi muu võib füüsilise isiku otseseks või kaudseks tuvastamiseks mõistliku tõenäosusega kasutada, näiteks teiste hulgast esiletoomine. Selleks et teha kindlaks, kas füüsilise isiku tuvastamiseks võetakse mõistliku tõenäosusega meetmeid, tuleks arvestada kõiki objektiivseid tegureid, näiteks tuvastamise maksumus ja selleks vajalik aeg, võttes arvesse nii andmete töötlemise ajal kättesaadavat tehnoloogiat kui ka tehnoloogilisi arenguid.“. Euroopa Kohtu seisukoha järgi „isikuandmeteks“ määratlemisel ei ole nõutud, et kõik isikut tuvastada võimaldavad andmed oleksid ühe isiku valduses.[173] Vastavaid andmeid ei saa lugeda

[167] Avaliku teabe seaduse ja sellega seonduvate seaduste muutmise seadus 1027 SE seletuskiri, lk 16.
[168] Avaliku teabe seadus 462 SE seletuskiri, lk 21.
[169] RKPJKm 19.05.2009, nr 3-4-1-1-09, p 19.
[170] RKHKo 17.10.2018, nr 3-15-3228, p 12.
[171] Vt isikuandmete mõistet IKÜM art 4 p 1.
[172] EKo C-582/14, p 41.
[173] Samas, p 43.

kaudselt tuvastatavateks isikuandmeteks üksnes juhul, „kui asjaomase isiku tuvastamine oleks seadusega keelatud või praktiliselt teostamatu, kuna see nõuaks nii ajaliselt, majanduslikult kui ka inimressursside poolest ülemäärast jõupingutust, nii et tuvastamise risk näib tegelikkuses olevat olematu.“.[174]

Näiteks kui andmekogu andmete pinnalt kavatsetakse luua mingi veebirakendus või portaal, milles kavatsetakse avalikustada näiteks konkreetsed aadressid koos vastava aadressiga seotud ettekirjutustest tulenevate kohustustega, tuleb arvestada, et vaid kinnistusregistris on igaühel võimalik saada teada selle aadressi omanik, tasudes vaid sümboolse tasu (1 eur). Seega konkreetsete aadressidega seonduva täiendava teabe avalikustamisel on samuti tegemist isikuandmete avalikustamisega (juhul, kui omanik on füüsiline isik), mis vajab seadusest tulenevat alust, mis on omakorda õigusselge ja vastab proportsionaalsuse põhimõttele.

Vahejäreldused:

- **Andmekogu asutamisel analüüsida, kas AvTS-s sätestatud juurdepääsupiirangu alused on piisavad või on vaja seaduse tasemel kehtestada eraldi juurdepääsupiirang.**
- **Kui isikuandmetele juurdepääsupiirangut ei kehtestata, ei tähenda see automaatselt isikuandmete aktiivset avalikustamist.**
- **Isikuandmete aktiivseks avalikustamiseks on eraelu puutumatuse intensiivsema riive tõttu nõutav õigusselguse põhimõttele ja proportsionaalsuse põhimõttele vastav õiguslik alus.**

2.3.5. Erinevate andmekogude andmesõelumine lauspäringutega

Andmekaitse Inspektsioon tõstatas oma 2015. aasta aastaülevaates seoses maksukorralduse seaduse muutmise eelnõuga[175] õigustatult küsimuse: „Millises ulatuses võib korrakaitseorgan KoRS § 5 lg 7 alusel kasutada kõikvõimalike andmekogude andmeid üleüldiseks riskianalüüsiks?“.[176]

KorS § 5 lg 7: „Ohu ennetamine on see osa korrakaitsest, kus puudub ohukahtlus, kuid saab pidada võimalikuks olukorda, mille realiseerumisel tekib ohukahtlus või oht. Ohu ennetamine on muu hulgas **teabe kogumine, vahetamine ja analüüs**, toimingute kavandamine ja elluviimine ning riikliku järelevalve meetmete kohaldamine avalikku korda tulevikus ähvardada võivate ohtude tõrjumiseks, sealhulgas süütegude ennetamine.“.

AKI esitas samas ka oma seisukoha: *„Meie hinnangul seondub muudatus ka laiema, põhimõttelise küsimusega, kuivõrd võib korrakaitseorgan ohu ennetamiseks kasutada andmekogusid (ja veel laiemalt, kuivõrd võib sel eesmärgil andmeid andmekogusse koguda ja säilitada). And-*

[174] Samas, p 46.

[175] Nimelt „sooviti eelnõuga sätestada maksukorralduse seaduses maksuõigusrikkumise riski hindamine (MKS täiendamine §-dega 63 lg 21 ja 59 lg 21) ning kasutada selleks andmekogudes olevaid andmeid. Tegime ettepaneku sõnastada andmekogude kasutamise eesmärk täpsemalt, et oleks aru saada, millisel juhul maksuõigusrikkumise hindamine (ja selleks andmekogust andmete päring) aset leiab.“ Andmekaitse Inspektsioon. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest aastal 2015 ja soovitused aastaks 2016, lk 60.

[176] Samas, lk 60.

mekogust andmete nõudmist korrakaitseseadus meetmena ei nimeta, kuid sätestab § 30 lõikes 5, et isikult dokumentide esitamise nõudmine ei ole lubatud, kui teavet on võimalik saada andmekogust. Samas KorS §-st 24 ja § 5 lõikest 7 tuleneb, et riikliku järelevalve erimeetmeid võib kasutada ohu ennetamiseks, kui ohuprognoosile tuginedes saab pidada võimalikuks olukorda, mille realiseerumisel tekib oht (st veel puudub konkreetne ohukahtlus). KorS § 5 lg 7 samas räägib, et ohu ennetamine on mh teabe kogumine, vahetamine ja analüüs. Sisejulgeoleku valdkonna andmekogude puhul on tavaline, et andmeid kogutaksegi (nt broneeringuinfo andmekogu, majutusteenuse kasutajate andmete säilitamiskohustus) või säilitatakse pikema perioodi vältel (nt viisaregister, piirikontrolli andmekogu) selleks, et kasutada neid õigusrikkumiste avastamiseks. Tekib küsimus, kas KorS § 5 lg 7 alusel võikski korrakaitseorgan kõikvõimalike andmekogude andmeid kasutada üleüldiseks ohtude väljaselgitamiseks (maksukorralduse seaduse eelnõu mõttes riskihindamiseks). Sisuliselt tähendab see massjälgimise ja massandmetöötluse lubatavust, mida näiteks EL institutsioonid ei ole pidanud lubatavaks (nt Euroopa Kohtu otsused Safe Harbouri ning andmesäilitusdirektiivi osas). Teisalt on EL ise tolliõiguses ette näinud riskihindamise kohustuse ning broneeringuinfo direktiivi ettepanekus broneeringuinfo massedastuse ning analüüsi. Viimase osas märgime, et broneeringuinfo andmekogu põhimääruse eelnõuga soovitakse anda Maksu- ja Tolliametile ka püsiv otsejuurdepääs broneeringuinfole (tõsi, andmete kasutamine on riigipiiri seaduse kohaselt piiratud raskete kuritegude menetlemise, avastamise ja ärahoidmisega).“.[177]

