ÕIGUSANALÜÜS

Adressaat:	Majandus- ja Kommunikatsiooniministeerium digimajanduse osakonna reaalajamajanduse valdkond
Autor:	Partner ja vandeadvokaat Liisi Jürgen, NJORD Advokaadibüroo OÜ
Kuupäev:	14.04.2026
Teema:	Andmepõhise aruandluse õigusanalüüs

TEAVITUS

*Käesolev õigusanalüüs („**Analüüs**") põhineb Analüüsi koostamise kuupäeva seisuga Eestis ja Euroopa Liidu tasandil kehtival õigusel ning asjakohasel kohtupraktikal. Analüüs ei käsitle ega arvesta teiste riikide, sealhulgas Euroopa Liidu liikmesriikide siseriiklikke õiguskordi.*

Analüüs ei hõlma õigusakte, regulatsioone ega kohtupraktikat, mis jõustuvad pärast Analüüsi koostamise kuupäeva. Samuti ei võta Analüüs arvesse võimalikke tulevasi õigusmuudatusi ega nende mõju.

Analüüs on koostatud konkreetse tellija jaoks ning lähtub Analüüsi koostamise hetkel kättesaadavast teabest. Analüüsi võib edastada kolmandatele isikutele, kuid NJORD Advokaadibüroo ei vastuta selle kasutamise eest kolmandate isikute poolt ega Analüüsile tuginemise eest väljaspool selle algset eesmärki.

Sisukord

Sissejuhatus 4

Kokkuvõte ja järeldused 5

Vastused tellija küsimustele 7

Õigusanalüüs 36

1. Raamistik ja metoodika 36

1.1. Teabe korraldamine 36

1.2. Andmepõhise aruandluse andmete käsitlus ja metoodika 39

1.3. Andmete omaniku määramise metoodika 46

1.4. Primaarse andmekoguja ja sekundaarse kasutaja õiguste ja kohustuste metoodika once-only põhimõtte rakendamisel 49

2. Õiguslikud piirangud 53

2.1. Põhiseadusest tulenevad piirangud 53

2.2. Andmete kasutamise piirangud süüteomenetluse eesmärgil 54

2.3. Andmete töötlemistoimingute lõikes kehtivad piirangud 56

2.4. Andmete jagamisest keeldumise ja kohustuslikkuse metoodika 57

2.5. Metoodika andmete jagamiseks piiratud õigusraamistikus 59

3. Andmete olemus 61

3.1. Andmete jaotus struktureerituse alusel 61

3.2. APA-spetsiifiline andmetüüpide kaardistus 63

3.3. Andmetüübi miinimumkirjelduse nõuded 69

3.4. Struktureerimata andmete erikäsitlus 73

4. Juhtumipõhine analüüs 75

4.1. Andmete kogumise ja jagamise viisid 75

4.2. Juhtum I – Otsene andmete esitamine ettevõtjalt asutusele (Traditsiooniline kogumismudel) 75

4.3. Juhtum II – Andmete esitamine keskse andmejagamise punkti kaudu (Keskse andmevärava või vahendusteenuse mudel) 76

4.4. Juhtum III – Asutustevaheline andmete jagamine ja väärindatud andmete edastamine (Ristkasutuse ja väärindamise mudel) 78

4.5. Mudelite võrdlus 80

4.6. Teise asutuse eest andmete kogumise metoodika 81

5. APA Rakendamine praktikas 84

5.1. Andmete klassifikatsioon APA kontekstis 84

5.2. Tuletatud andmed APA kontekstis 86

6. Õiguskeskkond ja seos AvTS muutmise VTK-ga kavandatud lahendustega 88

6.1. Andmete teabevärav kui keskne ligipääsu- ja halduskiht 88

6.2. Andmekirjelduste reform ja semantiline koosvõime 88

6.3. Andmekogude asutamise paindlikkuse suurendamine 89
6.4. Sünteetiline hinnang 89
6.5. Kriitiline hinnang VTK piisavusele andmepõhise aruandluse vaates 89
7. Normitehnilised muudatusettepanekud 92
7.1. Avaliku teabe seaduse üldpõhimõtete täiendamine 92
7.2. Andmete kategoriseerimise õiguslik raamistik 94
7.3. Ristkasutuse ja teisese töötlemise regulatsioon 96
7.4. Andmekirjelduse ja kvaliteedi nõuded 99
7.5. Põhiandmete kvaliteedikohustus 100
7.6. Rakendusmääruste vajadus ja roll 101
7.7. Lõppjäreldus 102
Kasutatud allikad 104
Kasutatud kirjandus 104
Kasutatud euroopa liidu õigusaktid 104
Kasutatud eesti õigusaktid 105

Sissejuhatus

Käesoleva õigusanalüüsi eesmärk on hinnata andmepõhise aruandluse (APA) rakendamisega seotud õiguslikke eeldusi, piiranguid ja võimalusi Eesti ning Euroopa Liidu õiguse kontekstis. Analüüs keskendub eelkõige sellele, millistel tingimustel on võimalik vähendada ettevõtjate halduskoormust, tagades samal ajal andmete õiguspärase töötlemise, põhiõiguste kaitse ning avaliku sektori ülesannete tõhusa täitmise.

Õigusanalüüs lähtub *once-only* põhimõttest, mille kohaselt esitab ettevõtja riigile andmeid üksnes ühe korra ning riik tagab nende edasise õiguspärase kasutamise ja jagamise erinevate asutuste vahel. Selle põhimõtte rakendamine eeldab aga selget ja diferentseeritud õiguslikku raamistikku, mis arvestab andmete olemust, tundlikkust, kasutuseesmärki ning töötlemisega kaasnevaid riske.

Analüüsi käigus on välja töötatud metoodika andmete kategoriseerimiseks, tundlikkuse hindamiseks ning andmete kasutamise, jagamise ja korduvkasutuse õiguslikuks hindamiseks. Samuti käsitletakse andmete töötlemisega seotud rolle, toiminguid ja piiranguid ning hinnatakse, millistel juhtudel on võimalik rakendada *once-only* põhimõtet, millistel juhtudel üksnes „ühekordse sisestamise“ lähenemist ning millistel juhtudel tuleb andmete kasutamist piirata. Analüüsis käsitletakse seejuures nii once-only kui ka laiemalt nn *once interaction* põhimõttega kooskõlas olevaid lahendusi

Käesoleva analüüsi põhifookus ei ole riikliku statistika erirežiimi detailne käsitlus APA kontekstis, kuid analüüs arvestab, et APA raamistik ei saa statistikat käsitleda pelgalt ühe andmekasutuse liigina teiste seas. Vajalikud põhimõttelised eristused on sisse toodud eelkõige andmekogumise ja andmete korduvkasutuse üldraamistiku kirjelduses.

Käesoleva õigusanalüüsi tulemusel tehakse ettepanek täiendada avaliku teabe seadust andmete kategoriseerimise, tundlikkuse hindamise, teisese kasutuse, andmekirjelduste miinimumnõuete, põhiandmete kvaliteedikohustuse ning nõusolekupõhise andmejagamise regulatsiooniga. Kavandatavad muudatused loovad õigusliku aluse andmepõhise aruandluse lahenduste rakendamiseks ning *once-only* põhimõtte diferentseeritud kohaldamiseks.

Kokkuvõte ja järeldused

Käesolev õigusanalüüs näitab, et andmepõhine aruandlus ei ole käsitletav ühetaolise tehnilise või õigusliku lahendusena, vaid eeldab diferentseeritud lähenemist, mis arvestab andmete olemust, nende töötlemise eesmärke ning kohaldatavaid õiguslikke piiranguid.

Analüüsist järeldub et ei ole realistlik ega õiguspärane kujundada ühtset universaalset andmete kogumise ja jagamise mudelit. Selle põhjuseks on eelkõige kolm tegurit. Esiteks on andmete tundlikkus erinev, mis mõjutab otseselt andmete töötlemise lubatavust ja tingimusi. Teiseks tulenevad andmete kogumise õiguslikud alused erinevatest seadustest ning ei ole ühtlustatavad ühe üldnormi kaudu. Kolmandaks on andmete töötlemise eesmärgid erinevad, hõlmates muu hulgas maksustamist, statistikat, järelevalvet ja avaliku teabe avalikustamist.

Sellest tulenevalt eeldab APA rakendamine mitmetasandilist ja diferentseeritud õiguslikku raamistikku.

Peamised järeldused kehtiva õiguse kohta

Analüüsi tulemusel ilmnevad mitmed süsteemsed lüngad kehtivas õiguses, mis takistavad andmepõhise aruandluse täiemahulist rakendamist.

Esiteks puudub selge ja üldine regulatsioon andmete teisese kasutuse kohta. Kehtiv õigus ei sisalda ühtset normi, mis määratleks, millistel tingimustel võib üks asutus kasutada teise asutuse kogutud andmeid, mistõttu on andmete ristkasutus killustatud ja õigusselgus piiratud.

Teiseks ei ole seaduse tasandil kehtestatud põhiandmete kvaliteedinõudeid. Andmete kvaliteet on aga *once-only* põhimõtte rakendamise eelduseks, kuna vigased või ebaühtlased andmed takistavad nende korduvkasutust.

Kolmandaks puudub andmete tundlikkuse ühtne klassifikatsioon. Ilma selleta ei ole võimalik rakendada diferentseeritud andmejagamise reegleid ega hinnata andmete kasutamisega seotud riske süsteemselt.

Neljandaks on nõusolekuteenuse õiguslik alus killustatud. Kuigi nõusolek võib teatud juhtudel võimaldada andmete jagamist, ei ole selle kasutamise tingimused avaliku sektori kontekstis piisavalt selgelt määratletud.

Viiendaks ei ole andmekirjelduse miinimumnõuded sätestatud seaduse tasandil ning puuduvad ka piisavad tehnilised standardid määruse tasemel, mis tagaksid andmete semantilise koosvõime ja ühtse tõlgendamise.

Andmete olemus ja struktureeritus

Analüüs kinnitab, et andmete struktureeritus on keskne tegur APA rakendamisel. Struktureeritud andmed võimaldavad automatiseeritud, masinloetavat ja standardiseeritud andmevahetust, mis on *once-only* põhimõtte toimimise eelduseks.

Struktureerimata andmete puhul rakendub korduvkasutus piiratumalt ning tugineb eelkõige dokumentide leitavusele ja kontrollitud jagamisele. Sellest tulenevalt on struktureerimata andmete puhul suurem nii õiguslik kui ka praktiline risk, eelkõige seoses konfidentsiaalsuse, eesmärgipiirangu ja tõlgendusvastutusega.

Seega määrab andmete struktureeritus otseselt nii nende kasutatavuse kui ka nendega seotud riskitaseme.

Horisontaalsed õiguslikud piirangud

Analüüs toob esile ka horisontaalsed piirangud, mis mõjutavad APA rakendamist sõltumata andmete liigist.

Eelkõige puudutab see andmete kasutamist süüteomenetluse eesmärgil, kus kohaldub eriregulatsioon ning kõrgendatud põhiõiguste kaitse standard. Andmete kasutamine süütegude ennetamiseks või uurimiseks ei saa toimuda ilma selge õigusliku aluseta ning nõuab eraldi kaalutlust iga konkreetse kasutusjuhtumi puhul.

Samuti tuleb arvestada, et andmete töötlemine avalikus sektoris peab alati olema kooskõlas proportsionaalsuse, minimaalsuse ja eesmärgipiirangu põhimõtetega.

Nõusolekuteenuse roll

Nõusolekuteenuse kasutamine APA kontekstis on oma olemuselt täiendav, mitte asendav mehhanism.

Kuigi nõusolek võib võimaldada andmete jagamist olukordades, kus seadusest tulenev alus puudub, ei saa see asendada avaliku sektori ülesannete täitmiseks vajalikku seaduslikku alust. Lisaks seab kehtiv õigus nõusolekule ranged tingimused, eelkõige seoses vabatahtlikkuse ja teadlikkusega.

Samas võimaldavad Euroopa Liidu andmemajanduse arengusuunad ning Eesti kavandatavad lahendused kasutada nõusolekuteenust kontrollitud ja läbipaistva andmejagamise mehhanismina, eelkõige ettevõtjate huvides.

Juhtumipõhine järeldus

Juhtumipõhine analüüs kinnitab, et andmete kogumise ja jagamise erinevad mudelid (otsene kogumine, keskne vahendamine ja asutustevaheline ristkasutus) toovad kaasa erinevad õiguslikud probleemid.

Eelkõige ilmnevad probleemid seoses:

- andmete teisese kasutuse lubatavusega,
- vastutuse ja rollide määratlemisega,
- eesmärgipiirangu järgimisega.

Sellest tulenevalt ei ole võimalik rakendada ühtset regulatsioonimudelit, vaid vajalik on diferentseeritud normitehniline lähenemine.

Lõppjäreldus

Kokkuvõttes näitab analüüs, et andmepõhise aruandluse edukas rakendamine eeldab terviklikku õigusraamistiku arendamist, mis põhineb andmete diferentseerimisel, selgetel volitusnormidel ning riskipõhisel lähenemisel.

Õiguslikult toimiva APA mudeli eelduseks on:

- andmete liigitamine ja tundlikkusepõhine käsitlus,
- selge regulatsioon andmete teisese kasutuse kohta,
- andmekirjelduste ja kvaliteedinõuete kehtestamine,
- rollide ja vastutuse täpne määratlemine,
- kontrollitud mehhanismid andmete jagamiseks, sealhulgas vajaduse korral nõusolekupõhiselt.

Selline raamistik võimaldab ühtaegu vähendada ettevõtjate halduskoormust ning tagada andmete õiguspärane, turvaline ja läbipaistev kasutamine avalikus sektoris.

Vastused tellija küsimustele

Analüüsi käigus peab töövõtja käsitlema vähemalt järgmisi teemasid:

1.2.1. Andmepõhise aruandlusega seotud õigusaktide analüüs (s.o hetkel kehtiv õigusraamistik) ja sellest tulenevad nõuded ja praktikad andmepõhise aruandluse täieulatuslikuks riigiüleseks rakendamiseks. Analüüs peab vastama järgmistele tingimustele, analüüsipunktidele ja küsimustele:

1.2.2. APA lahenduste puhul on eelistatud *once-only* põhimõte, mille kohaselt esitab ettevõtja aruandluseks või muul põhjusel esitatavaid andmeid riigile ainult ühe korra. Edaspidi tagab riik nende andmete korduvkasutuse, jagamise ja töötlemise erinevate asutuste vahel. Samu või sarnaseid andmeid koguvad asutused peaksid juhul, kui selleks ei ole õiguslikke või tehnilisi või sisulisi takistusi, andmeid omavahel vahetama ning vajadusel koguma lisaandmeid ka teise asutuse eest, et ettevõtja halduskoormust vähendada. *Once-only* põhimõtet on rakendatud ka juhul, kui ettevõte on andmed ühe korra oma tarkvarasse sisestanud ja need seal seadistanud ning saadab need ühe korraga välja erinevatele riigiasutustele.

***Once-only* põhimõtte rakendamine andmepõhise aruandluse raamistikus**

Once-only põhimõte kujutab endast andmepõhise aruandluse keskset korralduspõhimõtet, mille eesmärk on vähendada ettevõtjate halduskoormust ning suurendada avaliku sektori andmekasutuse efektiivsust. Selle kohaselt esitab ettevõtja andmed riigile üksnes ühe korra, mille järel toimub nende edasine kasutamine, jagamine ja töötlemine riigisiseselt asutuste vahel.

Käesolev analüüs lähtub seisukohast, et *once-only* põhimõte ei ole üksik tehniline lahendus, vaid mitmetasandiline õiguslik ja korralduslik raamistik, mille rakendamine eeldab erinevate andmete kogumise ja jagamise mudelite koostoimet. Nagu on täpsemalt käsitletud peatükis „Andmete kogumise ja jagamise viisid: juhtumipõhine käsitlus“, realiseerub *once-only* põhimõte kolmes peamises olukorras: (i) esmase andmete kogumise etapis, (ii) keskse andmejagamise mehhanismi kaudu ning (iii) asutustevahelise ristkasutuse ja väärindatud andmete edastamise kaudu.

Lisaks hõlmab *once-only* põhimõte ka olukordi, kus ettevõtja sisestab andmed üksnes oma infosüsteemi ning edastab need sealt automatiseeritult erinevatele riigiasutustele. Sellisel juhul ei toimu küll andmete jagamine riigi sees, kuid ettevõtja vaates on halduskoormus samaväärselt vähenenud. Seetõttu tuleb *once-only* põhimõtet käsitada laiemalt kui pelgalt andmete riigisisest taaskasutust – see hõlmab ka andmete ühekordset tekkimist ettevõtja tasandil ning nende korduvat kasutamist erinevates kontekstides.

Once-only ja *once interaction* põhimõtted

APA raamistik toetub klassikalisele once-only põhimõttele, mille kohaselt ei peaks ettevõtja esitama sama andmestikku korduvalt erinevatele asutustele. Statistikaameti vaatenurgast ei pruugi see üksnes iseenesest halduskoormust vähendada, kui andmekogumise protsesse ei koordineerita sisuliselt.

Seetõttu on APA kujundamisel oluline arvestada ka nn *once interaction* põhimõttega: ettevõtjat ei tohiks koormata sama teema kohta mitme asutuse paralleelse või ajas hajutatud suhtlusega. Eelistada tuleks lahendust, kus andmeid kogub see asutus, kellel on andmeesitajaga kõige sisulisem ja otstarbekam kontakt, ning teised asutused kasutavad neid andmeid APA raamistikus korduvkasutusena. Once-only ja *once interaction* põhimõtted peaksid APA-s toimima koos: andmeid esitatakse ühe korra ning võimalusel ühe peamise kontaktasutuse kaudu.

Õiguslikust perspektiivist ei ole *once-only* põhimõte kehtivas õiguses terviklikult ja ühtselt reguleeritud. Selle üksikuid elemente võib tuvastada erinevates normides (nt andmete minimaalsuse põhimõte (IKÜM art 5 lg 1 p c), andmete ristkasutuse võimalused), kuid puudub selge üldnorm, mis kohustaks asutusi vältima dubleerivat andmete kogumist ning eelistama olemasolevate andmete taaskasutust. Samuti ei ole üheselt määratletud, millistel tingimustel võivad asutused koguda andmeid „teise asutuse eest" või millal on selline tegevus lubatav.