Sama problemaatika käsitlemist jätkas AKI oma 2016. aasta ülevaates, kus tõdeti, et vahepeal toimunud kohtumisel avaldas Justiitsministeeriumi esindaja arvamust, et KorS § 5 lõige 7 ei ole siiski käsitletav üldise õigusliku alusena kõigi andmekogude kõikvõimalikuks järelevalve otstarbeliseks massandmetöötluseks ning et sellekohane norm on korrakaitseseadusest lihtsalt puudu.[178] Aastaraamatu sissejuhatus rõhutas AKI toonane peadirektor V.Peep: „Üldiselt suhtutakse elanikkonna lausjälgimisse eitavalt. Euroopa Liidu Kohus on seda korduvalt väljendanud, sh sidevõrkude jälgimise osas. Üldine arusaam on, et kui kõik või suur osa inimestest on võimuasutuste pideva andmetraalimise objektiks ilma selleks põhjust andmata, tekib ühiskonnas hirmupaine. Inimene, kes teab, et salasilm võib teda iga hetk luurata, ei käitu enam loomulikult ja muutub manipuleeritavaks. Lausjälgimisest tekkinud andmemassiiv on omakorda väärkasutusriski allikaks,“[179] esitades samas ka konkreetsed ettepanekud ohuennetuse eesmärgil massandmetöötluse reguleerimiseks:

„Regulatsiooni loomisel tuleks anda vastused järgmistele küsimustele:

1. Kas andmekogude kombineerimine massandmetöötluseks tuleks sätestada KoRSis üldise erimeetmena, mille kasutamiseks võib iga eriseadus õiguse anda; KorSis piiratud korrakaitseasutustele kasutatava erimeetmena; kindla valdkonna eriseaduses erimeetmena;

2. Millised on tingimused ja garantiid, et selle meetme kasutamine oleks proportsionaalne. Näiteks:

- mis eesmärgil sellist meedet kasutada võib – kas ainult juba toimunud rikkumiste avastamine või ka ennetamine ja tõkestamine ning suisa ohuprognoosi koostamine;
- millega on piiritletud – ainult kuriteod, väärteod, oluline oht vms;

[177] Samas, lk 60-61.
[178] M.Juha. Õigusaktide eelnõud. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2016. Aastal. Soovitused aastaks 2017. Lk 62.
[179] V.Peep. Kokkuvõte ja soovitused peadirektorilt. Lk 11.

- kas hõlmab ainult riigi infosüsteemi kuuluvaid riigi- ja omavalitsuse andmekogusid, st mitte eraõiguslikke, kes avalikke ülesandeid ei täida (nt pangad);
- ei saa laieneda kõikidele andmekogudele (nt sõrmejälgede ja DNA register, e-tervis ei saa kõne alla tulla);
- tekkinud vaheandmeid („puhaste inimeste kohta“) ei säilitata ja kustutakse viivitamatult;
- ohuprognoosi koostamiseks ning ohtude ennetamiseks tuleks kasutada isikustamata andmeid või privaatsust tagavaid tehnoloogiaid (nt ühissalastus);
- muud tehnoloogilised piirangud – kas lubatakse luua andmekogudest tervikkoopiad ning moodustada neist üks super-andmeladu.

Need on olulised andmekaitselised küsimused, kuid laiemas vaates on küsimus korrakaitseseadusega soovitud järelevalvemenetluste ühtsuses ja selguses. Iga asutuse omal äranägemisel koostatud erimeetmed eriseadustes viivad paratamatult tagasi korrakaitseseaduse eelsesse kirjususse.“ [180]

Haldusmenetluse seaduse § 35 lg 1 p 3 võimaldab küll haldusorganil haldusmenetlust alustada esimese menetlustoimingu sooritamisega, ent põhiõigusi intensiivselt riivav menetlustoiming vajab eraldi seaduslikku alust. Riigikohtu praktikas on kujunenud seisukoht, et põhiõigustesse sekkuva järelevalvemenetluse toimingu tegemiseks peab täidesaatval võimul olema seaduslik alus, kuivõrd põhiseadus lubab riigivõimu teostamiseks põhiõigusi piirata üksnes põhiseadusega kooskõlas oleva seaduse alusel (PS § 3 lg 1 esimene lause ja § 11). Täitevvõimu tegutsemise aluseks olev volitusnorm ning menetlusnormid peavad olema seda üksikasjalikumad, mida intensiivsem on põhiõiguste riive.[181]

Kui andmekogu andmeid töödeldakse ohuennetuseks (olukorras, kus puudub konkreetse korrarikkumise kahtlus) lausaliselt, selleks, et välja sõeluda võimalikke rikkujaid, **vajab selline isikuandmete töötlemine seaduslikku alust, mis sätestab piisava õigusselgusega isikuandmete töötlemise ning vastab proportsionaalsuse põhimõttele** (vt ka IKÜM art 6 lg 3).

Tuleb arvestada ka tehisintellekti üha ulatuslikuma rakendamisega, mis võimaldab veelgi efektiivsemalt ka üksnes statistiliste andmete pinnalt prognoosida võimalikke rikkujaid ja rakendada profileerimist. Andmetöötluse läbipaistvuse tagamine on eriti oluline profileerimisel. Nii näiteks lõpetas Poola valitsus töötute profileerimise rakenduse kasutamise, kuivõrd see oli diskrimineeriv, läbipaistmatu ja rikkus andmekaitsenõudeid.[182] Sarnaste probleemide tõttu peatas 5.veebruaril 2020 Hollandi kohus sealse riikliku maksupettuste ja tööseaduste rikkumise automatiseeritud riskihindamise.[183]

---

[180] Lk 62-63. Vt ka Andmekaitse Inspektsioon. Avaliku teabe seaduse ja isikuandmete kaitse seaduse täitmisest 2017. aastal. Soovitused aastaks 2018, lk 67-68; Andmekaitse Inspektsioon. Avaliku teabe seaduse täitmisest ja isikuandmete kaitse tagamisest aastal 2018. Soovitused aastaks 2019, lk 63.

[181] RKKKo 09.02.2021, nr 4-20-1588, p 19 edasiste viidetega.

[182] https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf; https://algorithmwatch.org/story/polnische-regierung-schafft-umstrittenes-scoring-system-fuer-arbeitslose-ab/.

[183] The Dutch government's risk indication system (SyRI) is a risk calculation model developed over the past decade by the social affairs and employment ministry to predict the likelihood of an individual committing benefit or tax fraud or violating labour laws.. Deployed primarily in low-income neighbourhoods, it gathers government data previously held in separate silos, such as employment, personal debt and benefit records, and education

Vahejäreldus:

- **Justiitsministeerium analüüsib käesoleva analüüsi jätkutegevusena massandmetöötluse lubatavuse tingimusi, eesmärgiga töötada välja õiguslik alus korrakaitseseaduses andmevõrdluseks ohuennetuse faasis.**

2.3.6. Andmekogu(de) koopia(d) andmeladudes ja -aitades

Selleks, et ametiasutuse valduses olevatest andmetest saada abi asutusel lasuvate ülesannete tõhusamaks täitmiseks ning vajalike juhtimisotsuste tegemiseks, kasutatakse üha rohkem andmeanalüütika tööriistu ning ka tehisintellekti. Seetõttu on koondatakse mitme andmekogu sisu teise keskkonda, ulatuslikku andmekaevet võimaldavasse andmelattu, mis võimaldab tõhusamalt genereerida aruandlust, esitada erinevaid graafikuid, luua geograafilisi ülevaateid ja kasutada muid visuaalseid info kuvamise võimalusi. Andmekaitse Inspektsioon alustas 2021.a riigiasutuste andmeladude seiret, mille menetlus on veel pooleli, millest on juba kinnitust leidnud, et selliseid andmeladusid on mitmeid ning neid kasutatakse klassikaliste andmelao funktsioonide kõrval üha enam asutusel lasuvate põhiülesannete täitmiseks. Samas on andmeladu reguleeritud vaid üksikutel juhtudel. Näiteks:

Sotsiaalteenuste ja -toetuste andmeregistri põhimäärus

§ 3. Registri pidamise viis ja ülesehitus
(1) Registrisse kantavaid andmeid töödeldakse elektroonselt.
(2) Registri alusandmed võivad olla elektroonsed või paberil. Paberil alusdokumentide andmed kantakse registrisse elektroonselt.
(3) **Registri koosseisu kuulub analüütikarakendus (andmeladu).**
(4) Register on liidestatud infosüsteemide andmevahetuskihiga.