Sellest tulenevalt eeldab *once-only* põhimõtte tõhus rakendamine:

- andmete esmakogumise kvaliteedi ja ulatuse selget reguleerimist (vt peatükid andmetüüpide kaardistuse ja miinimumkirjelduse nõuete kohta);
- keskse andmejagamise mehhanismi õiguslikku raamistikku (vt normitehnilised ettepanekud AvTS täiendamiseks);
- asutustevahelise andmekasutuse ja teisese töötlemise selget regulatsiooni (vt peatükid ristkasutuse ja õigusliku riskihindamise kohta).

Kokkuvõttes tuleb *once-only* põhimõtet käsitada kui süsteemset eesmärki, mille saavutamine eeldab nii tehnilisi lahendusi kui ka terviklikku õigusraamistiku kujundamist. Käesolev analüüs näitab, et põhimõtte realiseerimiseks ei piisa üksikute muudatuste tegemisest, vaid vajalik on diferentseeritud ja riskipõhine lähenemine, mis arvestab andmete tüüpi, tundlikkust ja kasutuseesmärki.

1.2.3 Millised kehtivates õigusaktides sätestatud nõuded kujundavad täna andmepõhise aruandluse õiguslikku keskkonda?

Sissejuhatav raamistik

Andmepõhise aruandluse õiguslik keskkond ei tulene ühest tervikseadusest, vaid on kujunenud mitme horisontaalse ja valdkondliku õigusakti koosmõjus.

Need õigusaktid reguleerivad:

- andmete kogumise õigust ja kohustust,
- andmete vormi ja esitamise viisi,
- andmete töötlemise eesmärke,
- andmete säilitamist,
- andmete jagamist asutuste vahel,
- juurdepääsu ja avalikustamist.

APA visiooni rakendatavus sõltub seega sellest, kuidas olemasolevad normid võimaldavad või piiravad:

- struktureeritud andmete kogumist,
- masinloetavust,
- ristkasutust,
- *once-only* põhimõtet.

Euroopa Liidu õigusest tulenevad nõuded

Isikuandmete kaitse üldmäärus (IKÜM)[1]

IKÜM kujundab APA õigusliku keskkonna kõige tugevamalt isikuandmete osas.

Peamised nõuded:

a) Õigusliku aluse nõue (art 6)

Iga andmevälja kogumiseks peab eksisteerima õiguslik alus:

- seadusest tulenev kohustus,
- avaliku ülesande täitmine,
- nõusolek (piiratud juhtudel).

b) Eesmärgipiirang (art 5)

Andmeid tohib kasutada vaid kogumise eesmärgiga kooskõlas oleval viisil. See mõjutab otseselt ristkasutust ja *once-only* rakendamist.

c) Minimaalsuse põhimõte

Koguda tohib ainult vajalikke andmeid. Piirab ülemäärast andmepõhist aruandlust.

d) Säilitamise piirang

Eriliiki andmete pikaajaline säilitamine võib olla keelatud.

e) Automatiseeritud otsustamine (art 22)

Väärindatud andmete kasutamisel otsustusprotsessis tekivad täiendavad nõuded.

Avaandmete direktiiv[2]

Mõjutab APA-t avaandmete osas:

- masinloetavus,
- avatud vormingud,
- korduskasutus.

Horisontaalne riigisisene õigusraamistik

Avaliku teabe seadus (AvTS)[3]

AvTS on APA keskne horisontaalne seadus.

Peamised APA-d mõjutavad nõuded:

a) Andmekogude asutamine ja pidamine

- andmekogu põhimäärus,

---

[1] 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). - ELT L 119, lk 1.

[2] 20. juuni 2019. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2019/1024, avaandmete ja avaliku sektori valduses oleva teabe taaskasutamise kohta (uuesti sõnastatud). – ELT L 172, lk 56–83.

[3] RT I, 06.03.2026, 3

- vastutav töötleja,
- andmekoosseis.

b) Põhiandmete regulatsioon

- kohustus vältida dubleerimist,
- keskallika põhimõte.

c) Avaandmete ja juurdepääsupiirangute regulatsioon

- määrab andmete jagamise ulatuse.

d) Andmekirjelduste nõuded (RIHA kaudu)

- metaandmed,
- kirjelduste avalikustamine.

Haldusmenetluse seadus (HMS)[4]

HMS mõjutab APA-t menetlusandmete kaudu.

Peamised nõuded:

- tõendite kogumine,
- selgitamiskohustus,
- andmete kontrollimise kohustus.

See võib piirata täielikku automatiseerimist, sest asutus peab säilitama menetlusliku kontrolli.

Tsiviilseadustiku üldosa seadus (TsÜS)[5]

Mõjutab:

- juriidilise isiku andmete esitamise õigust,
- esindusõigust,
- tahteavalduse andmist (nt API kaudu esitatud andmed).

Isikuandmete kaitse seadus (IKS)[6]

IKS täpsustab IKÜMi rakendamist Eesti kontekstis.

Olulised aspektid:

- avaliku sektori erisused,
- järelevalve,
- sanktsioonid.

IKS võib piirata andmete ristkasutust, kui puudub selge avaliku huvi alus.

Valdkondlikud aruandlus- ja andmekogumisseadused

[4] RT I, 06.07.2023, 31
[5] RT I, 31.12.2024, 48
[6] RT I, 06.03.2026, 10

APA toimimine sõltub otseselt valdkondlikest normidest, mis sätestavad konkreetsete andmete kogumise.

Maksukorralduse seadus (MKS)[7]

- maksudeklaratsioonid,
- andmete esitamise kohustus,
- maksusaladuse kaitse.

Piirab ristkasutust maksusaladuse tõttu.

Riikliku statistika seadus (RStS)[8]

- õigus koguda andmeid otse ettevõtjatelt,
- dubleeriva kogumise probleem,
- agregeerimise kohustus.

Raamatupidamise seadus (RPS)[9]

- majandustehingute dokumenteerimine,
- säilitamistähtajad,
- algandmete kvaliteet.

Loob APA algandmete õigusliku aluse.

Keskkonna- ja sektoriseadused

Näiteks:

- kütusearuandlus,
- jäätmearuandlus,
- heiteandmed.

Sageli dokumendipõhised — vajavad andmepõhist üleminekut.

Andmete jagamist reguleerivad normid

Asutustevaheline andmevahetus

Tulenevad:

- eriseadustest,
- põhimäärustest,
- andmekogude asutamisdokumentidest.

Probleem:

- jagamisõigus on killustatud,

[7] RT I, 02.10.2025, 4
[8] RT I, 11.03.2022, 2
[9] RT I, 10.07.2025, 3

- puudub üldnorm teisese kasutuse kohta.

Saladusrežiimid

Olulised piirangud tulenevad:

- maksusaladusest,
- ärisaladusest,
- statistikasaladusest,
- julgeolekupiirangutest.

Need määravad, milliseid andmeid saab ristkasutada.

Tehnilised ja registripõhised nõuded

APA-t kujundavad ka tehnilised regulatsioonid:

- RIHA andmekirjeldused,
- klassifikaatorite süsteem,
- X-tee andmevahetus,
- autentimine (eIDAS[10], e-identimise ja e-tehingute usaldusteenuste seadus[11]).

Need ei ole üksnes tehnilised, vaid omavad õiguslikku tähendust (nt andmete õigsus, jälgitavus).

Sünteetiline hinnang

Kehtiv õigusraamistik:

- võimaldab APA elemente osaliselt;
- kuid ei toeta süsteemselt ristkasutust;
- ei reguleeri piisavalt teisest kasutust;
- ei käsitle väärindatud andmete jagamist;
- ei sätesta andmete tundlikkuse klassifikatsiooni.

Õiguslik keskkond on seega fragmentaarne, valdkonnapõhine ja dokumendikeskne, mitte andmepõhine.

Kokkuvõte

Täna kujundavad APA õiguslikku keskkonda eelkõige:

1. IKÜM ja IKS – isikuandmete töötlemise piirangud;
2. AvTS – andmekogud, põhiandmed, juurdepääs;
3. HMS – menetluslikud nõuded;
4. Maksu- ja statistikaõigus – aruandluskohustused;

[10] 23. juuli 2014. aasta Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. – ELT L 257, lk 73.

[11] E-identimise ja e-tehingute usaldusteenuste seadus, RT I, 30.12.2025, 16.

5. Raamatupidamise seadus – algandmete kvaliteet;
6. Saladusrežiimid – jagamise piirangud;
7. Tehnilised registriraamistikud – andmevahetuse toimeloogika.

Need normid loovad APA rakendamiseks vajaliku aluse, kuid ei moodusta veel terviklikku, *once-only* põhimõttel toimivat andmepõhist aruandlusraamistikku.

1.2.4. Millistest Eesti ja Euroopa Liidu õigusaktidest tulenevad piirangud APA rakendamisel? Muuhulgas tuua välja, millised Eesti ja Euroopa Liidu õigusaktid kehtestavad täna õigusliku aluse andmete esitamiseks ettevõtjalt riigile või seavad sellele piiranguid? Millised Eesti või Euroopa Liidu õigusaktid kehtestavad õigusliku aluse andmete vahetamiseks riigiasutuse vahel või seavad sellele piiranguid?

Õiguslikud piirangud andmepõhise aruandluse rakendamisel

Andmepõhise aruandluse rakendamisel tuleb arvestada olemasoleva Eesti ja Euroopa Liidu õigusraamistiku kontekstiga, mis ühelt poolt loob alused andmete kogumiseks ja vahetamiseks, kuid teiselt poolt seab sellele olulised piirangud. Need piirangud tulenevad eelkõige andmekaitseõigusest, haldusõigusest ning valdkondlikest eriseadustest, mis reguleerivad nii andmete esmast kogumist ettevõtjalt kui ka andmete edasist kasutamist ja jagamist riigiasutuste vahel.

1. Andmete esitamine ettevõtjalt riigile

Eestis tuleneb ettevõtjate kohustus andmete esitamiseks eelkõige valdkondlikest eriseadustest, mis sätestavad nii kogutavate andmete liigi kui ka nende esitamise tingimused. Olulisemad õigusaktid on:

- Maksukorralduse seadus ja maksuseadused (nt tulumaksuseadus, käibemaksuseadus), mis sätestavad maksuarvestuseks vajalike andmete esitamise kohustuse ning kehtestavad maksusaladuse kaitse;
- Raamatupidamise seadus, mis reguleerib majandustehingute kajastamist ning aruandluse aluseks olevate andmete pidamist;
- Riikliku statistika seadus, mis annab Statistikaametile õiguse koguda andmeid statistilistel eesmärkidel;
- valdkondlikud eriseadused (nt keskkonna-, energia- või tööõiguse valdkonnas), mis sätestavad spetsiifilised aruandluskohustused.

Euroopa Liidu tasandil tulenevad andmete esitamise kohustused muu hulgas:

- sektoripõhistest määrustest ja direktiividest (nt finantsaruandlus, kestlikkusaruandlus (CSRD));
- Euroopa statistika õigusaktidest;
- ning kaudselt ka digitaalse ühtse turu regulatsioonidest, mis mõjutavad andmete esitamise ja kättesaadavuse nõudeid.

Samas piirab andmete kogumist eelkõige isikuandmete kaitse üldmäärus, mis nõuab, et igasugune andmete kogumine tugineb õiguslikule alusele, on eesmärgipärane ja proportsionaalne. Lisaks tulenevad piirangud ka põhiseadusest[12], eelkõige eraelu puutumatuse ja ettevõtlusvabaduse kaitse põhimõtetest.

[12] RT I, 11.04.2025, 3.

2. Andmete vahetamine riigiasutuste vahel

Andmete vahetamine riigiasutuste vahel on Eestis lubatud üksnes juhul, kui selleks on olemas selge õiguslik alus. Peamised õigusaktid, mis seda reguleerivad, on:

- **Avaliku teabe seadus (AvTS)**, mis sätestab andmekogude pidamise, teabe avalikustamise ning juurdepääsupiirangute üldraamistiku;
- **Isikuandmete kaitse seadus (IKS)** koos IKÜM-iga, mis reguleerib isikuandmete töötlemist, sh nende edastamist erinevate vastutavate töötlejate vahel;
- valdkondlikud eriseadused (nt maksukorralduse seadus), mis sageli piiravad andmete edastamist (nt maksusaladuse kaitse);
- **Riigi infosüsteemi haldussüsteemi (RIHA)**[13] **ja X-tee raamistik**[14], mis küll tehniliselt võimaldavad andmete vahetust, kuid ei loo iseseisvat õiguslikku alust andmete jagamiseks.

Euroopa Liidu tasandil mõjutavad asutustevahelist andmevahetust eelkõige:

- **IKÜM**, mis seab tingimused andmete edastamisele ja teisesele kasutamisele;
- **Andmehalduse määrus (*Data Governance Act*)**[15], mis reguleerib avaliku sektori andmete taaskasutust;
- **Andmemäärus (*Data Act*)**[16], mis käsitleb andmete kättesaadavust ja jagamist, sh ettevõtjate ja avaliku sektori vahel;
- sektoripõhised EL regulatsioonid, mis võivad nii lubada kui ka piirata andmete ristkasutust.

3. Peamised piirangud APA rakendamisel

Kehtivast õigusraamistikust tulenevad APA rakendamise peamised piirangud on järgmised:

- **eesmärgipiirang** – andmeid võib kasutada üksnes eesmärgil, milleks need on kogutud, välja arvatud juhul, kui teisene kasutus on selgelt lubatud;
- **õigusliku aluse nõue** – iga andmete kogumine ja edastamine peab tuginema seadusele või muule õiguspärasele alusele;
- **konfidentsiaalsus- ja saladuse režiimid** – nt maksusaladus, ärisaladus ja statistiline konfidentsiaalsus piiravad andmete jagamist;
- **proportsionaalsuse ja minimaalsuse põhimõtted** – kogutavate ja jagatavate andmete maht peab olema piiratud vajalikuga;
- **vastutuse ja rollide ebaselgus** – eriti kesksete andmejagamise mehhanismide puhul puudub sageli selge regulatsioon, kes vastutab andmete edastamise ja kasutamise eest.

Kokkuvõte

---

[13] RT I, 29.12.2024, 15.
[14] RT I, 06.08.2019, 17.
[15] 30. mai 2022. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2022/868, Euroopa andmehalduse kohta ning millega muudetakse määrust (EL) 2018/1724 (andmehalduse määrus). – ELT L 152, lk 1–44.
[16] 13. detsembri 2023. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2023/2854, ühtlustatud õigusnormide kohta, millega reguleeritakse õiglast juurdepääsu andmetele ja andmete kasutamist, millega muudetakse määrust (EL) 2017/2394 ja direktiivi (EL) 2020/1828 (andmemäärus). – ELT L.

Kokkuvõttes võib järeldada, et kuigi Eesti ja Euroopa Liidu õigusaktid loovad ulatusliku aluse andmete kogumiseks ja kasutamiseks, on need kujundatud valdavalt valdkonnapõhiselt ning ei toeta täiel määral andmepõhise aruandluse terviklikku rakendamist. Eelkõige piiravad APA rakendamist eesmärgipiirangu põhimõte, andmete jagamise selge õigusliku aluse nõue ning konfidentsiaalsusrežiimid. See tingib vajaduse arendada õigusraamistikku suunas, mis võimaldab diferentseeritud ja kontrollitud andmete ristkasutust, säilitades samal ajal põhiõiguste kaitse ja õigusselguse.

1.2.5. Millised teised Eestis või Euroopa Liidus kehtestatud õiguslikud piirangud täna APA lahenduste juurutamist mõjutavad? Muuhulgas tuua välja, kas ja millistel tingimustel nõutakse andmete edastamisel ettevõtjalt riigile andmete edastaja elektroonilist tuvastamist (e-ID)?

Muud õiguslikud piirangud APA lahenduste juurutamisel, sh elektrooniline tuvastamine

Lisaks andmete kogumist ja vahetamist otseselt reguleerivatele õigusaktidele mõjutavad andmepõhise aruandluse lahenduste juurutamist mitmed horisontaalsed õiguslikud nõuded, mis puudutavad eelkõige isikutuvastust, infosüsteemide turvalisust, elektroonilist asjaajamist ning digitaalse identiteedi kasutamist. Need nõuded ei pruugi reguleerida andmete sisu, kuid seavad olulised tingimused andmete esitamise viisile ja tehnilisele korraldusele.

1. Elektroonilise tuvastamise (e-ID) nõuded

Eestis toimub ettevõtjate ja riigi vaheline elektrooniline suhtlus üldjuhul turvalise elektroonilise identiteedi alusel. Elektroonilise tuvastamise ja autentimise raamistik tuleneb eelkõige:

- isikut tõendavate dokumentide seadusest (ITDS)[17], mis sätestab elektroonilise isikutuvastuse vahendite (nt ID-kaart, mobiil-ID, Smart-ID) kasutamise alused;
- eIDAS määrusest (EL) nr 910/2014, mis reguleerib elektroonilist identiteeti ja usaldusteenuseid Euroopa Liidus ning sätestab nõuded elektroonilisele autentimisele ja allkirjastamisele;
- avaliku sektori teenuste toimimise praktikast, kus autentimine on vajalik nii isiku tuvastamiseks kui ka esindusõiguse kontrollimiseks.

Praktikas tähendab see, et andmete esitamine ettevõtjalt riigile toimub valdavalt autentitud keskkondades, kus andmete edastaja tuvastatakse elektroonilise identiteedi vahendite abil. Eelkõige on see vajalik olukordades, kus:

- esitatakse õiguslikke tagajärgi omavaid andmeid (nt maksudeklaratsioonid);
- kontrollitakse isiku või esindaja õigust tegutseda juriidilise isiku nimel;
- tagatakse andmete päritolu ja terviklus.