Tervise infosüsteemi põhimäärus

§ 2[1]. Infosüsteemi ülesehitus

(1) Infosüsteem koosneb infosüsteemi keskandmekogust, meditsiiniliste ülesvõtete andmekogust ja **andmelaost.**
(4) Andmeladu koosneb keskandmekogu ja andmeandjate edastatavatest pseudonüümitud isikuandmetest, mis ei võimalda isikut tuvastada.

§ 14. Andmelao kasutamine

(1) Andmelaos töödeldakse **pseudonüümitud isikuandmeid** äriprotsesside toetamiseks, poliitika kujundamiseks, mõjude hindamiseks ja teabenõuetele vastamiseks.
(2) Andmelaos tagatakse juurdepääs:

---

and housing histories, then analyses it using a secret algorithm to identify which individuals might be at higher risk of committing benefit fraud. The court ruled that the SyRI legislation contained insufficient safeguards against privacy intrusions and criticised a "serious lack of transparency" about how it worked. It concluded in its ruling that, in the absence of more information, the system may, in targeting poor neighbourhoods, amount to discrimination on the basis of socioeconomic or migrant status. The system did not pass the test required by the European convention on human rights of a "fair balance" between its objectives, namely to prevent and combat fraud in the interest of economic wellbeing, and the violation of privacy that its use entailed, the court added, declaring the legislation was therefore unlawful. https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules; https://www.dutchnews.nl/news/2020/02/governments-fraud-algorithm-syri-breaks-human-rights-privacy-law/.

1) andmeandjale tema enda edastatud andmetele;
2) haldusorganile nendele andmetele, mis on vajalikud tema seadusest tulenevate ülesannete täitmiseks.
(3) Andmelao avaandmed avalikustatakse § 3 lõikes 2 nimetatud volitatud töötleja veebilehel masinloetaval kujul.

On ka andmeladusid, kuhu on koondatud enam kui 10 erineva andmekogu andmed. Eesti kui digiriigi ülesehitamisel on seni lähtutud hajusa infrastruktuuri põhimõttest. Andmevahetuskiht X-tee on võimaldanud asutustel pärida ja näha täpselt neid andmeid, mis on vajalikud talle pandud ülesannete täitmiseks, ilma, et tekiks superandmebaas, kus ühe klikiga oleks võimalik luua inimesest ulatuslik profiil. Just sellise ohu eest kaitseb inimesi põhiõigus informatsioonilisele enesemääratlemisele.[184] Kui ühte andmelattu koondatakse paljude erinevate andmekogude andmed, tähendab see sinna sissemurdmisel oluliselt suuremat kahju nii inimeste õigustele kui ka riigile. Superandmeladude puhul saaks ründaja juurdepääsu mitte enam konkreetsetele andmekoosseisudele (isikute pildid, isikukoodid), vaid kõigile selle asutuse alla koondatud andmelattu kopeeritud andmestikele.

Andmekogude andmete kopeerimine teise keskkonda ei muuda isikuandmete töötlemisega kaasnevat põhiõiguste riivet olematuks. Andmeladu ei ole õigusvaba ruum, kus reeglid ei kehti.

AKI on oma andmekogude juhendis väljendanud seisukohta, et „kui andmeait sisaldab isikuandmeid, peab sellisel viisil töötlemiseks olema asutusel seadusest tulenev alus. Kui andmeait moodustatakse mitme asutuse andmekogudest, peab ühelt asutuselt teisele isikuandmete edastamiseks olema õiguslik alus. [---]Andmeait võib endast kujutada märksa suuremat eraelu puutumatuse riivet kui primaarsed andmekogud. Mitmest andmekogust kokku pandud teave võimaldab ju isikut rohkem profileerida kui eri andmekogudes laiali paiknevad teabekillud.“.[185] Samuti rõhutas AKI, et kui riigiasutus soovib andmelaos olevad isikuandmeid töödelda teadusuuringute või statistika eesmärgil, tuleb juhinduda vastavatest erinormidest (juhendi koostamise ajal kehtinud IKS (2008-2019) § 16 asemel reguleerib seda nüüd IKS § 6; riikliku statistika osas tuleb juhinduda riikliku statistika seadusest.

Vahejäreldused:

- Andmelao funktsioon saab olla vaid **statistilist laadi agregeeritud analüüside koostamine** või andmete ette valmistamine selleks. Andmeladu ei tohi kasutada asutuse põhiülesannete täitmiseks. Seda tuleb teha(primaar)andmekogus endas.
- Andmelaost võib väljastada isikuandmeid teadusuuringuteks, kui rakendatakse andmejälgijat või kui väljastatakse anonüümseid andmeid.
- Kui andmekogul on **andmeladu, tuleb see andmekogu põhimääruses reguleerida**, sh mis on andmelao pidamise eesmärk, kuidas selles andmeid töödeldakse (kas pseudonüümitult), kaua säilitatakse.

[184] „This information can also be combined – especially if integrated information systems are set up – with other collections of data to assemble a partial or essentially complete personality profile without giving the party affected an adequate opportunity to control the accuracy or the use of that profile. As a result, the possibilities for consultation and manipulation have expanded to a previously unknown extent, which can affect the conduct of the individual because of the mere psychological pressure of public access." 1983.a Volkszählungsurteil, mitteametlik inglisekeelne tõlge.
[185] https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf.

- Juhul kui andmeladu tahetakse teha siiski rohkema kui ühe andmekogu andmetest (seejuures ilma et minnaks vastuollu hajusa arhitektuuri nõudega), tuleb selline andmeladu **asutada seadusega**, nagu iga muu andmekogu.

Justiitsministeerium analüüsib täiendavalt koostöös Majandus- ja Kommunikatsiooniministeeriumi ja Andmekaitse Inspektsiooniga andmeladusid puudutavaid järeldusi.

.

2.3.7. Isikuandmete päringute logid ja andmejälgija

Isikuandmete töötlemisel logimise kohustus on otsesõnu ettenähtud isikuandmete töötlemist süüteomenetluses reguleerivas IKS §-s 36. Isikuandmete kaitse üldmäärus isikuandmete töötlemisel logimise kohustust ei sätesta, kuid see on kaudselt tuletatav IKÜM art 5 lg 1 punktist f, mis näeb ette, et:

> isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“);

Kui päringud toimuvad andmevahetuskihi kaudu, on päringute logimine ette nähtud ka nn X-tee määruses.[186]

See, kas üldse ja milliseid päringuid logitakse ning kaua logisid säilitatakse, on enamasti reguleeritud andmekogude põhimäärustes. Näiteks pakendiregistri põhimääruses sätestatakse[187]:

> § 17. Andmete logimine
> (1) Registris logitakse andmete lisamine, muutmine ja kustutamine ning isikuandmeid sisaldavate vormide avamine.
> (2) Logisid säilitatakse registris seitse aastat.