Samas ei ole elektrooniline tuvastamine alati absoluutne nõue. APA kontekstis on oluline eristada olukordi, kus andmed edastatakse:

- inimese poolt (nt deklaratsiooni kinnitamine) – sellisel juhul on tugev autentimine üldjuhul vajalik;
- masin-masin liidese kaudu (API-põhine edastus) – sellisel juhul asendub isikupõhine autentimine süsteemipõhise autentimisega (nt sertifikaadid, teenusepõhised identiteedid), kuid ka siis peab olema tagatud vastutuse ja päritolu tuvastatavus.

[17] RT I, 26.06.2025, 6.

Seega ei seisne piirang mitte niivõrd e-ID kohustuslikkuses igas olukorras, vaid nõudes, et andmete edastamine peab toimuma usaldusväärselt tuvastatud ja kontrollitud identiteedi kaudu.

2. Infosüsteemide turvalisuse ja andmekaitse nõuded

APA lahenduste juurutamist mõjutavad oluliselt ka küberturvalisuse ja andmekaitse nõuded, mis tulenevad muu hulgas:

- küberturvalisuse seadusest (KüTS)[18], mis sätestab oluliste teenuste ja infosüsteemide turvanõuded;
- IKÜM-ist, mis nõuab andmete töötlemisel sobivate tehniliste ja organisatsiooniliste meetmete rakendamist;
- riigi infosüsteemi toimimise põhimõtetest (nt X-tee turvaraamistik).

Need nõuded seavad piiranguid sellele, kuidas andmeid võib edastada (nt krüpteerimine, autentimine, logimine) ning välistavad lahendused, mis ei taga piisavat turvalisust.

3. Elektroonilise asjaajamise ja digitaalse tõendatavuse nõuded

APA rakendamisel tuleb arvestada ka elektroonilise asjaajamise nõuetega, eelkõige:

- vajadusega tagada andmete tõendatavus ja jälgitavus;
- nõudega, et esitatud andmed oleksid seostatavad konkreetse esitajaga;
- kohustusega säilitada andmete esitamise ja kasutamise kohta logid.

See tuleneb nii haldusmenetluse üldpõhimõtetest kui ka usaldusteenuste regulatsioonist (eIDAS), mis nõuab, et elektroonilised toimingud oleksid õiguslikult tõendatavad.

4. Mõju APA rakendamisele

Eeltoodud nõuded mõjutavad APA lahenduste kujundamist mitmel viisil. Esiteks tähendab see, et täielikult anonüümne või kontrollimatu andmevahetus ei ole lubatav – igal andmeedastusel peab olema tuvastatav allikas ja vastutav subjekt. Teiseks tuleb API-põhiste lahenduste puhul tagada, et süsteemipõhine autentimine on õiguslikult samaväärne isikupõhise tuvastamisega. Kolmandaks tuleb andmete esitamise ja kasutamise protsessid kujundada viisil, mis võimaldab hilisemat kontrolli ja auditeerimist.

Kokkuvõttes ei takista elektroonilise tuvastamise nõuded APA rakendamist, kuid seavad selged raamid sellele, kuidas andmeid võib edastada. APA lahendused peavad seetõttu integreerima nii isiku- kui ka süsteemipõhise autentimise mehhanismid ning tagama andmete päritolu, tervikluse ja kasutamise jälgitavuse kooskõlas kehtiva õigusega.

1.2.6. Kuidas on APA rakendamist mõjutavates Eesti ja Euroopa Liidu õigusaktides täna kirjeldatud erinevat tüüpi andmeid? (isikuandmed, avaandmed etc)? Millised on erinevat tüüpi andmete töötlemisele seatud õiguslikud piirangud ning millistest õigusaktidest need tulenevad?

Andmeliikide käsitlus ning nendega seotud õiguslikud piirangud APA kontekstis

Eesti ja Euroopa Liidu õigusraamistikus ei ole andmeid käsitletud ühtse klassifikatsiooni alusel, vaid erinevate õigusaktide kaudu, lähtudes andmete sisust, kasutuseesmärgist ja nendega seotud riskidest. Sellest tulenevalt on andmete liigitus killustunud ning sama andmeliik võib olla erinevates kontekstides

[18] RT I, 30.12.2025, 15.

erineva õigusliku režiimiga. Andmepõhise aruandluse rakendamisel on keskse tähtsusega mõista, milliseid andmeliike kehtiv õigus eristab ning millised piirangud nende töötlemisele kehtivad.

1. Isikuandmed

Kõige selgemalt reguleeritud andmeliik on isikuandmed, mida käsitletakse Euroopa Liidu tasandil **isikuandmete kaitse üldmääruses (IKÜM)** ning Eestis täiendavalt **isikuandmete kaitse seaduses (IKS)**. Isikuandmeteks loetakse igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta.

Isikuandmete töötlemisele kehtivad ranged piirangud, sealhulgas:

- nõue tugineda selgele õiguslikule alusele (nt seadus, nõusolek, avalik huvi);
- eesmärgipiirangu põhimõte (andmeid võib kasutada üksnes kindlaksmääratud eesmärgil);
- minimaalsuse ja proportsionaalsuse põhimõtted;
- täiendavad piirangud eriliigilistele isikuandmetele.

APA kontekstis tähendab see, et isikuandmete ristkasutus on lubatav üksnes selge õigusliku aluse olemasolul ning nõuab sageli täiendavaid kaitsemeetmeid.

2. Avalik teave ja avaandmed

Avaliku sektori valduses olev teave on reguleeritud eelkõige **avaliku teabe seadusega (AvTS)**. AvTS eristab:

- avalikku teavet, millele on üldjuhul juurdepääs;
- juurdepääsupiiranguga teavet;
- avaandmeid, mis on masinloetaval kujul vabalt taaskasutatavad.

Avaandmete taaskasutust toetab ka Euroopa Liidu **avaandmete direktiiv (*Open Data Directive*)**, mis soodustab avaliku sektori teabe kättesaadavust ja korduvkasutust.

Avaliku teabe puhul on piirangud seotud eelkõige:

- juurdepääsupiirangutega (nt isikuandmed, ärisaladus);
- turvalisuse ja konfidentsiaalsuse nõuetega.

APA seisukohalt on just avaandmed kõige kõrgema ristkasutatavusega andmeliik.

3. Ärisaladus ja maksusaladus

Teatud andmed on kaitstud eraldi konfidentsiaalsusrežiimidega, näiteks:

- **ärisaladus**, mida kaitstakse nii lepinguliselt kui ka seaduse alusel (nt võlaõigusseadus, ebaausa konkurentsi regulatsioon);
- **maksusaladus**, mis on sätestatud **maksukorralduse seaduses (MKS)**.

Selliste andmete töötlemisele kehtivad ranged piirangud:

- andmeid võib kasutada üksnes seaduses sätestatud eesmärgil;
- andmete edastamine teistele asutustele on piiratud või eraldi reguleeritud;
- rikkumisel võivad kaasneda sanktsioonid.

APA kontekstis on need andmeliigid olulised piiravad tegurid, kuna nende ristkasutus ei ole võimalik ilma selge õigusliku aluseta.

4. Statistilised andmed

Statistiliste andmete kogumine ja kasutamine on reguleeritud riikliku statistika seadusega ning Euroopa Liidu statistikaõigusega. Statistilise töötlemise eripäraks on:

- andmete kasutamine anonümiseeritud või koondatud kujul;
- statistilise konfidentsiaalsuse põhimõte, mis keelab üksikandmete avalikustamise.

Kuigi statistilised andmed on sageli hästi struktureeritud, on nende ristkasutus piiratud konfidentsiaalsusnõuetega. Statistilisi andmeid ei tohi APA raames kasutada üksikjuhtumite haldus-, menetlus- või järelevalveotsuste tegemiseks, isegi kui tehniliselt oleks andmete tagasi sidumine üksikettevõtjaga võimalik.

5. Administratiivandmed ja eraldi statistiline kogumine

Statistika seisukohalt on APA üks eeldus see, et statistikaasutused saavad maksimaalsel määral tugineda olemasolevatele administratiivandmetele, eeldusel et need vastavad kvaliteedi- ja kasutusnõuetele. Riikliku statistika regulatiivne raamistik näeb ette, et statistilisi otstarbeid silmas pidades ei tohi ettevõtjaid koormata tarbetult korduva andmete esitamisega.

Samas ei pruugi kõik administratiivandmed olla statistiliseks kasutuseks sobivad, näiteks kui andmed on kogutud järelevalve või menetluse raames, on ebaühtlase kvaliteediga või ei kata vajalikku populatsiooni. APA raamistikus on vajalik selgem metoodiline raamistik, mille alusel hinnata:

(i) millal on administratiivandmete kasutamine statistika eesmärgil piisav (kvaliteet, täielikkus, ajakohasus, juriidiline kasutusõigus);
(ii) millal on põhjendatud eraldi statistiline andmekogumine, hoolimata administratiivandmete olemasolust.

Nende kriteeriumide täpne määratlemine eeldab koostööd Statistikaameti ja teiste andmekogujatega, kuid APA õigusraamistik peab looma selge aluse selliste otsuste tegemiseks ja dokumenteerimiseks.

6. Tuletatud ja analüütilised andmed

Kehtiv õigus ei käsitle ühtselt tuletatud või väärindatud andmeid (nt riskihinnangud, koondnäitajad). Selliste andmete õiguslik režiim sõltub:

- sisendandmete liigist (nt kas sisaldavad isikuandmeid);
- kasutuseesmärgist (nt kas tehakse haldusotsuseid).

Siin tekivad sageli õiguslikud küsimused:

- kas tegemist on uue andmekogumiga;
- millised piirangud laienevad tuletatud andmetele;
- kes vastutab andmete õigsuse eest.

7. Euroopa Liidu andmemajanduse regulatsioon

Lisaks eeltoodule mõjutavad andmete liigitust ja kasutamist ka uued EL õigusaktid, eelkõige:

- *Data Governance* Act, mis reguleerib avaliku sektori andmete taaskasutust;
- *Data Act*, mis käsitleb andmete kättesaadavust ja jagamist erinevate osapoolte vahel.

Need õigusaktid ei loo uusi klassikalisi andmeliike, kuid mõjutavad oluliselt seda, kuidas andmeid võib jagada ja taaskasutada.

Kokkuvõte

Kokkuvõttes käsitletakse Eesti ja Euroopa Liidu õiguses andmeid erinevate kategooriate kaudu, mis tulenevad peamiselt andmete sisust ja nendega seotud riskidest. Kõige olulisemad eristused tehakse isikuandmete, avaliku teabe, konfidentsiaalsete andmete (nt ärisaladus, maksusaladus) ning statistiliste andmete vahel. Iga andmeliigi töötlemisele kehtivad erinevad piirangud, mis tulenevad eelkõige IKÜM-ist, AvTS-ist, maksukorralduse seadusest ja muudest eriseadustest.

APA rakendamise seisukohalt tähendab see, et andmete ristkasutus ei saa toimuda ühtse reeglistiku alusel, vaid eeldab diferentseeritud lähenemist, mis arvestab andmete liigi, tundlikkuse ja kasutuseesmärgiga. Selline killustunud regulatsioon on ühtaegu nii APA rakendamise piirang kui ka alus vajadusele luua süsteemsem ja ühtsem andmekäsitlusraamistik.

1.2.7. Millistel õigusaktidel on puutumus nõusolekuteenuse lahendusega? Millised Eesti või euroopa Liidu õigusaktid seavad piirangud nõusolekuteenuse kasutamiseks? Millised Eesti või Euroopa Liidu õigusaktid mis toetavad nõusolekuteenuse kasutamist?

Nõusolekuteenuse õiguslik raamistik ja piirangud APA kontekstis

Nõusolekuteenuse lahendus, mille kaudu ettevõtja saab hallata oma andmete jagamist erinevate asutuste vahel, paikneb mitme õigusvaldkonna ristumiskohas. Selle kasutamist mõjutavad nii Eesti kui ka Euroopa Liidu õigusaktid, mis ühelt poolt seavad nõusolekule ranged tingimused, kuid teiselt poolt loovad ka aluse andmete kontrollitud ja läbipaistvaks jagamiseks.

1. Õigusaktid, mis seavad piirangud nõusolekuteenuse kasutamisele

Nõusolekuteenuse kasutamise peamised piirangud tulenevad eelkõige isikuandmete kaitse regulatsioonist.

- **Isikuandmete kaitse üldmäärus (IKÜM)** sätestab nõusoleku kui ühe võimaliku õigusliku aluse andmete töötlemiseks. IKÜM kohaselt peab nõusolek olema:
    - vabatahtlik,
    - konkreetne,
    - teadlik ja
    - üheselt väljendatud.

Lisaks sätestab IKÜM, et:

- nõusolekut ei tohi kasutada juhul, kui isiku ja avaliku võimu vahel on selge ebavõrdne suhe (nt haldusmenetluses kohustuslike andmete esitamisel);
- nõusolekut peab olema võimalik igal ajal tagasi võtta;
- nõusolek ei saa asendada seadusest tulenevat kohustust.

Seetõttu ei ole nõusolekuteenust võimalik kasutada universaalse alusena andmete jagamiseks, vaid üksnes juhtudel, kus puudub otsene seaduslik kohustus ning andmete jagamine on vabatahtlik.

Täiendavad piirangud tulenevad:

- **Isikuandmete kaitse seadusest (IKS)**, mis täpsustab IKÜM rakendamist Eestis;
- **Avaliku teabe seadusest (AvTS)**, mis seab piirangud juurdepääsupiiranguga teabe (nt ärisaladus, isikuandmed) avalikustamisele ja edastamisele;

- Maksukorralduse seadusest (MKS) ja muudest eriseadustest, mis piiravad konfidentsiaalsete andmete (nt maksusaladus) jagamist isegi nõusoleku olemasolul, kui seadus seda ei luba.

Samuti võib nõusolekuteenuse kasutamist piirata põhiseadusest tulenev põhiõiguste kaitse, eelkõige olukordades, kus nõusolek ei ole sisuliselt vabatahtlik.

2. Õigusaktid, mis toetavad nõusolekuteenuse kasutamist

Samas loob mitme õigusakti koosmõju ka aluse nõusolekupõhiste lahenduste rakendamiseks.

- IKÜM ise tunnustab nõusolekut kui legitiimset andmete töötlemise alust, eeldusel et selle tingimused on täidetud;
- eIDAS määrus toetab turvalist elektroonilist identiteeti ja usaldusteenuseid, mis on eelduseks nõusolekute usaldusväärsele andmisele ja haldamisele digitaalses keskkonnas;
- *Data Governance Act* (DGA) soodustab andmete jagamist ning näeb ette mehhanisme, mis toetavad andmete kasutamist kontrollitud ja usaldusväärsel viisil, sealhulgas andmete jagamise vahendajate ja andmealtruismi kaudu;
- *Data Act* edendab andmete kättesaadavust ja jagamist erinevate osapoolte vahel, luues üldise poliitilise ja õigusliku raamistiku andmete laiemaks kasutamiseks.

Eesti õiguses toetab nõusolekuteenuse arendamist ka:

- riigi infosüsteemi toimimise praktika (nt eesti.ee keskkond ja andmejälgija), mis loob tehnilise aluse nõusolekute haldamiseks;
- Avaliku teabe seaduse arendussuund (sh VTK), mis näeb ette andmete teabevärava ja nõusolekupõhiste lahenduste tugevdamist.

3. Õiguslik tasakaal APA kontekstis

Nõusolekuteenuse kasutamine APA raamistikus eeldab tasakaalu kahe põhimõtte vahel. Ühelt poolt võimaldab nõusolek paindlikku ja kasutajakeskset andmete jagamist olukordades, kus seaduslik alus puudub või oleks ebaproportsionaalne. Teiselt poolt seab kehtiv õigus selged piirid, välistades nõusoleku kasutamise olukordades, kus andmete töötlemine peab tuginema seadusele või kus nõusolek ei ole sisuliselt vabatahtlik.

Seetõttu tuleb nõusolekuteenust käsitada täiendava mehhanismina, mis ei asenda seadusest tulenevaid aluseid, vaid võimaldab laiendada andmete ristkasutust kontrollitud ja läbipaistval viisil. Õiguslikult toimiv nõusolekuteenuse lahendus peab tagama nõusoleku kehtivuse, selle tagasivõetavuse, kasutamise jälgitavuse ning selge seose konkreetse andmekasutuse eesmärgiga.

1.2.8. Nõusolekuteenust saaks kasutada andmete edastamisel, kui andmete omanik (APA puhul ettevõte, kes on andmeid esitanud), on nõus avaliku sektori asutusele esitatud andmete edastamisega kas mõnele teisele riigiasutusele aruandluskohustuse täitmiseks või siis mõnele teisele ettevõttele näiteks oma keskkonnamõjude näitamiseks, paremate laenutingimuste saamiseks või muul ettevõtte huvidest lähtuval viisil kasutamiseks.

Nõusolekuteenuse kasutamise võimalikkus andmete edastamisel

Nõusolekuteenuse kasutamine andmete edastamisel on andmepõhise aruandluse kontekstis võimalik ja põhjendatud eelkõige olukordades, kus andmete jagamiseks puudub otsene seadusest tulenev kohustus või volitus, kuid andmete kasutamine on ettevõtja huvides. Sellisel juhul võib ettevõtja kui

andmete esitaja anda nõusoleku riigile esitatud andmete edastamiseks kas teisele avaliku sektori asutusele või kolmandale isikule, näiteks teisele ettevõttele.

Avaliku sektori asutuste vahelises andmevahetuses saab nõusolekuteenust kasutada eeskätt täiendava õigusliku alusena olukordades, kus andmete teisene kasutus ei ole selgelt reguleeritud, kuid ei ole ka seadusega välistatud. Selline lähenemine võimaldab laiendada *once-only* põhimõtte rakendamist, vähendades ettevõtjate aruandluskoormust, kuid säilitades samal ajal andmete kasutamise kontrollitavust. Samas tuleb arvestada, et nõusolek ei saa asendada seadusest tulenevat kohustust ega olla aluseks andmete jagamisele juhtudel, kus seadus seda otseselt piirab (nt maksusaladus).

Eriti oluline on nõusolekuteenuse roll olukordades, kus andmeid soovitakse kasutada väljaspool avaliku sektori traditsioonilisi ülesandeid, näiteks ettevõtjate vahelises andmevahetuses. Ettevõtja võib anda nõusoleku oma andmete kasutamiseks kolmandate isikute poolt näiteks keskkonnamõjude tõendamiseks, krediidivõime hindamiseks või muude äriliste eesmärkide saavutamiseks. Selline kasutus toetab andmete majanduslikku väärtust ning võimaldab ettevõtjatel oma andmeid aktiivselt kasutada konkurentsieelise saavutamiseks.

Õiguslikult eeldab nõusolekuteenuse kasutamine, et nõusolek vastab kehtivatele nõuetele, eelkõige on see teadlik, vabatahtlik ja konkreetse eesmärgiga seotud. Lisaks peab olema tagatud nõusoleku andmise ja tagasivõtmise võimalus, samuti andmete kasutamise läbipaistvus ja jälgitavus. Tehniliselt eeldab see usaldusväärset nõusolekuteenust, mis võimaldab hallata andmete jagamise õigusi ning kontrollida, millised asutused või isikud andmeid kasutavad.

Kokkuvõttes saab nõusolekuteenust käsitada APA raamistikus paindliku mehhanismina, mis võimaldab laiendada andmete ristkasutust olukordades, kus seaduslik alus puudub või oleks ebaproportsionaalne, tingimusel et on tagatud andmete kasutamise õiguspärasus, läbipaistvus ja kontrollitavus.

1.2.9. Kas ja millistes Eesti ja Euroopa Liidu õigusaktides on määratud see, millise granulaarsusega tohib erinevatesse kategooriatesse kuuluvaid andmeid koguda? Kas ja kui täpselt on granulaarsus määratud?

Andmete granulaarsuse regulatsioon Eesti ja Euroopa Liidu õiguses

Kehtivas Eesti ja Euroopa Liidu õiguses ei ole andmete granulaarsust – st andmete detailiastet või täpsusastet – üldjuhul määratletud ühtse ja süsteemse õigusliku kategooriana. Selle asemel tuleneb andmete lubatav granulaarsus kaudselt erinevatest põhimõtetest ja valdkondlikest regulatsioonidest, mis seavad piirangud andmete kogumise ulatusele ja täpsusele.

1. Üldised põhimõtted EL-i õiguses

Euroopa Liidu tasandil tuleneb andmete granulaarsuse peamine piirang isikuandmete kaitse üldmäärusest, eelkõige:

- andmete minimaalsuse põhimõttest, mille kohaselt tohib koguda üksnes selliseid andmeid, mis on eesmärgi saavutamiseks vajalikud;
- eesmärgipiirangu põhimõttest, mis seob andmete kogumise konkreetse kasutuseesmärgiga.

Need põhimõtted ei määra konkreetset granulaarsuse taset (nt kas koguda üksikute tehingute tasemel või koondandmetena), kuid piiravad kaudselt liigse detaili kogumist, kui see ei ole põhjendatud.

2. Eesti õiguse üldraamistik

Eesti õiguses ei ole samuti kehtestatud üldnormi, mis määraks andmete lubatud granulaarsuse taseme. Granulaarsus kujuneb eelkõige:

- valdkondlike eriseaduste kaudu, mis määravad, milliseid andmeid tuleb esitada (nt maksudeklaratsioonide või statistiliste aruannete detailsus);
- haldusõiguse proportsionaalsuse põhimõtte kaudu, mille kohaselt ei tohi andmete kogumine olla ülemäärane võrreldes eesmärgiga;
- Avaliku teabe seaduse (AvTS) ja andmekogude regulatsiooni kaudu, mis eeldab andmete eesmärgipärast ja põhjendatud kogumist.

Seega ei ole granulaarsus normina ette määratud, vaid tuleneb konkreetse andmekohustuse sisust.

3. Valdkondlikud eriregulatsioonid

Teatud valdkondades on andmete granulaarsus määratud kaudselt või osaliselt täpsemalt:

- Maksuõigus (nt MKS ja maksudeklaratsioonid) – sageli nõutakse detailseid tehingupõhiseid andmeid (nt palgaandmed, käibed), mis viitab kõrgele granulaarsusele;
- Statistikaõigus – võib nõuda nii detail- kui ka koondandmeid, kuid andmete kasutamine on piiratud konfidentsiaalsuse nõuetega;
- Finants- ja kestlikkusaruandlus (nt EL CSRD[19]) – sätestab teatud näitajate esitamise, kuid jätab sageli metoodilise detailsuse standardite tasandile;
- keskkonna- ja energiavaldkond – võib nõuda spetsiifilisi mõõdetavaid näitajaid (nt emissioonid), kuid mitte alati üksiktehingu tasemel.

Seega on granulaarsus nendes valdkondades määratud pigem kaudselt läbi nõutavate andmeväljade ja aruandlusvormide.

4. Andmete vahetus ja ristkasutus

Andmete granulaarsus mõjutab oluliselt ka andmete ristkasutust. Mida detailsemad on andmed (nt üksiktehingu tasemel), seda suuremad on:

- andmekaitse riskid (eriti isikuandmete puhul),
- konfidentsiaalsus- ja ärisaladuse riskid,
- võimalik mõju isikute õigustele.

Kehtiv õigus ei sätesta siiski üldreeglit, millisel granulaarsuse tasemel andmeid võib asutuste vahel jagada, vaid see sõltub:

- andmete liigist (nt kas tegemist on isikuandmetega),
- kasutuseesmärgist,
- olemasolevast õiguslikust alusest.

5. Kokkuvõte

Kokkuvõttes võib järeldada, et Eesti ja Euroopa Liidu õiguses ei ole andmete granulaarsus ühtselt ja otseselt reguleeritud. Selle asemel tuleneb lubatav granulaarsus kaudselt üldpõhimõtetest, eelkõige

[19] 14. detsembri 2022. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2464, millega muudetakse määrust (EL) nr 537/2014, direktiivi 2004/109/EÜ, direktiivi 2006/43/EÜ ja direktiivi 2013/34/EL seoses äriühingute kestlikkusaruandlusega. – ELT L 322, lk 15.

andmete minimaalsuse ja proportsionaalsuse nõuetest, ning valdkondlikest regulatsioonidest, mis määravad konkreetsete andmete esitamise kohustuse.

APA rakendamise seisukohalt tähendab see, et andmete granulaarsus ei ole täna süsteemselt juhitud, vaid kujuneb hajusalt erinevate õigusaktide alusel. See loob vajaduse selgema regulatiivse lähenemise järele, mis seoks andmete detailiastme nende tundlikkuse, kasutuseesmärgi ja riskitasemega ning võimaldaks diferentseeritud ja õiguspärast andmete ristkasutust.

1.2.10. Millistes Eesti ja Euroopa Liidu õigusaktides määratud andmete töötlemisega seotud rollid? Millised rollid on õiguslikes raamistikes välja toodud? Millised on iga rolliga kaasnevad õigused, kohustused, piirangud ja neile kehtivad nõuded?

Andmete töötlemise rollid Eesti ja Euroopa Liidu õigusraamistikus

Andmete töötlemisega seotud rollid on Eesti ja Euroopa Liidu õiguses määratletud eelkõige andmekaitseõiguse, avaliku teabe regulatsiooni ning valdkondlike eriseaduste kaudu. Kuigi erinevad õigusaktid kasutavad mõnevõrra erinevat terminoloogiat, on nende keskmes sarnased funktsionaalsed rollid, mis määravad, kes vastutab andmete kogumise, töötlemise, jagamise ja kasutamise eest.

1. Vastutav töötleja ja volitatud töötleja (IKÜM ja IKS)

Kõige kesksemad rollid on sätestatud isikuandmete kaitse üldmääruses ning täpsustatud isikuandmete kaitse seaduses:

- Vastutav töötleja – isik või asutus, kes määrab andmete töötlemise eesmärgid ja vahendid.
    - Õigused ja pädevus otsustada, milliseid andmeid kogutakse ja kuidas neid kasutatakse; määrata töötlemise õiguslik alus.
    - Kohustus tagada töötlemise õiguspärasus, läbipaistvus, turvalisus ja vastavus IKÜM nõuetele; viia vajadusel läbi mõjuhindamine; tagada andmesubjekti õiguste kaitse.
    - Piirangud on seotud eesmärgipiirangu, minimaalsuse ja proportsionaalsuse põhimõtetega; ei tohi töödelda andmeid ilma õigusliku aluseta.
- Volitatud töötleja – isik või asutus, kes töötleb andmeid vastutava töötleja nimel.
    - Õigused töödelda andmeid üksnes vastutava töötleja juhiste alusel.
    - Kohustused tagada andmete turvalisus, konfidentsiaalsus ning järgida lepingulisi ja seadusest tulenevaid nõudeid.
    - Piirangud, mille kohaselt ei tohi kasutada andmeid oma eesmärkidel ega edastada neid ilma loata.

Lisaks näeb IKÜM ette ka kaasvastutavate töötlejate (*joint controllers*) rolli, kus mitu osapoolt määravad ühiselt töötlemise eesmärgid ja vahendid, jagades vastutust.

2. Andmekogu vastutav ja volitatud töötleja (AvTS)

Eesti õiguses sätestab avaliku teabe seadus andmekogude kontekstis sarnased rollid:

- Andmekogu vastutav töötleja – asutus, kes vastutab andmekogu pidamise, andmete õigsuse ja töötlemise õiguspärasuse eest.
- Andmekogu volitatud töötleja – tehniline või halduslik teostaja, kes töötleb andmeid vastutava töötleja ülesandel.

Nende rollidega kaasnevad:

- kohustus tagada andmete kvaliteet, turvalisus ja ajakohasus;
- kohustus järgida juurdepääsupiiranguid ja andmete avalikustamise reegleid;
- vastutus andmekogu toimimise eest tervikuna.

3. Andmete esitaja ja andmesubjekt

APA kontekstis on oluline eristada ka:

- **Andmete esitaja (nt ettevõtja)** – isik, kes esitab andmed riigile õigusliku kohustuse või vabatahtliku otsuse alusel.
    - **Õigused:** saada teavet andmete kasutamise kohta; teatud juhtudel kontrollida andmete jagamist (nt nõusoleku kaudu).
    - **Kohustused:** esitada õiged ja täielikud andmed seaduses sätestatud korras.
- **Andmesubjekt** – füüsiline isik, kelle kohta andmed käivad (IKÜM mõistes).
    - **Õigused:** juurdepääs andmetele, parandamine, kustutamine, töötlemise piiramine jms.
    - **Piirangud:** õigusi võib piirata avaliku huvi või seadusest tulenevate kohustuste tõttu (nt maksukohustused).

4. Andmete kasutaja ja vastuvõttev asutus

Andmete ristkasutuse kontekstis tekib eraldi roll:

- **Andmete kasutaja (vastuvõttev asutus)** – asutus, kes saab andmed teisest andmekogust.
    - **Õigused:** kasutada andmeid üksnes seaduses sätestatud eesmärgil ja ulatuses.
    - **Kohustused:** kontrollida õiguslikku alust, tagada andmete turvalisus ja mitte ületada kasutuspiire.
    - **Piirangud:** ei tohi kasutada andmeid uuel eesmärgil ilma õigusliku aluseta (eesmärgipiirang).

5. Euroopa Liidu andmemajanduse regulatsiooni rollid

Uuemates EL õigusaktides lisanduvad täiendavad rollid:

- **Andmete vahendaja (*data intermediary*)** – *Data Governance Act*'i kohaselt neutraalne osapool, kes vahendab andmete jagamist;
- **Andmevaldaja (*data holder*)** – *Data Act*'i mõistes isik või asutus, kelle valduses andmed on;
- **Andmekasutaja (*data user*)** – isik, kes kasutab andmeid kokkulepitud tingimustel.

Nende rollide eesmärk on toetada andmete jagamist, kuid samal ajal tagada usaldusväärsus, läbipaistvus ja turvalisus.

6. Kokkuvõte

Kokkuvõttes on andmete töötlemise rollid Eesti ja Euroopa Liidu õiguses mitmetasandilised ning tulenevad erinevatest õigusaktidest. Keskne eristus tehakse vastutava ja volitatud töötleja vahel, kuid APA kontekstis on vajalik arvestada ka andmete esitaja, kasutaja ning andmete vahendamisega seotud rollidega. Iga rolliga kaasnevad konkreetsed õigused, kohustused ja piirangud, mis on suunatud eelkõige andmete õiguspärasele kasutamisele, turvalisuse tagamisele ning põhiõiguste kaitsele. Selline rollijaotus

on eelduseks toimivale ja usaldusväärsele andmepõhisele aruandlusele, kuid eeldab selget ja ühtset regulatiivset käsitlust, eriti andmete ristkasutuse ja kesksete andmejagamise mehhanismide kontekstis.

1.2.11. Millistes Eesti ja Euroopa Liidu õigusaktides määratud andmete töötlemisega seotud täpsemad toimingud? Millised andmete töötlemisega täpsemad toimingud on õiguslikes raamistikes välja toodud? Millised on iga tegevusega kaasnevad õigused, kohustused, piirangud ja nõuded asutustele, mis neid tegevusi teevad?

Andmete töötlemise toimingud ning nendega seotud õigused, kohustused ja piirangud

Eesti ja Euroopa Liidu õigusraamistikus on andmete töötlemisega seotud toimingud määratletud eelkõige üldiste kategooriatena, mitte detailsete tehniliste protsessidena. Kõige kesksem loetelu tuleneb isikuandmete kaitse üldmäärusest, mille kohaselt hõlmab andmete töötlemine igasuguseid toiminguid andmetega, sealhulgas kogumine, salvestamine, korrastamine, säilitamine, muutmine, päringute tegemine, kasutamine, edastamine, avalikustamine, piiramine ja kustutamine. Eesti õiguses (nt avaliku teabe seadus, valdkondlikud eriseadused) käsitletakse neid toiminguid sarnaste funktsionaalsete etappidena, kuigi terminoloogia võib erineda.

1. Andmete kogumine ja esitamine

Andmete kogumine ettevõtjalt või muult isikult on reguleeritud eelkõige valdkondlikes eriseadustes (nt maksukorralduse seadus, statistika seadus, keskkonnaõigust reguleerivad seadused).

- Õigused: asutusel on õigus nõuda andmeid seaduses sätestatud ulatuses;
- Kohustused: andmete kogumine peab olema eesmärgipärane ja proportsionaalne;
- Piirangud: ei tohi koguda rohkem andmeid, kui on vajalik; tuleb arvestada minimaalsuse põhimõtet;
- Nõuded: peab eksisteerima selge õiguslik alus.

APA kontekstis on oluline ka kohustus vältida dubleerivat kogumist (*once-only* põhimõte), kuigi see ei ole kehtivas õiguses ühtselt sätestatud.

2. Andmete salvestamine ja säilitamine

Andmete säilitamist reguleerivad nii üldnormid (nt IKÜM) kui ka eriseadused (nt arhiveerimise ja raamatupidamise nõuded).

- Õigused: asutus võib säilitada andmeid nii kaua, kui see on vajalik eesmärgi täitmiseks;
- Kohustused: määrata säilitamistähtaeg ja tagada andmete turvalisus;
- Piirangud: säilitamine ei tohi olla tähtajatu ilma põhjenduseta;
- Nõuded: andmete terviklus, konfidentsiaalsus ja kättesaadavus peavad olema tagatud.

3. Andmete kasutamine ja analüüs

Andmete kasutamine hõlmab nii haldusotsuste tegemist kui ka analüütilist töötlemist.

- Õigused: kasutada andmeid seaduses sätestatud eesmärgil;
- Kohustused: järgida eesmärgipiirangu põhimõtet;
- Piirangud: ei tohi kasutada andmeid uuel eesmärgil ilma õigusliku aluseta;
- Nõuded: andmete õigsus ja ajakohasus peavad olema tagatud.

Tuletatud andmete (nt analüüsid, riskihinnangud) puhul võivad tekkida täiendavad nõuded, eriti kui need mõjutavad isikute õigusi.

4. Andmete edastamine ja jagamine

Andmete edastamine asutuste vahel või kolmandatele isikutele on üks rangemalt reguleeritud toiminguid.

- **Õigused:** edastamine on lubatud üksnes õigusliku aluse olemasolul (seadus, nõusolek vms);
- **Kohustused:** kontrollida vastuvõtja õigust andmeid kasutada;
- **Piirangud:** konfidentsiaalsusrežiimid (nt maksusaladus, ärisaladus) võivad edastamist piirata;
- **Nõuded:** tagada andmete turvaline edastamine ning kasutamise jälgitavus (logimine).

APA kontekstis on see keskne toiming, mille puhul on vajalik selge regulatsioon ristkasutuse lubatavuse kohta.

5. Andmete avalikustamine

Avalikustamist reguleerib eelkõige avaliku teabe seadus ning EL avaandmete regulatsioon.

- **Õigused:** avalikustada avalikku teavet;
- **Kohustused:** kontrollida, kas andmetele kehtib juurdepääsupiirang;
- **Piirangud:** isikuandmeid, ärisaladust ja muud piiratud teavet ei tohi avalikustada;
- **Nõuded:** avaandmete puhul tagada masinloetavus ja korduvkasutatavus.

6. Andmete muutmine ja parandamine

Andmete ajakohastamine ja parandamine on vajalik andmete kvaliteedi tagamiseks.

- **Õigused:** parandada ebaõigeid andmeid;
- **Kohustused:** tagada andmete õigsus ja ajakohasus;
- **Piirangud:** muudatused peavad olema jälgitavad;
- **Nõuded:** säilitada andmete muutmise ajalugu teatud juhtudel.

7. Andmete kustutamine ja piiramine

Andmete kustutamine või töötlemise piiramine tuleneb eelkõige IKÜM-ist.

- **Õigused:** kustutada andmed, kui töötlemise alus langeb ära;
- **Kohustused:** järgida säilitamistähtaegu ja kustutada andmed nende möödumisel;
- **Piirangud:** andmeid ei tohi kustutada, kui nende säilitamine on seadusest tulenevalt kohustuslik;
- **Nõuded:** kustutamine peab olema turvaline ja pöördumatu.