Põllumajandustoetuste ja põllumassiivide registri põhimäärusest jääb aga mulje, et andmete vaatamist (päringute tegemist) andmekogu kasutajate poolt ei logitagi.[188]

> § 15. Andmete logimine
> (1) Andmete registrisse kandmine, sealhulgas registriandmete muutmine, logitakse. Logis säilitatakse kande sisu, kuupäev ja kellaaeg ning selle tegija nimi.
> (2) Logi säilitatakse kolm aastat kande tegemisest arvates.

Andmekogudes talletatud isikuandmete töötlemise logimine aitab tagada andmetöötluse läbipaistvust, aitab ära hoida isikuandmete ebaseaduslikku kasutamist. Riigi Infosüsteemi Amet

[186] Vabariigi Valitsuse 23.09.2016 määrus nr 105 „Infosüsteemide andmevahetuskiht“, vt päringulogidega seondutaid sätteid.
[187] Analoogne säte näiteks probleemtooteregistri põhimääruse § 21;
[188] Analoogne säte näiteks maaparandussüsteemide registri põhimääruse § 17; väetiseregistri põhimääruse § 15; riigi toidu ja sööda käitlejate registri põhimääruse § 16; taimetervise registri põhimäärus § 16; kultuurimälestiste registri põhimääruse § 22.

on välja töötatud andmejälgija: „Andmejälgija eesmärk on pakkuda kodanikule selget ülevaadet tema andmetega sooritatud toimingutest. Terviklik ülevaade kuvatakse riigiportaalis eesti.ee. RIA pakub andmekogu omanikule paindlikud standardkomponendid lahenduse tehniliseks teostuseks, võimaldades logida nii X-tee liiklust kui asutusesiseseid päringuid. Andmejälgija loob läbipaistvuse isikuandmete töötlemisel, parandades nii kodanike informeeritust kui abistades asutusi isikuandmete päringute selgitamisel.“.[189] Andmekaitse Inspektsiooni hinnangul on andmejälgija suur samm läbipaistvuse tagamiseks, kuid 2017.aastast käivitunud lahendust rakendavad üksnes vähesed andmetöötlejad: „Hetkel saab andmejälgija kaudu teada, kui meie andmeid on vaadatud rahvastikuregistris, retseptikeskuses, töötuskindlustuse andmekogus või siis sotsiaalteenuste ja toetuste registris. Samuti saab patsiendiportaalis digilugu.ee näha tervise infosüsteemis tehtud päringuid.“.[190]

Arvestades seda, kui ebaühtlaselt on isikuandmete töötlemise logimist erinevates põhimäärustes reguleeritud, tuleks kaaluda andmejälgija kohustuslikuks muutmist.

Vahejäreldus:

- **Andmekogu, milles töödeldakse isikuandmeid, puhul on kohustuslik rakendada andmejälgijat, kui seadus ei sätesta teisiti.**

2.3.8. Andmekogu andmete õiguslik või informatiivne tähendus

AvTS sätestab, et andmetele antakse õiguslik tähendus seaduse tasemel.

§ 43[6]. Põhiandmed ja andmete tähendus

(4) Õiguslik tähendus antakse andmetele seadusega.

Eestis on mõned keskse tähtsusega andmekogud, mille eesmärk on andmete kogumine ja avalikuks tegemine, eesmärgiga tagada usaldusväärne tehingukäive. Silmas on peetud kohtu juures peetavaid kindla õigusliku tähendusega registreid: kinnistusraamat ja äriregister.[191]

ÄS § 34. Kande õiguslik tähendus

(1) Äriregistri kanne jõustub, kui kandele on alla kirjutanud kandemääruse täitnud isik ja kande otsustamiseks pädev isik.

(2) Kanne kehtib kolmanda isiku suhtes õigena, välja arvatud, kui kolmas isik teadis või pidi teadma, et kanne ei ole õige. Kannet ei loeta kehtivaks tehingute suhtes, mis tehakse 15 päeva jooksul pärast kande tegemist, kui kolmas isik tõendab, et ta kande sisu ei teadnud ega pidanudki teadma.

(3) Kui registrisse kandmisele kuuluvaid asjaolusid ei ole registrisse kantud, on neil asjaoludel kolmanda isiku suhtes õiguslik tähendus üksnes juhul, kui kolmas isik neist teadis või pidi teadma.

Andmekogude juhendis on selgitatud: „Andmetele andmekogus saab õigusliku tähenduse anda vaid seadusega. Nii sätestab konkreetselt AvTS § 43[6] lg 4. Ilma selleta on andmed vaid informatiivse tähendusega.

[189] https://www.ria.ee/et/riigi-infosusteem/x-tee/andmejalgija.html.
[190] Andmekaitse Inspektsioon (21.01.2020): „Miks minu andmeid on vaadatud?“.
[191] Andmekogude juhend, lk 6.

Näiteks võib tuua omandit näitavate andmete tähenduse. Kinnisasja omand tekib, muutub ja lõpeb kinnistusraamatu kandega, selleks ei piisa ainuüksi pooltevahelisest tehingust (asjaõigusseaduse § 64[1] ja 64[2]). Sõiduki omandiõigus läheb üle tehinguga ning liiklusregistri andmed on üksnes informatiivsed. Samas liiklusregistrisse kantud sõiduki registerpandi andmete õigsust aga eeldatakse (liiklusseaduse § 178).“.[192]

AÕS § 64[1]. Kinnisomandi üleandmine ja koormamine

Kinnisomandi üleandmiseks ja kinnisasja koormamiseks asjaõigusega, samuti kinnisasja koormava asjaõiguse üleandmiseks, koormamiseks või selle sisu muutmiseks on nõutav õigustatud isiku ja teise poole notariaalselt tõestatud kokkulepe (asjaõigusleping) ja sellekohase kande tegemine kinnistusraamatusse, kui seadus ei sätesta teisiti.

§ 64[2]. Õiguse lõpetamine

Kinnisasja koormava asjaõiguse lõpetamiseks on nõutav õigustatud isiku notariaalselt kinnitatud avaldus õiguse lõpetamise kohta ja õiguse kustutamine kinnistusraamatust, kui seadus ei sätesta teisiti. Avaldus tuleb anda kinnistusosakonda või isikule, kelle kasuks õigus lõpetatakse.

AvTS sätestab seega selgelt, et andmetele antakse õiguslik tähendus seaduse tasemel. AvTS ei näe ette, et seda tuleks sätestada ka põhimäärustes. Ometi on enamikes põhimäärustest sätestatud sarnaselt[193]:

§ 8. Andmete õiguslik tähendus

Andmekogu andmetel on informatiivne tähendus.