Kokkuvõte

Kokkuvõttes on andmete töötlemise toimingud Eesti ja Euroopa Liidu õiguses määratletud üldiste kategooriatena, millele rakenduvad erinevad õigused, kohustused ja piirangud sõltuvalt andmete liigist ja kasutuseesmärgist. Kõige rangemad nõuded kehtivad andmete kogumisele ja edastamisele, samas kui säilitamine, kasutamine ja kustutamine on reguleeritud eelkõige põhimõtete tasandil. APA rakendamise seisukohalt on oluline, et need toimingud oleksid selgelt eristatavad ning iga toimingu

puhul oleks määratud selle õiguslik alus, lubatavus ja riskitase, võimaldades seeläbi andmete õiguspärast ja efektiivset ristkasutust.

1.2.12. Õigusanalüüsi lõpparuanne peab võimaldama hinnata erinevatele ettevõtjalt riigile esitatavate andmete tundlikust ning töötada välja lahendused, mis võimaldaksid erinevat tüüpi andmete puhul kasutada *once-only* põhimõtet või muid lahendusi, mis vähendavad ettevõtja halduskoormust. Õigusanalüüsi lõpparuandes peavad olema välja toodud kogutavate ettevõtlusega seotud andmete edasise töötlemise ja jagamise õiguslikud piiranguid avaliku sektori jaoks. Samuti peavad olema välja toodud võimalikud lahendused, mis aitaksid APA-t rakendada. Selleks tuleb luua metoodika, mis peab vastama allolevatele küsimustele või nõuetele.

Metoodiline raamistik andmete tundlikkuse hindamiseks ja *once-only* rakendamiseks

Käesoleva õigusanalüüsi eesmärk on luua süsteemne metoodika, mis võimaldab hinnata ettevõtjalt riigile esitatavate andmete tundlikkust ning siduda see sobiva andmekasutuse ja -jagamise mudeliga. Analüüs lähtub eeldusest, et andmete töötlemise lubatavus ja ulatus ei saa olla ühtne, vaid peab sõltuma andmete liigist, granulaarsusest ning nendega seotud õiguslikest riskidest.

Selleks on analüüsis välja töötatud kolmetasandiline lähenemine, mis ühendab (i) andmetüüpide kaardistuse, (ii) tundlikkuse hindamise ning (iii) õigusliku riskihindamise maatriksi. Nimetatud metoodika võimaldab määrata, millistel juhtudel on võimalik rakendada *once-only* põhimõtet täiel määral, millal on vajalikud täiendavad tingimused (nt nõusolek, piiratud ligipääs, agregeerimine) ning millistel juhtudel ei ole andmete ristkasutus õiguspärane.

Analüüsi tulemusena tuuakse välja ka kehtivast õigusest tulenevad piirangud andmete edasisele töötlemisele ja jagamisele, eelkõige seoses isikuandmete kaitse, ärisaladuse, maksusaladuse ning eesmärgipiirangu põhimõttega. Samas pakutakse normitehnilisi ja korralduslikke lahendusi, mis võimaldavad neid piiranguid arvestades APA visiooni ellu viia, sealhulgas andmete tundlikkusel põhinev diferentseerimine, keskse andmejagamise mehhanismi loomine ning nõusolekupõhiste lahenduste kasutamine.

Selline metoodiline raamistik võimaldab siduda andmete kogumise, töötlemise ja jagamise ühtseks tervikuks, toetades nii õiguspärast andmekasutust kui ka ettevõtjate halduskoormuse vähendamist.

1.2.13. Õigusanalüüsi tulemusel peab olema võimalik kategoriseerida riigi poolt kogutavate ettevõtlusega seotud andmeid lähtuvalt sellest, millised on nende andmete töötlemisega seotud piirangud? Piirangud võivad lähtuda andmete kasutusotstarbest (nt statistika, järelevalve, maksustamine, avaandmed) ja/või tundlikkuseest (nt ärisaladus, isikuandmed, terviseandmed) või teistest õiguslikest aspektidest.

Andmete kategoriseerimine töötlemispiirangute alusel

Käesoleva õigusanalüüsi tulemusel on võimalik riigi poolt kogutavad ettevõtlusega seotud andmed süstematiseeritult kategoriseerida lähtuvalt nende töötlemisele kohalduvatest õiguslikest piirangutest. Analüüs näitab, et andmete töötlemise lubatavus ei sõltu üksnes andmete liigist, vaid kujuneb mitme teguri koosmõjus, eelkõige andmete kasutuseesmärgist, tundlikkusest ning õiguslikust kontekstist.

Metoodiliselt jaotatakse andmed kolme peamise kriteeriumi alusel: (i) kasutusotstarve (nt maksustamine, järelevalve, statistika, avalikustamine), (ii) andmete tundlikkus (nt isikuandmed, ärisaladus, avalik teave) ning (iii) töötlemisega seotud õiguslikud piirangud (nt eesmärgipiirang, konfidentsiaalsusnõuded, säilitamiskohustused). Nende kriteeriumide kombineerimine võimaldab määrata iga andmekategooria puhul, millised töötlemistoimingud on lubatud, millised piiratud ning millised välistatud.

Selline kategoriseerimine loob aluse diferentseeritud andmekasutuse mudelile, kus *once-only* põhimõtet rakendatakse vastavalt andmete riskitasemele. Madala tundlikkusega ja selge eesmärgiga andmete puhul on võimalik laiem ristkasutus ja automatiseeritud jagamine, samas kui kõrgema tundlikkusega andmete puhul tuleb rakendada täiendavaid piiranguid, nagu nõusolekupõhine jagamine, agregeerimine või kasutuse kitsendamine konkreetsele eesmärgile.

Kokkuvõttes võimaldab selline lähenemine siduda andmete liigituse, õiguslikud piirangud ja kasutusvõimalused ühtseks raamistikuks, mis toetab nii õiguspärast andmetöötlust kui ka ettevõtjate halduskoormuse vähendamist.

1.2.14. Luua metoodika riigi poolt kogutavate andmete omaniku määramiseks. Näiteks palgaandmete puhul on küsimus, kas andmete omanik on andmeid esitav ettevõte või isik, kelle kohta palgaandmeid esitatakse.

Käesoleva õigusanalüüsi raames on välja töötatud metoodika riigi poolt kogutavate andmete „omaniku" määramiseks, lähtudes funktsionaalsest lähenemisest, mille kohaselt ei ole andmetel ühtset omanikku klassikalises õiguslikus tähenduses. Selle asemel jaotub kontroll andmete üle erinevate subjektide vahel, eelkõige andmesubjekti, andmete esitaja ja vastutava töötleja vahel, sõltuvalt andmete liigist ja kasutuseesmärgist. Metoodika võimaldab määratleda, millisel subjektil on konkreetse andmekasutuse kontekstis otsustusõigus ja vastutus, mis on eelduseks nii *once-only* põhimõtte õiguspärasele rakendamisele kui ka nõusolekupõhiste lahenduste kasutamisele. Näiteks palgaandmete puhul jaguneb kontroll töötaja (andmesubjekt), tööandja (andmete esitaja) ja riigi (vastutav töötleja) vahel, mistõttu ei ole võimalik käsitada ühtki neist ainuomanikuna.

1.2.15. Millised on peamised piirangud erinevatesse eelpool kirjeldatud kategooriatesse kuuluvate andmete töötlemisel (vastuvõtmine, salvestamine, edastamine, jagamine, kustutamine, analüüs, andmetele juurdepääsu andmine jm)?

Käesoleva õigusanalüüsi põhjal kujunevad ettevõtlusega seotud andmete töötlemise peamised piirangud eelkõige andmete liigist, tundlikkusest ning konkreetsest töötlemistoimingust. Andmete kogumisel kehtivad õigusliku aluse, minimaalsuse ja proportsionaalsuse nõuded, mis välistavad põhjendamatu või dubleeriva andmete küsimise. Andmete säilitamisel ja töötlemisel tuleb järgida säilitamistähtaegu, andmete turvalisuse ja tervikluse tagamise kohustust ning eesmärgipiirangu põhimõtet, mille kohaselt ei tohi andmeid kasutada algsest eesmärgist erineval viisil ilma täiendava õigusliku aluseta.

Kõige rangemad piirangud kehtivad andmete edastamisele ja jagamisele, mis eeldavad selget õiguslikku alust ning arvestamist konfidentsiaalsusrežiimidega (nt isikuandmed, ärisaladus, maksusaladus), samuti ligipääsukontrolli ja kasutuse jälgitavust. Andmete analüüsimisel tuleb hinnata mõju isikute ja ettevõtjate õigustele, eriti automatiseeritud otsuste puhul. Andmete avalikustamine ja juurdepääsu võimaldamine on lubatud üksnes ulatuses, mis ei riku juurdepääsupiiranguid. Andmete kustutamisel tuleb tasakaalustada kustutamiskohustus ja seadusest tulenevad säilitamisnõuded. Kokkuvõttes eeldab andmete õiguspärane töötlemine toimingupõhist lähenemist, kus iga etapi puhul hinnatakse eraldi õiguslikku alust, eesmärki ja riskitaset.

1.2.16. Luua kehtivast õigusraamistikust lähtuv metoodika erinevatesse ülal kirjeldatud kategooriatesse kuuluvate andmete jagamiseks riigiasutuste vahel ka siis, kui tänane õigusraamistik seda piirab (nt nõusoleku alusel või anonümiseerimise kaudu).

Metoodika andmete jagamiseks piiratud õigusraamistikus

Käesoleva õigusanalüüsi tulemusel on võimalik kujundada metoodika, mis võimaldab hinnata andmete jagamise lubatavust riigiasutuste vahel ka olukordades, kus kehtiv õigusraamistik seab sellele piiranguid. Metoodika lähtub andmete tundlikkusest, kasutuseesmärgist ning olemasolevast õiguslikust alusest ning võimaldab valida sobiva mehhanismi andmete õiguspäraseks jagamiseks.

Metoodika kohaselt toimub andmete jagamise lubatavuse hindamine astmeliselt. Esmalt tuleb kontrollida, kas andmete jagamiseks eksisteerib otsene seadusest tulenev õiguslik alus. Sellisel juhul on andmete jagamine lubatud seaduses sätestatud ulatuses. Kui otsene alus puudub, tuleb hinnata, kas andmeid on võimalik kasutada kujul, mis ei võimalda isikute või ettevõtjate tuvastamist, näiteks anonümiseeritud või agregeeritud andmetena. Sellisel juhul võib andmete jagamine olla lubatav piiratud kujul, eelkõige statistilistel või analüütilistel eesmärkidel.

Kui anonümiseerimine ei ole võimalik või ei vasta kasutuseesmärgile, tuleb hinnata nõusolekupõhise jagamise võimalikkust. Nõusolekut saab kasutada üksnes juhul, kui see vastab õiguslikele nõuetele (teadlik, vabatahtlik ja konkreetne) ning kui seadus ei välista sellist andmete jagamist. Kui ükski eeltoodud alustest ei ole kohaldatav, tuleb järeldada, et andmete jagamine ei ole lubatav.

Selline astmeline lähenemine võimaldab siduda kehtivad õiguslikud piirangud praktiliste lahendustega ning loob selge otsustusloogika, mille alusel hinnata andmete ristkasutuse võimalikkust APA kontekstis.

1.2.17. Luua metoodika hindamaks, milliste ülal kirjeldatud kategooriate puhul on õiguslikult põhjendatud, et riik ei tohi vastu võtta algandmeid, vaid üksnes agregeeritud või tuletatud näitajaid?

Andmete granulaarsuse hindamiseks on analüüsi käigus välja töötatud metoodika, mille kohaselt tuleb igal andmekategoorial hinnata, kas algandmete kogumine on õiguspärane või tuleb piirduda agregeeritud või tuletatud näitajatega. Metoodika lähtub eelkõige andmete tundlikkusest, töötlemise eesmärgist ning proportsionaalsuse põhimõttest.

Algandmete kogumine ei ole õiguslikult põhjendatud eelkõige juhtudel, kus andmed on kõrge tundlikkusega (nt sisaldavad isikuandmeid või ärisaladust), kuid töötlemise eesmärk on saavutatav koondandmete või tuletatud näitajate abil, näiteks statistilisel või analüütilisel eesmärgil. Samuti tuleb algandmete kogumisest hoiduda olukordades, kus nende kogumine suurendab ebaproportsionaalselt õigusriske, sh konfidentsiaalsuse rikkumise või eesmärgipiirangu ületamise riski.

Seetõttu tuleb andmete kogumise taseme määramisel rakendada diferentseeritud lähenemist, mille kohaselt kogutakse üksnes sellisel granulaarsusel andmeid, mis on konkreetse eesmärgi saavutamiseks vajalikud ja piisavad. See võimaldab ühtaegu vähendada ettevõtjate halduskoormust ning tagada andmete töötlemise kooskõla andmekaitse ja proportsionaalsuse põhimõtetega.

1.2.18. Luua õiguslik metoodika hindamaks, millised ülal kirjeldatud andmekategooriad on sobivad *once-only* printsiibi rakendamiseks (andmete esitamine vaid üks kord), ja millised ainult "ühekordse sisestamise" printsiibi alusel (andmed sisestatakse tarkvarasse ühe korra kuid edastatakse riigiasutustele erinevate andmesektsioonidena).

Andmepõhise aruandluse kontekstis tuleb eristada *once-only* põhimõtte rakendamist ning ühekordse sisestamise (*single entry*) lahendust, kuna nende õiguslikud eeldused ja kohaldamisala on erinevad. Käesoleva analüüsi alusel on välja töötatud metoodika, mille kohaselt sõltub sobiva lähenemise valik eelkõige andmete tundlikkusest, struktureeritusest ning kasutuseesmärgist.

Once-only põhimõte on õiguslikult põhjendatud eeskätt standardiseeritud ja selge semantilise tähendusega andmete puhul, mille korduvkasutus erinevate asutuste vahel on vajalik ning mille töötlemiseks on olemas piisav õiguslik alus. Sellised on näiteks identifikaatorid, klassifikaatorid ning

teatud juhtudel ka struktureeritud tehinguandmed, mille puhul on võimalik tagada eesmärgipiirangu järgimine ja asjakohased turvameetmed.

Ühekordse sisestamise (*single entry*) põhimõte on seevastu sobiv juhtudel, kus andmete ristkasutus on õiguslikult piiratud või tehniliselt keerukas, eelkõige kõrge tundlikkusega või struktureerimata andmete puhul. Sellisel juhul vähendatakse ettevõtja halduskoormust andmete ühekordse sisestamise kaudu, kuid andmete edasine kasutamine toimub eraldiseisvate edastustena ning ei eelda riigisisest automaatset ristkasutust.

Seega võimaldab metoodika rakendada diferentseeritud lähenemist, mille kohaselt kasutatakse *once-only* põhimõtet seal, kus see on õiguslikult ja tehniliselt põhjendatud, ning ühekordse sisestamise lahendust juhtudel, kus ristkasutus ei ole lubatav või otstarbekas.

1.2.19. Luua metoodika, mille alusel määrata primaarse andmekoguja (kes andmed vastu võtab) ja sekundaarse kasutaja (kellega andmeid jagatakse) õigused ja kohustused *once-only* põhimõtte rakendamisel.

Andmepõhise aruandluse raames on välja töötatud metoodika, mille alusel eristatakse primaarset andmekogujat ja sekundaarset kasutajat ning määratletakse nende õigused ja kohustused *once-only* põhimõtte rakendamisel. Metoodika lähtub põhimõttest, et andmete esmakogumine ja nende teisene kasutamine on õiguslikult eristatavad toimingud, millele kohalduvad erinevad nõuded.

Primaarne andmekoguja vastutab andmete esmakogumise õiguspärasuse, kvaliteedi ja piisava kirjeldatuse eest, sealhulgas andmete õigusliku aluse, eesmärgi ja tundlikkuse määratlemise eest. Sekundaarne kasutaja vastutab seevastu andmete teisese kasutamise õiguspärasuse eest, eelkõige eesmärgipiirangu järgimise, õigusliku aluse olemasolu ning andmete kasutamise proportsionaalsuse hindamise eest.

Metoodika kohaselt tuleb rollide jaotus siduda andmete tundlikkuse, kasutuseesmärgi ja töötlemise riskiga, tagades ühtlasi andmete kasutamise läbipaistvus ja jälgitavus. Selline lähenemine võimaldab rakendada *once-only* põhimõtet viisil, mis väldib andmete dubleerivat kogumist, kuid säilitab selge vastutuse jaotuse ning kooskõla andmekaitse ja põhiõiguste kaitse nõuetega.

1.2.20. Luua metoodika, mille alusel erinevatesse kategooriatesse kuuluvate andmete puhul primaarse andmekoguja ja sekundaarse andmete kasutaja õigused, kohustused, nõuded ja nendele kehtestatud piirangud.

Andmepõhise aruandluse rakendamiseks on välja töötatud andmekategooriapõhine metoodika, mille alusel määratakse primaarse andmekoguja ja sekundaarse kasutaja õigused, kohustused ning neile kohalduvad piirangud. Metoodika lähtub põhimõttest, et andmete töötlemise tingimused ei ole universaalsed, vaid sõltuvad andmete liigist, tundlikkusest ja kasutuseesmärgist.

Madala tundlikkusega andmete (nt klassifikaatorid ja metaandmed või muud andmeid kirjeldavad andmed) puhul on õigused laiemad ning piirangud minimaalsed, võimaldades ulatuslikku ristkasutust. Kõrge tundlikkusega andmete (nt isikuandmed, maksusaladus ja ärisaladus) puhul on õigused seevastu rangelt piiratud ning sekundaarne kasutus eeldab selget õiguslikku alust, eesmärgipiirangu järgimist ning täiendavaid turvameetmeid. Tehinguandmete või algandmete puhul rakendub tingimuslik lähenemine, samas kui tuletatud ja koondandmete puhul on võimalik laiem kasutus, arvestades nende mõju õigustele ja kohustustele.

Metoodika kohaselt vastutab primaarne andmekoguja andmete kogumise õiguspärasuse, kvaliteedi, klassifitseerimise ja piisava kirjeldatuse eest, sealhulgas andmete õigusliku aluse, eesmärgi ja tundlikkuse määratlemise eest, samas kui sekundaarne kasutaja vastutab andmete kasutamise

õiguspärasuse, proportsionaalsuse ja eesmärgipiirangu järgimise eest. Selline diferentseeritud lähenemine võimaldab rakendada *once-only* põhimõtet viisil, mis toetab andmete tõhusat kasutamist, kuid tagab samal ajal põhiõiguste kaitse ja õiguskindluse.

1.2.21. Luua metoodika hindamaks, millistel tingimustel ja milliste andmekategooriate puhul võib üks asutus keelduda andmete jagamisest teise asutusega? Sama metoodika alusel peab saama hinnata, millal on andmete jagamine kohustuslik.

Käesoleva analüüsi raames on välja töötatud metoodika, mille alusel hinnata andmete jagamise kohustuslikkust, lubatavust või keelatust avaliku sektori asutuste vahel. Metoodika lähtub andmete kategooriast, tundlikkusest, kasutuseesmärgist ning õigusliku aluse olemasolust.

Andmete jagamine on kohustuslik eelkõige juhtudel, kus teisel asutusel on selge seadusest tulenev õiguslik alus ning andmete kasutamine on vajalik avaliku ülesande täitmiseks ja kooskõlas algse kogumise eesmärgiga. Tingimuslik jagamine rakendub juhtudel, kus andmed on kõrgema tundlikkusega ning nende kasutamine eeldab täiendavat proportsionaalsuse, minimaalsuse ja eesmärgipiirangu hindamist või täiendavaid kaitsemeetmeid (nt agregeerimine või ligipääsupiirangud).

Andmete jagamisest tuleb keelduda olukordades, kus puudub õiguslik alus, andmete kasutamine ei ole kooskõlas eesmärgipiirangu põhimõttega või jagamine tooks kaasa ebaproportsionaalse riive isikute või ettevõtjate õigustele, sealhulgas konfidentsiaalse teabe põhjendamatu avaldamise.

Selline diferentseeritud metoodika võimaldab tagada, et *once-only* põhimõtet rakendatakse õiguspäraselt ja sihipäraselt, vältides nii põhjendamatut andmete dubleerimist kui ka õigusvastast andmete jagamist.

1.2.22. Luua metoodika, millest lähtudes luua andmete töötlemisega seotud toimingute (vastuvõtmine, salvestamine, edastamine, jagamine, kustutamine, analüüs, andmetele juurdepääsu andmine jms), metaandmed.

Käesoleva analüüsi raames on välja töötatud töötlemistoimingupõhine metaandmete metoodika, mille eesmärk on siduda andmete elutsükli erinevad etapid selgete õiguslike ja tehniliste kirjeldustega. Metoodika lähtub põhimõttest, et iga andmete töötlemise toiming (nt kogumine, salvestamine, edastamine, kasutamine, kustutamine) peab olema varustatud metaandmetega, mis võimaldavad hinnata selle toimingu õiguspärasust, eesmärki ja ulatust.

Metaandmed peavad hõlmama eelkõige toimingu õiguslikku alust, töötlemise eesmärki, andmete tundlikkust, kasutamise ulatust, ligipääsupiiranguid ning säilitamistingimusi. Selline lähenemine võimaldab tagada andmete kasutamise läbipaistvuse, jälgitavuse ja kontrollitavuse kogu andmete elutsükli vältel.

Metoodika rakendamine loob eelduse andmete automatiseeritud ja turvaliseks ristkasutuseks, toetab *once-only* põhimõtte rakendamist ning aitab tagada, et andmete töötlemine toimub kooskõlas andmekaitse, eesmärgipiirangu ja proportsionaalsuse põhimõtetega.

1.2.23. Luua metoodika, millest lähtudes avaldada andmete töötlemisega seotud toimingute (vastuvõtmine, salvestamine, edastamine, jagamine, kustutamine, analüüs, andmetele juurdepääsu andmine jms), metaandmeid.

Käesoleva analüüsi raames on välja töötatud metoodika, mille alusel avaldada andmete töötlemisega seotud toimingute metaandmeid viisil, mis tagab nii andmete läbipaistvuse kui ka konfidentsiaalsuse kaitse. Metoodika lähtub põhimõttest, et metaandmeid tuleb avaldada ulatuses, mis võimaldab

tuvastada andmete olemasolu, nende tähendust, kasutuseesmärki ja kasutustingimusi, ilma et avaldataks piiratud juurdepääsuga andmeid endid.

Metaandmete avaldamine toimub kihiliselt, eristades avalikku, piiratud juurdepääsuga ja sisemist tasandit. Avalikus kihis avaldatakse üldised andmekirjeldused ja kasutuseesmärgid, samas kui detailsemad ligipääsu- ja kasutustingimused on kättesaadavad üksnes õigustatud asutustele. Selline lähenemine võimaldab tagada andmete leitavuse ja ristkasutuse võimalikkuse, säilitades samal ajal andmekaitse, ärisaladuse ja muude konfidentsiaalsusnõuete järgimise.

Metoodika toetab andmete automatiseeritud kasutamist ja *once-only* põhimõtte rakendamist, võimaldades asutustel tuvastada olemasolevaid andmeid ja hinnata nende kasutamise õiguspärasust enne ligipääsu taotlemist. Lisaks loob see aluse andmete kasutamise jälgitavusele ja auditeeritavusele, mis on vajalik avaliku sektori andmehalduse usaldusväärsuse tagamiseks.

1.2.24. Luua õiguslik metoodika, mille rakendamisel üks asutus tohib teisele asutusele anda õigus enda eest lisaandmevälju koguda, kui andmeid koguval või vastu võtval asutusel ei ole õiguslikku alust nende andmete töötlemiseks? Kui tänane õiguslik raamistik seda ei võimalda, tuleb välja tuua õiguslikud muudatused, mille sisse viimisel saaks üks asutus teisele asutusele taolise õiguse anda. Tuua välja, milliste eelpool mainitud andmekategooriate puhul on võimalik taolist lahendust kasutada? Tuua välja, milliste eelpool mainitud andmekategooriate puhul ei ole võimalik taolist lahendust kasutada ja miks.

Küsimusele 1.2.24 vastab käesolev analüüs eelkõige peatükis 4.6. „Teise asutuse eest andmete kogumise metoodika“ (sh andmekategooriapõhine eristus lubatavate ja mittelubatavate lahenduste kohta) ning normitehniliste ettepanekutena peatükkides 7.2 ja 7.3, kus on välja toodud vajalikud volitusnormid ja teisese kasutuse raamistik.

1.2.25. Kas ja milliseid õigusakte ning mis ulatuses on vaja APA visiooni realiseerimiseks muuta, täiendada või luua, arvestades õigusaktidest tulevaid nõudeid nimetatud visiooni ning võimalikku õigusaktide muutmise vajadust, skoopi ja sisu lahenduse kasutuselevõtuks.

<u>Õigusaktide muutmise vajadus APA realiseerimiseks</u>

APA kontseptsioon eeldab:

1. andmete esitamise ühekordsust (*once-only*);
2. andmete struktureeritust ja masinloetavust;
3. asutustevahelist ristkasutust;
4. keskset andmejagamise infrastruktuuri;
5. nõusolekupõhise jagamise võimalust;
6. andmete tundlikkuse diferentseeritud käsitlust.

Kehtiv õigusraamistik ei ole nende põhimõtetega täielikult kooskõlas, kuna regulatsioon on killustatud ning ei käsitle süsteemselt teisest kasutust, väärindatud andmete jagamist ega keskset andmeväravat. Samuti on kehtivast õigusest puudu põhimõtted, mis reguleeriks olukorrad, kus andmete jagamine on lubamatu.

2. Õigusaktide muutmise vajadus – üldine hinnang

APA visiooni realiseerimiseks on vajalik:

I. Horisontaalne raamistik (keskne regulatsioon)

Eeskätt avaliku teabe seaduse (AvTS) muutmine.

II. Valdkondlikud seadused

Üle kontrollida ja vajadusel täiendada valdkondlike õigusakte, eelkõige maksundus, statistika, keskkond, tööõigus, riiklikud toetused jms.

III. Rakendusaktid ja tehnilised standardid

Lisaks seadustele tuleb üle kontrollida, vajadusel täiendada või kehtestada rakendusaktid (määrused) ja tehnilised standardid (nt klassifikaatorid, andmekirjelduse standardid jms).

Horisontaalsed seadusemuudatused

Avaliku teabe seadus (AvTS)

APA visiooni keskne õiguslik raamistik tuleb luua AvTS-is.

Vajalikud muudatused:

1. *Once-only* põhimõtte siduv norm
    - asutus ei tohi dubleerivalt küsida andmeid;
    - kohustus kontrollida andmete olemasolu teises andmekogus.
2. Andmete teisese kasutuse üldnorm
    - sh mitte-isikuandmete teisene kasutus;
    - eesmärgipiirangu raamistik.
3. Keskse andmejagamise mehhanismi regulatsioon
    - andmete teabevärava õiguslik staatus;
    - rollid (vastutav/volitatud töötleja);
    - kasutuslogid ja läbipaistvus.
4. Väärindatud andmete jagamise regulatsioon
    - otsustusliku mõjuga andmete erikäsitlus;
    - metoodika läbipaistvus.
5. Andmekirjelduse miinimumnõuded
    - õiguslik alus;
    - tundlikkus;
    - säilitamistähtaeg;
    - ristkasutuse lubatavus.
6. Andmete tundlikkuse kategooriad
    - diferentseeritud ligipääs.

AvTS-i muudatuste ulatus

AvTS muudatused on keskmise kuni suure ulatusega, kuid ei eelda seaduse täielikku ümberkirjutamist — tegemist on uue peatüki lisamisega andmete kogumise ja jagamise kohta.

Valdkondlike seaduste muutmise vajadus

APA realiseerimine eeldab valdkondlike seaduste muutmist, kus:

- seadus eeldab dokumentide esitamist, mitte andmevälju;
- sätestatakse kohustus esitada andmeid konkreetses vormis;
- puudub volitus andmete rist- ja teiseseks kasutuseks;
- saladust või muud konfidentsiaalset teavet sisaldavate andmete põhjendatud rist- ja teisese kasutamise võimaldamiseks hinnata andmete jagamise tingimusi.

Isikuandmete kaitse ja IKÜM

APA visioon peab isikuandmete töötlemisel arvestama IKÜM-iga. APA raames isikuandmete töötlemiseks tuleb:

- välja töötada selge õiguslik alus isikandmete rist- ja teiseseks töötlemiseks;
- luua mõju hindamise mehhanism kõrge tundlikkusega andmete puhul;
- tagada läbipaistvust andmesubjekti suhtes.

Isikuandmete kaitse seadust (IKS) võib olla vaja täpsustada seoses:

- andmete rist- ja teisest kasutust toetava erisätetega;
- avaliku huvi aluse selgemaks määratlemisega.

Rakendusaktid ja tehniline raamistik

Lisaks seadusemuudatustele on vajalikud järgmised rakendusaktid:

1. Andmekirjelduse standardi määrus
2. Tundlikkuse klassifikaatori määrus
3. Keskse andmejagamise mehhanismi tehniline regulatsioon
4. Nõusolekuteenuse kord
5. Põhiandmete kvaliteedinõuded

Ilma rakendusaktideta jääks seadus deklaratiivseks.

Kas vajalik on uus eraldi APA seadus?

Õiguslikult ei ole tingimata vajalik eraldi APA seadus, kui:

- AvTS täiendatakse süsteemselt;
- valdkondlikud seadused kohandatakse;
- tehnilised nõuded sätestatakse määrustes.

Eraldi APA seadus oleks põhjendatud vaid juhul, kui soovitakse terviklikku andmepoliitika ümberkujundamist.

Praeguses etapis on proportsionaalsem lahendus AvTS keskne täiendamine.

Kokkuvõte

APA visiooni realiseerimiseks on vajalik:

1. Avaliku teabe seaduse täiendamine andmete kogumise, ristkasutuse ja keskse jagamise regulatsiooniga;
2. Valdkondlike seaduste kohandamine dokumendipõhisest aruandlusest andmepõhiseks;
3. Selget üldnormi, mis reguleeriks andmete teises kasutuse;
4. Väärindatud andmete jagamise regulatsioon;
5. Rakendusaktide kehtestamine andmekirjelduse, tundlikkuse ja kvaliteedinõuete kohta.

Õigusanalüüs

1. RAAMISTIK JA METOODIKA

1.1. Teabe korraldamine

1.1.1. Andmekogu

Teabe ja andmete korraldamise eesmärgiks on, et andmed oleksid lihtsasti leitavad ja taaskasutatavad. Selle eesmärgi tagamise seisukohalt on oluline, et andmed on hästi kirjeldatud ja selgelt määratletud kvaliteedi tasemega. Seadusandja on andmete õiguspärase, süstemaatilise ja jälgitava töötlemise tagamise eesmärgil loonud andmekogude kontseptsiooni, mida reguleerib AvTS.

Üks viis andmeid ja isikuandmeid töödelda, on teha seda andmekogus. AvTS § 43[1] lg 1 kohaselt on andmekogu

- 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.[20]

Andmekaitse Inspektsioon (**AKI**) on esile toonud, et andmekogu formaalseks tunnuseks on, et see on asutatud seaduse või selle alusel antud akti alusel. Märgitakse, et muul juhul on reeglina tegu üldise avaliku sektori andmetöötlusega ehk avaliku teabe töötlemisega. Avalik teave ei moodusta andmekogu automaatselt, isegi kui see on korrastatud andmete kogum.[21]

AvTS § 43[1] lg 1 kohaselt võib andmekogu asutada üksnes seaduses või selle alusel antud õigusaktis sätestatud ülesannete täitmiseks. See tähendab ühtlasi, et haldusorgan ei tohi andmekogu pidada oma pädevusse mittekuuluvate ülesannete tarvis.[22]

Kui andmekogu sisaldab isikuandmeid, peab seaduse tasemel olema muuhulgas sätestatud:

- millisel eesmärgil ning milliste ülesannete täitmiseks andmeid kogutakse[23];
- milliseid isikuandmeid andmekogusse kogutakse. Seaduses tuleb sätestada isikuandmete üldised grupid, mis annab määrusandjale raamid volituse ulatuse ja piiride osas ehk teisisõnu, määruses saab täpsustada, milliseid nendesse gruppidesse kuuluvaid andmeid kogutakse[24];

---

[20] Andmekaitse Inspektsioon. Andmekogude juhend. 2013. - https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf (30.03.2026), lk 3, 12.
[21] *Ibid.*, lk 3, alapunkt 1.1.
[22] *Ibid.*, lk 6, alapunkt 2.1.
[23] Mikiver, M. Analüüs. Andmekogud ja isikuandmed: EV põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile. Justiitsministeerium 2021. – https://www.just.ee/media/3193/download (30.03.2026). Lk 34.
[24] *Ibid.*, lk 34.

- vajadusel andmete juurdepääsupiirangud[25];
- muul eesmärgil andmete kasutamise piirangud[26];
- kui kaua andmeid säilitatakse[27].

Andmekogude reguleerimise eesmärk on tagada kontroll andmete töötlemise üle ning välistada võimalikud ebaseaduslikud andmete töötlemise võimalused avalikke ülesandeid täitvate isikute poolt. AvTS § 43^3 lg 2 kohaselt on keelatud asutada ühtede ja samade andmete kogumiseks eraldi andmekogusid.[28,29,30] Seadusandja on loonud põhjendatult andmekogude loomise regulatsiooni, et vältida põhjendamatut andmete töötlemist ning tagada seaduslik andmete töötlemine ning võimalikult minimaalne puudutatud isikute õiguste riive. Andmekogu loomise protsessi on kaasatud Riigi Infosüsteemi Amet, Andmekaitse Inspektsioon ja Statistikaamet. Eeltoodud asutused on kaasatud nii andmekogu asutamise ja lõpetamise protsessidesse kui ka andmekogu andmete koosseisu muutmiste protsessi. Möönda tuleb, et andmekogu asutamise, lõpetamise ja andmekogu andmete koosseisu muutmise protsess võib olla aja- ja töömahukas. Kuid andmekogu asutamist puudutavad seadusest tulenevad protsessid on igati põhjendatud ja proportsionaalsed, võttes arvesse, et avalikke ülesandeid täitva isiku tegevus sh andmete töötlemise alus peab tulenema seadusest ja töötlemine peab vastama seadusele.

1.1.1.1. Andmekogu dokumentatsioon

Nõuded andmekogu dokumentatsioonile on reguleeritud AvTS rakendusaktis Vabariigi Valitsuse määruses 28.02.2008 nr 58 Riigi infosüsteemi haldussüsteem (edaspidi RIHA määrus)§-des 6-8. RIHA määrus § 6 lg 1 sätestab, et enne andmekogu asutamist või andmekogus kogutavate andmete koosseisu muutmist kontrollib andmekogu asutaja või vastutav töötleja, kas vajalikke andmeid juba kogutakse mõnes olemasolevas andmekogus. Vastavalt RIHA määruse § 6 lg-le 3 koosneb andmekogu dokumentatsioon RIHA määruse § 18 lg 2 p-des 1-22, 24, 26-28, lg-s 3,4 ja § 19 lg-s 2 ja § 20 lg-s 2 loetletud andmetest ning §-s 26 viidatud AvTS § 43^9 lg 1 p-s 1 viidatud Vabariigi Valituse klassifikaatorite süsteemi määruse[31] alusel kehtestatud klassifikaatorite andmetest. Eeltoodud andmed ja teave, mis tuleb andmekogu asutamise ettevalmistamisel kaardistada, on seadusandja loonud eesmärgiga, et andmekogu asutamisel mõeldaks läbi andmekogu eesmärgid ja töödeldavate andmete koosseis, et vältida ebaseaduslikku ja/või ebavajalikku andmete töötlemist, kohustatud isikute ning teiste avalikke ülesandeid täitvate isikute asjakohatut koormamist jne. Seadusandja ei ole loonud kuidagi ebaloogilist või ebavajalikku kohustust seoses andmekogu dokumentatsiooniga või ülevaadet andmetest andmekogu asutamisel või muutmisel.