Mõnes põhimääruses on ka rõhutatud, et „Registrisse kantud andmetel on õiguslik tähendus seaduses sätestatud ulatuses“.[194]

Haldusorganid saavad ka üksnes informatiivse tähendusega andmeid oma ülesannete täitmisel kasutada, kui neil on pädevus ja volitus selleks. Nii on ka Riigikohus selgitanud liiklusregistriga seoses: „Riikliku liiklusregistri pidamise põhimääruse § 13 sätestab, et liiklusregistri andmed ei oma õiguslikku tähendust, vaid on informatiivsed. Kolleegium on seisukohal, et liiklusregistri kanded ei tekita, muuda ega lõpeta omandiõigust sõidukile. Tegemist on informatiivse andmekoguga, mida riik, kohaliku omavalitsuse üksus, kohtutäiturid ja notarid kasutavad avalike ülesannete täitmiseks (LS § 65 lg 2).“.[195] See, et andmetel on informatiivne tähendus, ei tähenda, et isikuandmete õigsus ja andmekvaliteet ei pea olema tagatud (IKÜM art 5 lg 1 p d).

Vahejäreldused:

- Andmekogude regulatsioonides ei ole vaja deklareerida andmete informatiivset tähendust. Sellised sätted põhimäärustes võiks kehtetuks tunnistada.

[192] Andmekogude juhend, lk 8.
[193] Näiteks: Julgeolekuasutuste riigivara registri asutamine ja registri pidamise põhimääruse § 10; Geodeetiliste punktide andmekogu asutamine ja andmekogu pidamise põhimäärus § 8; Sadamaregistri pidamise põhimäärus § 8; Riigi personali- ja palgaarvestuse andmekogu asutamine ja selle põhimäärus § 4; Mobilisatsiooniregistri põhimäärus § 3; E-toimiku süsteemi asutamine ja e-toimiku süsteemi pidamise põhimäärus § 14; Tsiviiltoetuse registri põhimäärus § 4; Testide andmekogu asutamine ja põhimäärus § 6 jpt.
[194] Riikliku DNA-registri asutamine ja registri pidamise põhimäärus § 6.
[195] RKHKo 09.03.2010, 3-3-1-94-09, p 12.

- Andmetele annab õigusliku tähenduse seadusandja, seejuures tuleb täpsustada, milles see õiguslik tähendus seisneb. Põhimõtteliselt tuleb kõne alla kaks varianti:
    - registris olevaid andmed on õiged, isegi kui need on päriselus valed (s.t õigus tekib ja kaob registrikandega) – näiteks kinnistusraamat;
    - registris olevate andmete õigsust eeldatakse, kuid tegemist on ümberlükatava eeldusega. Sellisel juhul võiks seaduses olema täpsustatud näiteks, et registrikannete loetakse õigeks, kui ei tõendata vastupidist või välja arvatud juhul, kui isik teadis, et kanne on vale.

2.3.9. Isikuandmete kustutamine, hävitamine, arhiveerimine

AvTSi andmekogude sätted ei reguleeri andmete säilitustähtaegu ega ka seda, mis saab andmetest pärast säilitustähtaja lõppemist. Et isikuandmete säilitamisele on vaja seada tähtajad, tuleneb asjaolust, et põhiõiguste riive on õigustatud üksnes seni, kuni see on tõesti vajalik. Seetõttu nõuab ka IKÜM isikuandmetele säilitustähtaegade määramist:

IKÜM art 5 lg 1 punkt e:

isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada ainult seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse; isikuandmeid võib kauem säilitada juhul, kui isikuandmeid töödeldakse üksnes avalikes huvides toimuva arhiveerimise, teadus- või ajaloouuringute või statistilisel eesmärgil vastavalt artikli 89 lõikele 1, eeldusel et andmesubjektide õiguste ja vabaduste kaitseks rakendatakse käesoleva määrusega ettenähtud asjakohaseid tehnilisi ja korralduslikke meetmeid („säilitamise piirang“);

Ka pp 39 on sätestatud, et „Selle tagamiseks, et isikuandmeid ei säilitataks vajalikust kauem, peaks vastutav töötleja kindlaks määrama tähtajad andmete kustutamiseks või perioodiliseks läbivaatamiseks.“. **Isikuandmete säilitamise kestus on mõjutab eraelu riive kestust, seetõttu peaks selle otsustama seadusandja**. Samuti peab seadusandja tagama, et säilitustähtaja möödumisel isikuandmed kustutatakse või muudetakse anonüümseks. Põhjenduspunktis 26 selgitatakse: „Andmekaitse põhimõtteid ei tuleks seetõttu kohaldada anonüümse teabe suhtes, nimelt teave, mis ei ole seotud tuvastatud või tuvastatava füüsilise isikuga, või isikuandmete suhtes, mis on muudetud anonüümseks sellisel viisil, et andmesubjekti ei ole võimalik tuvastada või ei ole enam võimalik tuvastada. Käesolevas määruses ei käsitleta seega sellise anonüümse teabe töötlemist, sealhulgas statistilisel või uuringute eesmärgil.“.

Valdavalt ei ole seadusandja säilitustähtaegade küsimusega tegelenud. Andmekogude põhimäärustest ilmneb, et **andmete säilitamise lõppemine on reguleeritud väga erinevalt.** On põhimäärusi, kus on selge sõnaga ette nähtud andmete kustutamine peale tähtaja lõppu; on põhimäärusi, kus andmed kantakse andmekogu arhiivi. Andmete arhiveerimine tähendab ühel puhul, et andmed on samas andmekogus alles ja kasutatavad, teisel puhul tähendab see juurdepääsu režiimi muutust. Andmetöötluse läbipaistvus ei ole piisaval määral tagatud, kui ühes sättes on ette nähtud, et andmeid säilitatakse näiteks 5 aastat, aga sama põhimääruse teises kohas sätestatakse, et tegelikult tõstetakse need andmed siis andmekogu „teise sahtlisse“ – digitaalsesse arhiivi, kus neid säilitatakse veel mitu aastat. Selgelt lubamatu on olukord, kui isikuandmed tõstetakse andmelattu või mingisse teise keskkonda ja säilitatakse (ja kasutatakse nii haldusorgani enda poolt kui ka teiste haldusorganite poolt) neid seal edasi, hoolimata tõsiasjast, et säilitustähtaeg on lõppenud.

Andmete hävitamine ning sõna „arhiveerimine“ kasutus ja tõlgendus vajab üheselt määratlemist, sest arhiveerimist ei käsitleta siin ka arhiiviseaduse tähenduses, mis reguleerib riigiasutuse dokumentatsioonile arhiiviväärtuse omistamist ning Rahvusarhiivile üleandmist.

Näiteid põhimäärustest:

Teenistus- ja tsiviilrelvade registri põhimäärus

§ 13. Andmete arhiveerimine
(1) Relva ja laskekõlbmatu relva andmed arhiveeritakse, kui relv:
1) on hävitatud;
2) on lammutatud;
3) alaliselt Eestist välja viidud;
4) kantakse sõjaväerelvade registrisse;
5) antakse riiklikule ekspertiisiasutusele ekspertiiside tegemiseks või riigi- ja munitsipaalmuuseumi relvakollektsiooni.
(2) **Isiku andmed arhiveeritakse**, kui:
1) isikule väljastatud luba kaotab kehtivuse ja isiku omanduses või valduses ei ole enam relvi;
11) isiku relvaseaduse §-des 26, 32 ja 34 sätestatud loa taotlus jäetakse rahuldamata ja loa väljastamisest keeldutakse.
2) surnud isiku relv või laskekõlbmatu relv on kantud uue omaniku või valdaja nimele;
3) juriidilise isiku valduses ei ole enam relvi või laskekõlbmatuid relvi.