---

[25] Andmekaitse Inspektsioon. Andmekogude juhend. 2013. https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf (30.03.2026), lk 12.
[26] *Ibid.*, lk 12.
[27] Mikiver, M, lk 34.
[28] Majandus- ja Kommunikatsiooniministeerium. Andmeladude olemus ja selle funktsioonid. Selgitav juhis. 2023. – https://www.kratid.ee/_files/ugd/980182_5b9c740580a543c0ab48480b07c7ce5f.pdf (30.03.2026). Lk 14.
[29] Andmekaitse Inspektsioon. Andmeladude seire kokkuvõte. – https://www.aki.ee/sites/default/files/seired/andmeladude_seire_kokkuvote.pdf (30.03.2026). Lk 1.
[30] Andmekaitse Inspektsioon. Andmekogude juhend. 2013. – https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf (30.03.2026). Lk 5, alapunkt 1.6.
[31] RT I 2008, 4, 27.

Andmekogude asutamine ei ole tsentraliseeritud ehk iga andmekogu vastutav ja volitatud töötleja peavad eelkõige ise hindama andmekogu vajalikkust oma avalike ülesannete täitmise seisukohalt ja üleüldise riigi andmekogude vaates. Nentida tuleb, et asutustel on väga erinev teadlikkus ja valmisolek andmekogu asutaja, vastutava ja volitatud töötleja rolliks ning RIHA määruse § 6 lg-s 2 välja toodud andmete kajastamine andmekogu dokumentatsioonis võib osutuda väljakutseks. Selleks puhuks on seadusandja loonud AvTS § 43^3 lg-s 3 kooskõlastamise meetme. Nimelt AvTS § 43^3 lg 3 sätestab, et enne andmekogu asutamist, andmekogus kogutavate andmete koosseisu muutmist, andmekogu kasutuselevõtmist või andmekogu lõpetamist kooskõlastatakse andmekogu tehniline dokumentatsioon Riigi Infosüsteemi Ametiga, Andmekaitse Inspektsiooniga ja Statistikaametiga. Peale andmekogu dokumentatsiooni koostamist tuleb vastav dokumentatsioon kooskõlastada Riigi Infosüsteemi Ameti, Andmekaitse Inspektsiooni, Statistikaameti, Maa-ameti ning Rahvusarhiiviga vastavalt RIHA määruse § 7 lg-le 1. Võib kaaluda võimalust, et andmekogu dokumentatsiooni kooskõlastamisele eelneks konsulteerimise kohustus, mis võiks aidata andmekogu vastutavat töötlejat andmekogu asutamisel või andmekogu või selle andmeobjektides muudatuste tegemisel. Nimelt on kõigil eelpool nimetatud asutustel vastavalt oma pädevusele kompetents nõustada andmekogu vastutavat ja volitatud töötlejat andmekogu ja andmekogu andmete koosseisu puudutavates küsimustes. Kui leitakse, et eelpool toodud konsulteerimine on põhjendatud ja vajalik, siis tuleb AvTS-is lisaks dokumentide kooskõlastusele selgesõnaliselt välja tuua AvTS § 43^3 lg-s 3 toodud asutuste kohustus konsulteerida andmekogu asutajat. Ühtlase praktika ning andmekogude kvaliteedi seisukohalt oleks oluline, et andmekogu asutajatel ja vastutaval töötlejal oleks võimalus ja vastavatel asutustel (Riigi Infosüsteemi Amet, Andmekaitse Inspektsioon ja Statistikaamet) kohustus konsulteerida andmekogu vastutavat töötlejat. Konsulteerimine peaks loogiliselt eelnema andmekogu dokumentide kooskõlastusele. Sarnaselt andmekogu dokumentatsiooni nõuetele ja kooskõlastamisele tuleb konsulteerimise protsess täpsustada AvTS-i rakendusaktis ehk RIHA määruses.

RIHA määrus § 7 lg 2 p-d 1-2 sätestavad erandi, mille kohaselt eelviidatud kooskõlastamist ei ole vaja teostada ja andmekogu dokumentatsioon registreeritakse, kui (i) andmekogu asutatakse ainult organisatsiooni sisemise töökorralduse vajadusteks; või (ii) andmekogu on asutatud asutustevaheliseks dokumentide menetlemiseks ja see ei kuulu riigi infosüsteemi. Kui ei esine RIHA määruses § 7 lg 2 p-des 1 või 2 sätestatud juhtu, siis tuleb andmekogu dokumendid kooskõlastada.

RIHA määrus § 18 lg 3 p 4 sätestab, et andmekogu dokumentatsioonis tuleb kajastada põhiandmete loetelu ning vastavalt RIHA määruse § 18 lg 3 p-le 5 tuleb teha vastavad viited põhiandmeteks mitteolevate andmete algallikale. Andmekogu dokumentatsiooni kehtiva kooskõlastamise protsessi ja võimaliku konsulteerimise kohustuse tulemuslikkuse seisukohalt tuleb kaaluda täpsustust, mille kohaselt andmekogu vastutav töötleja peab selgitama, kuidas on jõutud järeldusele, et konkreetne andmeobjekt on põhiandmed. Samuti ei pea andmekogu vastutav või volitatud töötleja kirjeldama valmisolekut andmeid jagada teiste õigustatud isikutega. Andmekogu loomise kontseptsioon on pigem suunatud andmete saamisele ja loomisele mitte niivõrd andmete jagamisele. Samas lähtudes asjaolust, et ühte andmeobjekti ei saa korduvalt põhiandmetena määrata, siis peab andmekogu vastutav töötleja olema valmis andmeid jagama, et täita *once-only* põhimõttest tulenevat andmete rist- ja taaskasutust.

Seaduse alusel loodud andmekogud annavad andmekogule õigusliku tähenduse ning avalikke ülesandeid täitvale isikule õiguse ja kohustuse kasutada andmete töötlemisel konkreetset keskkonda, tingimusi, kindlat komplekti andmeobjekte ning vajadusel täita seadusest tulenevat andmete õigsuse eeldust. Seadusandja on loonud nõuded ja protsessid andmekogu vastutavale ja volitatud töötlejale eesmärgiga vältida ebaseaduslikku või suvalist andmete kogumist ja muud moodi töötlemist. Seega ei ole põhjendatud kuidagi leevendada andmekogude asutamise protsessi ja/või luua muu n-ö lihtsustatud andmekogu (andmestik). Eeltoodud andmekogude kontseptsiooni eesmärk on tagada andmete

õiguspärane töötlemine, korrastatus ning seeläbi avaliku halduse efektiivistamine ja e-riigi toimimise seisukohalt oluliste põhimõtete rakendamise võimalikkus. Olenemata eeltoodud andmekogu legaalkontseptsioonist ja reeglitest puudub mehhanism, mis tagaks andmete rist- ja taaskasutuse ning seeläbi *once-only* põhimõtte andmekogude ülese rakendamise. Selle tulemusel puudub terviklik ülevaade andmekogudes olevatest andmetest, sh põhiandmetest.

1.1.1.2. Andmekogu vastutav töötleja (haldaja)

Andmekogu ei ole võimalik luua ilma andmekogu vastutava töötlejata. Nimelt vastavalt AvTS § 43[3] lg-le 1 tuleb andmekogu vastutav töötleja alati määratleda andmekogu põhimääruses või kui andmekogu pidamine reguleeritakse seadusega, siis andmekogu vastutav töötleja sätestatakse vastavas seaduses .[32] Andmekogude vastutava töötleja legaaldefinitsioon on toodud AvTS-is. AvTS § 43[4] lg 1 sätestab, et andmekogu vastutav töötleja (haldaja) on riigi- või kohaliku omavalitsuse asutus, muu avalik-õiguslik juriidiline isik või avalikke ülesandeid täitev eraõiguslik isik, kes korraldab andmekogu kasutuselevõtmist, teenuste ja andmete haldamist. Andmekogu vastutav töötleja vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest.

Kuigi andmekogu vastutava töötleja legaaldefinitsioonis on funktsionaalseid aspekte, siis ei ole võimalik andmekogu vastutavat töötlejat määrata teatud faktiliste asjaolude ilmnemisel.[33]

Eelviidatud sättes kasutatud andmete haldamise korraldamise all tuleb mõista otsuste langetamist ja elluviimist andmetega seotud küsimustes, mis hõlmab väga laia hulka elulisi olukordi andmetöötluse kogu elutsükli jooksul. Seadusandja ei ole võimaldanud määrata mitut vastutavat töötlejat ühele andmekogule. Samas on õiguskirjanduses leitud, et iseenesest ei ole kaasvastutus andmekogude puhul välistatud.[34] Märkida tuleb, et praktikas siiski on andmekogudel kaasvastutavad töötlejad. Näiteks vastavalt tervise infosüsteemi põhimääruse[35] § 3 lg-le 1 on tervise infosüsteemi kaasvastutavad töötlejad Sotsiaalministeerium ja Tervisekassa.

Andmekogu vastutava töötleja tegevust reguleerivad IKÜM ja AvTS, andmekogu loomise aluseks olev seadus ja sellise seaduse alusel loodud andmekogu põhimäärus ning RIHA määrus, mis on kehtestatud AvTS alusel.

1.2. Andmepõhise aruandluse andmete käsitlus ja metoodika

Käesoleva õigusanalüüsi eesmärk on luua süsteemne ja rakendatav metoodika, mis võimaldab hinnata andmepõhise aruandluse raames kogutavate ettevõtlusandmete töötlemise, jagamise ja teisese kasutamise õiguslikke piiranguid ning *once-only* põhimõtte kohaldatavust.

1.2.1. APA tähendus ja regulatiivne lähtekoht

Andmepõhine aruandlus kujutab endast kvalitatiivset muutust ettevõtjate aruandluskohustuse täitmise viisis. Kui traditsiooniline aruandlus põhineb dokumentidel, siis APA keskmes on struktureeritud andmeväljad ning nende automatiseeritud liikumine infosüsteemide vahel.

---

[32] Värk, K. Isikuandmete vastutava ja volitatud töötleja kontseptsiooni rakendamine andmekogudes. Magistritöö. Juhendajad Julia Antonova, Paloma Krõõt Tupay. Tartu: TÜ õigusteaduskond 2021. Lk 44.
[33] *Ibid.,* lk 44.
[34] *Ibid.,* lk 44.
[35] RT I, 10.12.2025, 3.

APA toimeloogika põhineb kolmel sambal:

(i) **Andmed, mitte dokumendid**

Riik ei küsi enam aruandeid tervikdokumentidena, vaid konkreetseid andmevälju (nt töötasu väljamakse, kütusekogus, müügitehing vms).

(ii) **Automaatsus**

Andmed liiguvad ettevõtja majandustarkvarast riigi infosüsteemidesse masin-masin liideste kaudu (API). Automaatseks andmevahetuseks on vajalik ettevõtja kinnitus või püsiv nõusolek.

(iii) **Ühekordne küsimine *(once-only*)**

Kui andmed on esitatud ühele asutusele, peab teistel asutustel olema õigus neid nii samal kui ka erineval eesmärgil rist- ja taaskasutada.

Selline mudel eeldab andmete õigusliku režiimi diferentseeritud käsitlust, sest kõik andmed ei ole rist- ja taaskasutuseks võrdselt sobivad.

1.2.2. Andmetüüpide süsteem

Metoodika lähtub eeldusest, et andmete töötlemise lubatavus sõltub:

(i) andmete õiguslikust režiimist (isikuandmed, mitte-isikuandmed, konfidentsiaalsed andmed (ärisaladus, maksusaladus, pangasaladus, AvTS alusel juurdepääsu piiranguga andmed);

(ii) andmete funktsioonist (regulatiivsed, statistilised, aruandluslikud);

(iii) andmete tundlikkusest;

(iv) andmete mõjust õigustele ja kohustustele.

Sellest tulenevalt töötati välja APA-spetsiifiline viieastmeline tundlikkuse skaala (T1–T5), mis võimaldab diferentseerida andmeid vastavalt nende õiguslikule riskiprofiilile.

1.2.3. Tundlikkuse hindamine

Tundlikkuse hindamisel arvestatakse:

(i) kas andmed sisaldavad isikuandmeid;

(ii) kas andmed sisaldavad ärisaladust või maksusaladust;

(iii) kas andmete töötlemine võib mõjutada isiku või ettevõtte õigusi;

(iv) kas andmete avalikustamine või väärkasutus võib põhjustada olulist kahju.

Tabel nr 1. APA-spetsiifiline viieastmeline tundlikkuse skaala

Nr	Andmetüüp	Tundlikkus	*Once-only* sobivus
1.	Klassifikaatorid	T1	Väga kõrge
2.	Koondandmed	T2	Kõrge
3.	Tehinguandmed	T3	Tingimuslik

4.	Maksuandmed	T4	Madal
5.	Julgeolekuandmed	T5	Väga madal

(i) Skaala võimaldab määrata iga andmevälja tundlikkuse taseme ning sellest tulenevalt sobiva töötlemisrežiimi. Lisaks võimaldab skaala:prognoosida *once-only* rakendatavust

(ii) määrata vajaliku regulatsiooni rangust

(iii) kujundada diferentseeritud andmehalduse režiimi

Tabel nr 2. APA tundlikkuse skaala (T1-T5)

	T1 – madal tundlikkus	T2 – piiratud tundlikkus	T3 – keskmine tundlikkus	T4 – Kõrge tundlikkus	T5 – Väga kõrge tundlikkus
Iseloomustus	• Ei sisalda isikuandmeid • Ei sisalda ärisaladust • Ei mõjuta konkurentsiolukorda • Ei sisalda järelevalve- ega sanktsiooniriski	• Mitte-isikuandmed • Võib sisaldada äriliselt tundlikku infot • Mõõdukas konkurentsirisk	• Tavalised isikuandmed või ärisaladus • Sisaldab konkreetse ettevõtte strateegilist infot • Võib mõjutada õigusi või kohustusi	• Eriliiki isikuandmed • Maksusaladus • Karistusandmed • Sanktsioonimenetluse andmed	• Julgeolekuinfo • Kriitilise taristu andmed • Strateegilised riigikaitselised andmed • Ulatuslik mõju põhiõigustele
Näited	• agregeeritud majandusnäitajad • anonüümne statistika • keskmised sektorinäitajad	• ettevõtte kogukäive • toodangu maht • energiatarve ettevõtte tasandil	• töötajate palgaandmed • detailne kulustruktuur • toetuste taotluste detailandmed	• terviseandmed • maksuvõlgade detailandmed • järelevalvemenetluse info	• nt laovarude info riigisaladusega kaetud esemete osas • luurinfo • riigisaldusega kaitstud kauba eksport/import
***Once-only* sobivus**	Väga kõrge	Kõrge	Tingimuslik	Madal	Väga madal
Jagatavus	Piiranguteta (võivad olla avaandmed)	Riigiasutuste vahel üldjuhul lubatav	Vajab selget õiguslikku alust	Rangelt piiratud	Eriseaduse alusel
Riskitase	Väga madal	Madal–keskmine	Keskmine	Kõrge	Väga kõrge

1.2.4. Õigusliku riskihindamise maatriks

Andmepõhise aruandluse kontekstis ei ole andmete ristkasutuse lubatavus määratav üksnes andmete tüübi või tundlikkuse alusel. Selleks, et hinnata *once-only* põhimõtte kohaldatavust konkreetses olukorras, on vajalik kasutada struktureeritud õigusliku riskihindamise mudelit. Käesolevas analüüsis

rakendatakse kaheastmelist riskihindamise lähenemist, mis kombineerib andmete töötlemise mõju ning õigusliku regulatsiooni selguse.

Töötlemise mõju all mõistetakse eeskätt seda, milline on andmete kasutamise potentsiaalne mõju isiku või ettevõtja õigustele ja huvidele. See hõlmab muu hulgas andmete tundlikkust, töötlemise ulatust, võimalikku majanduslikku või õiguslikku mõju ning seda, kas andmete kasutamise tulemusena tehakse haldusotsuseid või muid õigusi mõjutavaid toiminguid. Mida suurem on töötlemise mõju, seda kõrgem on ka õiguslik risk.

Õigusliku regulatsiooni selgus viitab sellele, mil määral on andmete kogumine, kasutamine ja jagamine selgelt reguleeritud kehtivates õigusaktides. Selge regulatsiooni olemasolul on andmete ristkasutus paremini prognoositav ja õiguspärane, samas kui ebaselge või puuduv regulatsioon suurendab õiguslikku ebakindlust ning vajadust täiendavate normide järele.

Nende kahe mõõtme kombineerimisel kujuneb riskiskoor, mille alusel on võimalik hinnata, millises ulatuses on *once-only* põhimõtte rakendamine konkreetses olukorras lubatav. Riskihindamise tulemusena eristatakse neli peamist olukorda.

Esiteks võib andmete ristkasutus olla kohe rakendatav juhul, kui töötlemise mõju on madal ning õiguslik regulatsioon on selge ja piisav. Sellisel juhul ei esine olulisi õiguslikke takistusi andmete korduvkasutamiseks ning automatiseeritud andmevahetus on põhjendatud.

Teiseks võib ristkasutus vajada täpsustavat regulatsiooni olukorras, kus töötlemise mõju on mõõdukas või regulatsioon on osaliselt ebaselge. Sellisel juhul ei ole andmete kasutamine iseenesest välistatud, kuid nõuab täiendavat normatiivset või metoodilist täpsustamist, näiteks juhiste või alamaktide tasandil.

Kolmandaks võib andmete ristkasutus eeldada seaduse muutmist juhul, kui töötlemise mõju on kõrge ning kehtiv õiguslik alus ei võimalda andmete teisest kasutust piisava selgusega. Sellisel juhul ei ole võimalik *once-only* põhimõtet rakendada ilma seadusandliku sekkumiseta.

Neljandaks võib esineda olukordi, kus *once-only* põhimõtte kohaldamine ei ole lubatav. See puudutab eelkõige juhtumeid, kus töötlemise mõju on väga kõrge ning andmete kasutamine teisel eesmärgil oleks vastuolus põhiõiguste kaitse, konfidentsiaalsuse või eesmärgipiirangu põhimõttega.