(3) **Arhiveeritud andmed võib volitatud töötleja muuta aktuaalseks**, kui:
1) relva, laskekõlbmatu relva või isiku andmed, mis arhiveeriti, on muutunud uuesti aktuaalseks;
2) andmed on arhiveeritud ekslikult.

§ 14. Andmete säilitamine ja kustutamine
(1) Relvade ja laskekõlbmatute relvade andmeid ning registrisse kantud isikute isikuandmeid säilitatakse 30 aastat pärast nende andmete arhiivi kandmist.
(1^1) Nende isikute isikuandmeid, kes taotlesid relvaseaduse §-des 26, 32 ja 34 sätestatud luba ja kellele seda ei väljastatud, säilitatakse viis aastat pärast andmete arhiivi kandmist. Pädevatele asutustele tagatakse nendele andmetele juurdepääs, kui relvaseaduse alusel antakse luba või tunnistatakse see kehtetuks.
(2) Käesoleva paragrahvi lõikes 1 nimetatud andmed peavad olema kättesaadavad:
1) pädevatele asutustele relvaseaduse alusel loa andmise ja kehtetuks tunnistamise eesmärgil ning pädevatele asutustele tollimenetluste tarbeks 10 aasta jooksul pärast nende kandmist registriarhiivi;
2) asutustele, kes on pädevad kuritegude ennetamise, uurimise, avastamise ja nende eest vastutusele võtmise ning kriminaalkaristuste täitmisele pööramise valdkonnas, 30 aasta jooksul pärast nende kandmist registriarhiivi.
(3) Arhiivi kandmisest 30 aasta möödumisel kustutab volitatud töötleja isikuandmed registrist.

Sissesõidukeeldude riikliku registri pidamise põhimäärus reguleerib üksnes registriandmete arhiveerimist, kuid mitte seda, mis sellise arhiveerimise eesmärk või sisuline tähendus on.

§ 21. Registriandmete arhiveerimine

(1) Registrikaardid arhiveeritakse pärast sissesõidukeelu tähtaja lõppemist või sissesõidukeelu kehtetuks tunnistamist.

(2) Menetlustoimikud arhiveeritakse pärast sissesõidukeelu andmete lisamist registrikaardile.

(3) Arhiveeritud registrikaarte ja menetlustoimikuid säilitatakse 50 aastat.

Kaitseväekohustuslaste registri põhimäärus sätestab registrist kustutatud andmete kandmise arhiivi.

§ 10. Digitaalsesse arhiivi kantavad andmed
Digitaalsesse arhiivi kantakse digitaalsest registrist kustutatud andmed.
§ 16. Andmete kustutamine
(1) **Andmed kustutatakse digitaalsest registrist ja kantakse digitaalsesse arhiivi:**

1) andmesubjekti surma korral;
2) kui andmesubjekt on teadmata kadunud ning Politsei- ja Piirivalveamet on tema suhtes algatanud asukoha tuvastamise menetluse ega ole suutnud tema asukohta kindlaks teha 12 kuu jooksul;
3) Eesti kodakondsuse kaotamisel;
4) kaitseväekohustuslase piirvanuse ületamisel;
5) üle 60-aastase isiku tegevteenistusest vabastamisel;
6) isiku kaitseväekohustuse puudumisel;
7) kaitseväeteenistuse seaduses sätestatud juhtudel;
8) ebaõigete andmete tuvastamisel;
9) kande aluseks olevate andmete muutumisel;
10) kaitseväekohustuseta Kaitseliidu tegevliikme sõjaväelise auastmega sõjaaja ametikohalt vabastamisel, välja arvatud uuele sõjaväelise auastmega sõjaaja ametikohale nimetamise korral.

(2) **Digitaalsesse arhiivi kantud andmed võib volitatud töötleja kanda tagasi digitaalsesse registrisse, kui:**
1) andmete kustutamine on tühine;
2) isik, kelle andmed kustutati, on muutunud uuesti andmesubjektiks;
3) teadmata kadunud isiku asukoht on tuvastatud;
4) andmed on kustutatud ekslikult.

(3) Kui seaduses ei ole sätestatud teisiti, säilitatakse:
1) paragrahvi 8 lõigetes 2–10 nimetatud andmeid 50 aastat digitaalsesse arhiivi kandmisest arvates;
2) paragrahvi 8 lõikes 11 nimetatud andmeid Kaitseressursside Ameti teabehalduskorra kohaselt.

Kultuurmälestiste registri põhimääruse § 21 kohaselt:

(1) Registrisse kantud andmete alusdokumente säilitatakse kooskõlas vastutava töötleja asjaajamises kehtestatud dokumentide loetelus sarjadele ette nähtud säilitustähtaegadega, mille lõppemise järel antakse need arhiiviseaduse ja muude seaduste ning nende alusel kehtestatud õigusaktide kohaselt avalikku arhiivi või otsustatakse nende hävitamine.

(2) Andmeid säilitatakse alaliselt, välja arvatud neid andmeid, mille alusdokumentidele on kehtestatud säilitustähtajad.

(3) **Pärast säilitustähtaja möödumist kantakse andmed registri arhiivi. Isikuandmed anonüümitakse.**

(4) Kui mälestiseks olemine lõpetatakse või mälestise omaniku andmed muutuvad, säilitatakse mälestisega seotud isikuandmeid, mis on vajalikud asja kohta ajaloolise ülevaate saamiseks.

Riikliku sõrmejälgede registri asutamine ja registri pidamise põhimäärus

§ 19. Andmete säilitamine
(1) Registrisse kantud andmed säilitatakse kohtuekspertiisiseaduse §-s 99 sätestatu kohaselt.
(2) Registri arhiivi kantud andmeid säilitatakse kohtuekspertiisiseaduse §-s 910 sätestatu kohaselt.
(3) Andmete alusdokumente säilitatakse vähemalt sama kaua, kui andmed on kantud registrisse. Tähtaja möödumisel võib alusdokumendid arhiiviseaduse alusel viia üle vastavasse arhiivi või otsustada nende hävitamine.
(4) Andmete registrisse kandmise alusdokumente säilitatakse paberkandjal või elektroonselt.
(5) Registri alusdokumentide hävitamise kohta koostatakse protokoll, mida säilitatakse volitatud töötleja juures.

Politsei andmekogu põhimäärus

§ 24. Andmete säilitamine
(1) Ühiste infoobjektide andmestiku andmeid säilitatakse alljärgnevalt:
1) isikuandmeid, mis ei ole seotud infosüsteemi teise andmestikuga, säilitatakse infosüsteemis 1 aasta andmete infosüsteemi kandmisest arvates;

2) isikuandmeid, mis on seotud infosüsteemi teise andmestikuga, säilitatakse vastava andmestiku säilitamistähtaja lõppemiseni;
3) paragrahvi 8 punktides 2, 3, 4 ja 8 nimetatud andmeid, mis ei ole seotud infosüsteemi teise andmestikuga, säilitatakse 5 aastat andmete infosüsteemi kandmisest arvates;
4) paragrahvi 8 punktides 5–7 nimetatud andmeid, mis ei ole seotud infosüsteemi teise andmestikuga, säilitatakse 1 aasta andmete infosüsteemi kandmisest arvates;
5) paragrahvi 8 punktides 2–8 nimetatud andmeid, mis on seotud infosüsteemi teise andmestikuga, säilitatakse vastava andmestiku säilitamistähtaja lõppemiseni.
(2) Süüteomenetluse andmestiku andmeid säilitatakse infosüsteemis alljärgnevalt:
1) kriminaalmenetluse alustamata jätmise, kriminaalmenetluse lõppemise või kriminaalasja kohtueelse menetluse kokkuvõttega prokuratuuri saatmise korral 15 aastat alustamata jätmisest, lõpetamisest või prokuratuuri saatmisest arvates;
2) «Karistusseadustiku» § 81 lõikes 2 loetletud kuriteo korral alaliselt;
3) lõpetatud väärteoasjades 1 aasta väärteomenetluse lõpetamisest arvates;
4) väärteomenetluse alustamata jätmise korral ja suulise hoiatamise korral 1 aasta alustamata jätmisest või hoiatamisest arvates;
[RT I, 27.02.2012, 1 - jõust. 01.03.2012]
41) kirjaliku hoiatamismenetluse andmeid kuni hoiatustrahvi laekumiseni;
[RT I, 27.02.2012, 1 - jõust. 01.03.2012]
42) väärteo lühimenetluse andmeid kuni lühimenetluse otsuse jõustumiseni;
[RT I, 29.12.2018, 3 - jõust. 01.01.2019]
5) otsusega väärteoasjades 3 aastat lahendi tegemisest arvates;
6) täitmata lahendite korral täitmise aegumiseni;
7) sama isiku poolt korduvalt süütegude toimepanemise korral säilitatakse kõikide süütegude andmeid 5 aastat ajaliselt viimasena toime pandud süüteo materjalide prokuratuuri saatmisest või lahendi jõustumisest arvates, kui käesolevas paragrahvis ei sätestata andmete pikemat säilitamise tähtaega.
(21) Haldustegevuse andmestiku andmeid säilitatakse alljärgnevalt:
1) haldusmenetluse andmeid, mis ei ole seotud süüteomenetluse andmestiku või riiginõudega, säilitatakse kolm aastat haldusmenetluse lõppemisest arvates;
2) haldusmenetluse andmeid, mis on seotud riiginõudega, säilitatakse kolm aastat või kuni riiginõude täitmiseni;
3) haldusmenetluse andmeid, mis on seotud süüteomenetluse andmestikuga, säilitatakse süüteomenetluse andmete säilitamistähtaja lõppemiseni.
[RT I, 13.01.2017, 2 - jõust. 16.01.2017]
(3) Politsei ennetava tegevuse andmestiku andmeid säilitatakse alljärgnevalt:
1) piirkondlikke infoteateid 3 aastat andmete infosüsteemi kandmisest arvates;
2) õigusevastase teo toime pannud alaealise kohta kuni tema täisealiseks saamiseni;
3) numbrituvastuskaamera teadet, mis ei ole seotud infosüsteemi teise andmestikuga, kuni 3 kuud teate saabumisest arvates;
31) automaatse järelevalvesüsteemi teadet, mis ei ole seotud infosüsteemi teise andmestikuga, kuni 1 aasta teate saabumisest arvates;
4) automaatse järelevalvesüsteemi või numbrituvastuskaamera teadet, mis on seotud infosüsteemi teise andmestikuga, säilitatakse vastava andmestiku säilitamistähtaja lõppemiseni.
(4) Politsei reageeriva tegevuse andmestiku andmeid säilitatakse infosüsteemis 3 aastat väljakutse laekumisest arvates.
(5) Politsei arestimajade tegevuse andmestiku andmeid säilitatakse infosüsteemis 3 aastat arestimajast vabanemisest arvates.
(6) Otsimise andmestiku andmeid, mis on seotud süüteomenetluse andmestikuga, säilitatakse süüteomenetluse andmete säilitamistähtaja lõppemiseni, ülejäänud otsimise andmestiku andmeid säilitatakse 1 aasta andmete otsimise andmestikku kandmise põhjuse äralangemisest arvates.
(7) Jälitusmenetluse andmestikus andmeid säilitatakse 25 aastat andmete infosüsteemi kandmisest arvates, kui seaduses või seaduse alusel antud õigusaktiga ei ole ette nähtud teistsugust tähtaega.
(8) Käesoleva paragrahvis sätestatud säilitustähtaegade möödumisel kantakse andmed arhiivi, välja arvatud lõike 3 punktis 2 nimetatud andmed, mis säilitustähtaja möödumisel kustutatakse.

§ 25. Infosüsteemi arhiiv
(1) Arhiveeritud andmeid säilitatakse digitaalselt.
(2) **Arhiivist on õigus saada andmeid:**

1) politseiametnikul ja muul isikul põhjendatud teadmisvajadusel;
2) andmesubjektil tema kohta käivaid andmeid.

§ 26. Andmete kustutamine
(1) Paragrahvi 24 lõikes 1 nimetatud andmed kustutatakse infosüsteemi arhiivist järgmiselt:
1) punktis 1 nimetatud andmed 50 aasta möödumisel andmete arhiveerimisest arvates;
2) punktis 3 nimetatud andmed 5 aasta möödumisel andmete arhiveerimisest arvates;
3) punktis 4 nimetatud andmed 1 aasta möödumisel andmete arhiveerimisest arvates;
4) punktides 2 ja 5 nimetatud andmed vastava andmestiku andmete kustutamisel.
(2) Paragrahvi 24 lõikes 2 nimetatud andmed kustutatakse infosüsteemi arhiivist järgmiselt:
1) punktis 1 nimetatud andmed 50 aasta möödumisel andmete arhiveerimisest arvates;
2) punktis 4 nimetatud andmed 1 aasta möödumisel andmete arhiveerimisest arvates;
3) punktides 3, 5 ja 6 nimetatud andmed 10 aasta möödumisel süüteomenetluses lahendi jõustumisest arvates;
4) punktis 41 ja 42 nimetatud andmed 7 aasta möödumisel andmete arhiveerimisest arvates;
5) punktis 7 nimetatud andmed 5 aasta möödumisel andmete arhiveerimisest arvates.

(21) Paragrahvi 24 lõikes 21 nimetatud andmed kustutatakse infosüsteemi arhiivist järgmiselt:
1) punktis 1 nimetatud andmed 1 aasta möödumisel arhiveerimisest arvates;
2) punktis 2 nimetatud andmed 4 aasta möödumisel arhiveerimisest arvates;
3) punktis 3 nimetatud andmed süüteomenetluse andmete kustutamisel.

(3) Paragrahvi 24 lõikes 3 nimetatud andmed kustutatakse infosüsteemi arhiivist järgmiselt:
1) punktides 1 ja 4 nimetatud andmed 5 aasta möödumisel andmete arhiveerimisest arvates;
2) punktides 3 ja 31 nimetatud andmed 3 aasta möödumisel andmete arhiveerimisest arvates.
(4) Paragrahvi 24 lõikes 4 nimetatud andmed kustutatakse infosüsteemi arhiivist 2 aasta möödumisel andmete arhiveerimisest arvates.
(5) Paragrahvi 24 lõigetes 5 ja 6 nimetatud andmed kustutatakse infosüsteemi arhiivist 5 aasta möödumisel andmete arhiveerimisest arvates.
(6) Paragrahvi 24 lõikes 7 nimetatud andmed kustutatakse infosüsteemi arhiivist 50 aasta möödumisel andmete arhiveerimisest arvates.

Mobilisatsiooniregistri põhimäärus

§ 7. Digitaalne arhiiv

Digitaalsesse arhiivi kantakse digitaalsest registrist kustutatud andmed.

§ 15. Andmete kustutamine

(1) Kande aluseks olevate andmete muutmisel kantakse registrisse uued andmed ja varasemad andmed kustutatakse.

(2) Kustutatud andmed kantakse digitaalsesse arhiivi.

(4) Kustutatud andmeid säilitatakse kolm aastat nende digitaalsesse arhiivi kandmisest arvates, kui seadus ei sätesta teisiti.

Vahejäreldused:

- Seadusandja sätestab andmekogu isikuandmete säilitamise tähtaja, mida võib määrusega konkretiseerida, sh ka tähtaegu vähendada (kui andmekogu asutavas seaduses on selleks volitatud).
- Andmekogusisese arhiivi loomine ja arhiveeritud andmetele juurdepääsurežiimi sätestamine põhimääruses saab toimuda seaduse volituse ulatuses.
- Seaduses sätestatud säilitustähtaja lõppemisel tuleb tagada isikuandmete kustutamine.

2.3.10. Andmekogu hävitamine

Andmekogu lõpetamist reguleerib AvTS § § 43^3 lõikes 3 järgmiselt:

> Enne andmekogu asutamist, andmekogus kogutavate andmete koosseisu muutmist, andmekogu kasutusele võtmist või **andmekogu lõpetamist** kooskõlastatakse andmekogu tehniline dokumentatsioon Riigi Infosüsteemi Ametiga, Andmekaitse Inspektsiooniga ja Statistikaametiga.

Andmekogude lõpetamise täpsemat korraldust reguleerib enamik andmekogude põhimäärusi, tehes seda üsna erineval viisil. On põhimäärusi, milles on ette nähtud andmekogu asutaja (ministri või Vabariigi Valitsuse) õigus otsustada selle andmekogu likvideerimine; samas on põhimäärusi, milles viidatakse likvideerimisele seaduses sätestatud korras. Alljärgnevalt on esitatud ülevaade erinevatest lahendustest.

Näiteks politsei andmekogu põhimäärus:

> § 29. Infosüsteemi likvideerimine
>
> Infosüsteemi likvideerimise **otsustab siseminister.** Infosüsteemi likvideerimisel otsustatakse andmete teise andmekogusse või riiklikku registrisse või riiklikku arhiivi üleandmine või andmete hävitamisele kuulumine ja nende üleandmise või hävitamise tähtaeg.

Analoogne säte on piirikontrolli andmekogu põhimääruse § 21, sarnane ka piiriületuse ootejärjekorra andmekogu põhimääruse § 23, milles viidatakse lisaks arhiiviseadusele:

> § 23. Andmekogu likvideerimine
>
> Andmekogu likvideerimise **otsustab valdkonna eest vastutav minister**. Andmekogu likvideeritakse kooskõlas arhiiviseaduses sätestatud nõuetega.

Samuti sätestab loomeliitude andmekogu asutamine ja põhimäärus

> § 18. Andmekogu tegevuse lõpetamine
>
> Andmekogu tegevuse lõpetamise **otsustab valdkonna eest vastutav minister.** Andmekogu tegevus lõpetatakse kooskõlas avaliku teabe seaduses ja arhiiviseaduses sätestatud nõuetega.

Aukonsulite andmekogu põhimääruses reguleeritakse lõpetamist järgmiselt:

> § 15. Andmekogu lõpetamine
>
> Andmekogu lõpetamise **otsustab välisminister.**

Rahapesu Andmebüroo andmekogu põhimäärus sätestab likvideerimist järgmiselt:

> § 29. Andmekogu likvideerimine
>
> (1) Andmekogu likvideerimise **otsustab valdkonna eest vastutav minister.**
> (2) Andmekogu likvideeritakse kooskõlas arhiiviseaduses ja avaliku teabe seaduses sätestatud nõuetega.

Keskkonnaseire andmekogu asutamine ja andmekogu pidamise põhimäärus sätestab lõpetamise otsustamise määrusega:

> § 21. Andmekogu lõpetamine
>
> (1) Andmekogu tegevuse lõpetamise **otsustab valdkonna eest vastutav minister määrusega.**

(2) Andmekogu lõpetamine toimub kooskõlas arhiiviseadusega ning avaliku teabe seaduse § 43^9 lõike 1 punkti 6 alusel kehtestatud õigusaktiga.

Broneeringuinfo andmekogu põhimäärus tõdeb lakooniliselt:

§ 21. Andmekogu likvideerimine

Andmekogu likvideeritakse **seaduses sätestatud korras.**

Jälitustoimingute infosüsteemi asutamine ja infosüsteemi pidamise põhimäärus

§ 21. Infosüsteemi likvideerimine

Infosüsteemi likvideerimise otsustab Vabariigi Valitsus seaduse alusel.

Isikuandmete töötlemine andmekogudes on põhiõiguste riive, mida õigustab avalikul võimul lasuvate ülesannete täitmise tagamise kohustus. Andmekogu loomise ja sellega seonduvad olulised küsimused peab otsustama seadusandja. Olulisuse põhimõttest peab seadusandja otsustama ka, kas ja millistel juhtudel ja millist protseduuri arvestades tuleb andmekogu likvideerida ning kas likvideeritud andmekogu andmed hävitatakse või kantakse teise andmekogusse.

Näiteks on seaduse tasemel reguleeritud rahvastikuregistri likvideerimist järgnevalt:

RRS § 19. Rahvastikuregistri kasutamise peatamine

(1) Kui rahvastikuregistri kasutamine ohustab või võib ohustada riigi julgeolekut sõjaseisukorras, erakorralises seisukorras, eriolukorras või hädaolukorras, võib Vabariigi Valitsuse korraldusega või vastutava töötleja otsusega osaliselt või täielikult rahvastikuregistri kasutamise peatada.

(2) Vastutav töötleja on kohustatud võtma käesoleva paragrahvi lõikes 1 sätestatud juhul kasutusele abinõud rahvastikuregistri andmete säilitamiseks ja kaitsmiseks või hävitamiseks.

(3) Vabariigi Valitsus kehtestab määrusega rahvastikuregistri andmete säilitamise, kaitsmise, kasutamise peatamise ja hävitamise korra hädaolukorras.

Arvestades põhimääruste erinevaid andmekogu likvideerimise regulatsioone, näib vajalik, et AvTS-is oleks reguleeritud andmekogude konkreetsemad lõpetamise tingimused ja kord, et see oleksid ühetaoliselt läbi viidud. Andmekogu hävitamine on tagasipöördumatu, sest peale seda andmekogu koos selles sisalduvaga enam ei eksisteeri, mistõttu peab olema see kaalutletud otsus. Koostöös teiste pädevate ametkondadega tuleks ka eraldi analüüsida ka teiste andmekogude staatust eriolukorras, erakorralises seisukorras või sõjaseisukorras.

Vahejäreldus:

- **Justiitsministeeriumil koostöös Majandus- ja Kommunikatsiooniministeeriumi ja teiste asjakohaste koostööpartneritega (AKI, RIA) töötada välja konkreetsemad juhised andmekogu likvideerimiseks ning valmistada ette vastav seadusemuudatus.**