Õigusliku riskihindamise maatriks toimib seega analüütilise tööriistana, mis võimaldab siduda omavahel andmetüübi, andmete tundlikkuse, konkreetse töötlemistoimingu ning sellest tulenevad õiguslikud riskid. Selline lähenemine aitab vältida nii ülemäärast andmete jagamist kui ka põhjendamatuid piiranguid ning võimaldab kujundada diferentseeritud ja proportsionaalset andmekorraldust.

Kokkuvõttes loob riskihindamise maatriks süsteemse aluse otsustamiseks, millal ja millistel tingimustel on andmete ristkasutus APA raamistikus õiguspärane ning millal on vajalik täiendav regulatiivne sekkumine.

Tabel nr 3. Õigusliku riskihindmaise maatriks

Tase	Kirjeldus	Õiguslik
1	Mõju puudub või minimaalne	Selge õiguslik alus
2	Piiratud mõju ettevõttele	Mõningane tõlgendusvajadus
3	Mõõdukas mõju õigustele/kohustustele	Ebapiisav regulatsioon

4	Oluline mõju õigustele	Õiguslik vastuolu
5	Väga oluline mõju põhiõigustele	Puudub õiguslik alus

Tabel nr 4. Näide palgaandmete ristkasutamisest

Näide: palgaandmete ristkasutuse õiguslik riskihindamine

Õigusliku riskihindamise maatriksi rakendamist võib illustreerida palgaandmete näitel, mis on andmepõhise aruandluse kontekstis üks kesksemaid andmeliike.

Andmetüüp: tehinguandmed (kõrge granulaarsus)
Andmeväli: brutopalk, netopalk, tööandja makstud maksud
Tundlikkus: keskmine kuni kõrge (sisaldab isikuandmeid ning võib sisaldada ka ärisaladuse elemente)

1. Töötlemise mõju hindamine

Palgaandmete töötlemisel on mõju mitmetasandiline:

- Isikuandmete aspekt

  palk on otseselt seotud füüsilise isiku majandusliku olukorraga;

- Õiguslik mõju

  palgaandmete alusel määratakse maksukohustused, sotsiaalsed tagatised ja toetused;

- Majanduslik mõju

  andmete väär kasutamine võib mõjutada nii töötaja kui ka tööandja huve.

Sellest tulenevalt on töötlemise mõju hinnatav vähemalt keskmiseks kuni kõrgeks.

2. Õigusliku regulatsiooni selgus

Palgaandmete kogumine ja kasutamine on Eesti õiguses suhteliselt selgelt reguleeritud:

- Maksukorralduse seadus ja maksuseadused sätestavad andmete kogumise ja kasutamise alused;
- Tööõigus ja sotsiaalkindlustuse regulatsioonid määravad andmete kasutamise eesmärgid;
- IKÜM seab piirangud isikuandmete töötlemisele.

Samas ei ole kõigi võimalike ristkasutuse juhtude puhul (nt erinevate asutuste vahel analüütilisel eesmärgil) regulatsioon täielikult üheselt selge.

Seetõttu võib regulatsiooni selgust hinnata keskmiseks.

3. Riskiskoor ja järeldus

Kombineerides:

- töötlemise mõju: keskmine–kõrge
- õigusliku regulatsiooni selgus: keskmine

paigutub palgaandmete ristkasutus riskihindamise maatriksis kategooriasse, kus:

Järeldus: andmete ristkasutus on põhimõtteliselt lubatav, kuid vajab täpsustavat regulatsiooni.

4. *Once-only* kohaldamine

Sellest tulenevalt:

- palgaandmete esitamine Maksu- ja Tolliametile võib toimuda üks kord (esmane kogumine);
- teiste asutuste (nt Statistikaamet, Töötukassa) ligipääs samadele andmetele on põhjendatud;
- kuid andmete kasutus peab olema:
    - selgelt eesmärgipõhine,
    - piiratud vajaliku ulatusega,
    - ning vajadusel täpsustatud seaduse või alamaktidega.

5. Õiguslik järeldus

Palgaandmete näide illustreerib, et isegi suhteliselt hästi reguleeritud andmeliigi puhul ei ole *once-only* põhimõtte rakendamine täielikult automaatne. Kuigi ristkasutus on tehniliselt ja osaliselt ka õiguslikult võimalik, eeldab selle laiendamine täiendavat normatiivset selgust, eelkõige seoses teisese kasutuse ulatuse, eesmärgipiirangu ning andmete jagamise tingimustega.

Riskiskoori arvutamisel korrutatakse hinnanguline mõju (1–5) õigusliku ebakindluse tasemega (1–5); tulemuse põhjal otsustatakse, millisel määral on once-only põhimõtte rakendamine õiguspärane ja otstarbekas

Tabel 5. Riskiskoori tõlgendamine once-only rakendamisel

Skoor	Riskitase	Soovitus
1-5	Madal	Võib rakendada *once-only*
6-10	Mõõdukas	Vajab täpsustavat regulatsiooni
11-15	Kõrge	Vajab seaduse muutmist
16-25	Väga kõrge	*Once-only* mitte rakendada

1.2.5. Once-only põhimõtte diferentseeritud rakendamine

Metoodika keskne järeldus on, et *once-only* põhimõtte rakendamine ei saa olla absoluutne ega universaalne. Selle kohaldatavus peab sõltuma andmete tundlikkusest ja õiguslikust riskiprofiilist.

Madala tundlikkusega andmete puhul (T1–T2) võib rakendada automaatset ristkasutust. Keskmise tundlikkusega andmete puhul (T3) on vajalik täiendav õiguslik täpsustus või turvameetmed. Kõrge tundlikkusega andmete puhul (T4–T5) on vajalik eriseaduslik alus või *once-only* välistamine.

Tabel nr 6. *Once-only* põhimõtte diferentseeritud rakendamine

Nr	Andmetüüp	Õiguslik alus	Peamised piirangud	Jagatavus asutuste või andmekogude vahel	*Once-only* sobivus	Tingimuslikkus
1.	**Tavalised isikuandmed**	IKÜM art 6	eesmärgipiirang, minimaalsus	Lubatav õigusliku aluse olemasolul	Tingimuslik	Vajab selget teisese töötlemise alust
2.	**Eriliiki isikuandmed**	IKÜM art 9	rangemad alused, erikaitse	Väga piiratud	Madal	Vajab seadusest tuleneva alust või nõusolekut
3.	**Karistusandmed**	IKÜM art 10 + IKS	riiklik kontroll	Piiratud	Madal	Ainult seaduse alusel
4.	**Mitte-isikuandmed**	AvTS, eriseadused	ärisaladus, maksusaladus	Üldjuhul lubatav	Kõrge	Kui puudub konfidentsiaalsus
5.	**Ärisaladus**	AvTS juurdepääsupiirang	konfidentsiaalsus	Piiratud	Keskmine	Vajab eesmärgi- ja kasutuspiirangut
6.	**Maksusaladus**	MKS	range saladuse režiim	Piiratud	Keskmine	Vajab erisätet
7.	**Pangasaladus**	Krediidiasutuste seadus (KAS), IKÜM (kui sisaldab isikuandmeid)	range konfidentsiaalsus, kliendiandmete kaitse, avaldamise keeld ilma õigusliku aluseta	Väga piiratud (ainult seaduses sätestatud juhtudel, nt järelevalve, maksu- või kriminaalmenetlus)	Madal kuni keskmine	Vajab selget seaduslikku alust ja sageli erisätet; võimalik piiratud ulatuses või agregeeritult
8.	**Statistilised andmed (agregeeritud**	Riikliku statistika seadus	anonüümimise nõue	Hea	Kõrge	Kui identifitseerimisrisk puudub
9.	**Tuletatud andmed**	sõltub sisendist	metoodika läbipaistvus	Tingimuslik	Keskmine	Vajab arvutusreeglite selgust
10.	**Avaandmed**	AvTS § 29	isikuandmete välistus	Täielik	Väga kõrge	Masinloetavus kohustuslik

Once-only ja ühekordse sisestamise põhimõtete eristamise metoodika

Andmepõhise aruandluse kontekstis tuleb eristada kahte sisuliselt erinevat, kuid praktikas sageli kattuvat lähenemist: (i) *once-only* põhimõtet kitsas tähenduses ning (ii) ühekordse sisestamise (*single entry*) põhimõtet. Kuigi mõlemad aitavad vähendada ettevõtjate halduskoormust, erinevad need oma õigusliku iseloomu, rakendustingimuste ja regulatiivsete eelduste poolest.

Once-only põhimõte tähendab, et ettevõtja esitab andmed riigile üksnes ühe korra ning edaspidi tagab riik nende andmete õiguspärase ristkasutuse erinevate asutuste vahel. Tegemist on eelkõige õigusliku

mehhanismiga, mille rakendamine eeldab selget õiguslikku alust andmete teisese kasutuse jaoks, eesmärgipiirangu järgimist ning andmete tundlikkusest tulenevate riskide maandamist.

Ühekordse sisestamise põhimõte tähendab seevastu, et ettevõtja sisestab andmed oma infosüsteemi üks kord ning edastab need tehniliselt erinevatele asutustele kas samaaegselt või eraldi andmesektsioonidena. Sellisel juhul ei pruugi toimuda riigisisest ristkasutust, vaid tegemist on tehnilise lahendusega, mis vähendab ettevõtja sisestuskoormust, kuid ei lahenda iseenesest andmete dubleeriva kogumise probleemi õiguslikus tähenduses.

Käesolevas analüüsis on välja töötatud metoodika, mille alusel hinnata, milliste andmekategooriate puhul on põhjendatud *once-only* põhimõtte rakendamine ning millistel juhtudel tuleb piirduda ühekordse sisestamise lahendusega.

Metoodika lähtub kolmest põhikriteeriumist.

Esiteks hinnatakse andmete õiguslikku tundlikkust. Madala tundlikkusega andmete, näiteks klassifikaatorite ja avaliku teabe puhul, on *once-only* põhimõtte rakendamine üldjuhul täielikult põhjendatud. Kõrge tundlikkusega andmete, sealhulgas isikuandmete, maksusaladuse ja ärisaladuse puhul on ristkasutus võimalik üksnes tingimuslikult ning eeldab täiendavaid õiguslikke aluseid või piiranguid.

Teiseks hinnatakse andmete struktureeritust ja semantilist selgust. Struktureeritud ja standardiseeritud andmeväljad on sobivad automatiseeritud ristkasutuseks ning seega *once-only* põhimõtte rakendamiseks. Struktureerimata andmete puhul, mille sisu ei ole masinloetavalt määratletud, on ristkasutus piiratud ning praktikas rakendub pigem dokumentide leitavusel põhinev või nõusolekupõhine jagamine.

Kolmandaks hinnatakse andmete kasutuse eesmärki ja mõju. Kui andmeid kasutatakse mitmes haldusmenetluses või erinevate asutuste ülesannete täitmiseks, on *once-only* põhimõtte rakendamine õigustatud, eeldusel et eesmärgipiirang on tagatud. Kui andmete kasutus on kitsalt seotud ühe konkreetse menetlusega või eeldab kontekstipõhist tõlgendamist, võib olla põhjendatud piirduda ühekordse sisestamisega ilma laiemat ristkasutust võimaldamata.

Metoodika rakendamisel saab teha järgmise üldistuse: *once-only* põhimõte on sobiv eelkõige standardiseeritud, madalama tundlikkusega ja korduvkasutatavate andmete puhul, samas kui ühekordse sisestamise põhimõte on sobiv lahendus juhtudel, kus andmete ristkasutus on õiguslikult piiratud või tehniliselt keerukas.

Selline diferentseeritud lähenemine võimaldab ühtaegu saavutada andmepõhise aruandluse eesmärgid ning tagada andmete töötlemise kooskõla andmekaitse, eesmärgipiirangu ja proportsionaalsuse põhimõtetega.

1.3. Andmete omaniku määramise metoodika

1.3.1. Lähtekoht ja probleemipüstitus

Kehtivas Eesti ja Euroopa Liidu õiguses puudub ühtne ja selgesõnaline mõiste „andmete omanik“, mida saaks kasutada andmepõhise aruandluse kontekstis. Õiguslik regulatsioon lähtub eelkõige teistest kategooriatest, nagu vastutav töötleja, volitatud töötleja ja andmesubjekt (IKÜM), samuti andmekogu vastutav töötleja (avaliku teabe seadus). Seetõttu ei ole võimalik andmete „omandit“ käsitleda klassikalise omandiõiguse mõistes.

APA rakendamise seisukohalt on siiski vajalik määratleda, kellel on õigus otsustada andmete kasutamise, jagamise ja kontrolli üle. Eriti oluline on see nõusolekuteenuse, andmete ristkasutuse ning *once-only* põhimõtte rakendamisel. Seetõttu on käesolevas analüüsis välja töötatud funktsionaalne metoodika andmete „omaniku" määramiseks, mis ei lähtu formaalsest omandiõigusest, vaid andmetega seotud õiguste ja huvide jaotusest.

1.3.2. Funktsionaalne lähenemine

Käesolev metoodika lähtub põhimõttest, et andmete „omanik" ei ole üksainus subjekt, vaid roll jaotub mitme osapoole vahel sõltuvalt andmete liigist ja kasutusest. Seetõttu kasutatakse mõistet **andmete kontrolli kandja**, mille all mõistetakse isikut või asutust, kellel on õigus otsustada andmete kasutamise üle konkreetses kontekstis.

Andmete kontrolli määramisel tuleb eristada vähemalt järgmisi rolle:

- **andmesubjekt** – füüsiline isik, kelle kohta andmed käivad (IKÜM mõistes);
- **andmete esitaja** – isik või ettevõtja, kes esitab andmed riigile;
- **vastutav töötleja** – asutus, kes määrab andmete töötlemise eesmärgid ja vahendid;
- **andmete kasutaja** – asutus või isik, kes kasutab andmeid teisese töötlemise eesmärgil.

Ühelgi neist rollidest ei ole absoluutset „omandiõigust" andmete üle, vaid igaühel on piiratud õigused ja kohustused.

1.3.3. Andmete omaniku määramise test

Andmete kontrolli (nn „omaniku") määramiseks tuleb rakendada järgmine neljaastmeline test:

1. **Kelle kohta andmed käivad?**

Kui andmed on seostatavad füüsilise isikuga, on tegemist isikuandmetega ning andmesubjektil on andmete suhtes tugevad õigused (nt juurdepääs, parandamine, kustutamine).

2. **Kes on kohustatud andmeid esitama?**

Kui andmete esitamine tuleneb seadusest (nt maksuaruandlus), on andmete esitaja roll piiratud – ta ei otsusta andmete kasutamise üle, vaid täidab õiguslikku kohustust.

3. **Kes määrab andmete töötlemise eesmärgi?**

See on keskne kriteerium. Kui asutus määrab, miks ja kuidas andmeid kasutatakse, on ta vastutav töötleja ning tal on peamine kontroll andmete kasutamise üle.

4. **Kelle õigusi ja huve andmete kasutamine mõjutab?**

Kui andmete kasutamine mõjutab otseselt isiku või ettevõtja õigusi (nt maksustamine, järelevalve), tuleb arvestada nende subjekti õigustega ning piirata andmete kasutamist vastavalt.

1.3.4. Metoodika rakendamine (palgaandmete näide)

Palgaandmed on tüüpiline näide, kus andmete „omand" on jagatud mitme osapoole vahel.

Andmete kirjeldus: brutopalk, väljamaksed, maksud, töötaja identifikaator.

Metoodika rakendamine:

1. Andmesubjekt (töötaja)

- Palgaandmed on isikuandmed.
- Töötajal on IKÜM-ist tulenevad õigused (nt juurdepääs, parandamine).
- Töötaja ei kontrolli siiski andmete esitamist riigile, kui see tuleneb seadusest.

2. Andmete esitaja (tööandja)

- Tööandja kogub ja esitab palgaandmed maksuhaldurile.
- Tal on kohustus tagada andmete õigsus.
- Tööandjal puudub õigus otsustada, kas andmeid esitada või mitte.

3. Vastutav töötleja (nt Maksu- ja Tolliamet)

- Määrab andmete kasutamise eesmärgi (maksustamine, kontroll).
- Omab peamist kontrolli andmete edasise kasutamise üle.
- On seotud rangete piirangutega (maksusaladus).

4. Teisene kasutaja (nt Statistikaamet)

- Võib kasutada andmeid statistilistel eesmärkidel.
- Ei tohi kasutada andmeid individuaalsete otsuste tegemiseks.
- Kasutus sõltub eraldi õiguslikust alusest.

Järeldus

Palgaandmete puhul ei ole ühtset „omanikku“. Kontroll on jaotatud:

- isikule (põhiõigused),
- tööandjale (andmete esitamine),
- riigile (töötlemise eesmärk ja kasutus).

1.3.5. Järeldused APA kontekstis

Metoodika rakendamine näitab, et andmete „omandi“ küsimus tuleb APA raamistikus asendada **kontrolli ja vastutuse jaotuse analüüsiga**. See on kriitilise tähtsusega järgmistes aspektides:

- ***once-only* põhimõte:** ei tähenda, et andmete kontroll liigub täielikult riigile, vaid et andmete kasutus peab jääma piiratud eesmärgiga;
- **nõusolekuteenuse rakendamine:** nõusoleku saab anda üksnes ulatuses, milles andmete esitaja või andmesubjekt omab kontrolli;
- **andmete ristkasutus:** sõltub eelkõige vastutava töötleja volitusest ja eesmärgipiirangust, mitte „omandist“.

Kokkuvõttes võimaldab käesolev metoodika määratleda andmete kasutamise õigused ja piirid süsteemselt ning vältida ekslikku eeldust, et andmetel on üksainus omanik. Selline lähenemine on eelduseks õiguspärasele ja toimivale andmepõhisele aruandlusele.

1.4. Primaarse andmekoguja ja sekundaarse kasutaja õiguste ja kohustuste metoodika once-only põhimõtte rakendamisel

Andmepõhise aruandluse ja *once-only* põhimõtte rakendamine eeldab selget rollijaotust andmete esmakogumise ja nende edasise kasutamise vahel. Käesolevas analüüsis eristatakse kahte keskset rolli: **primaarne andmekoguja** (asutus, kes andmed esmakordselt kogub) ning **sekundaarne kasutaja** (asutus, kes kasutab samu andmeid teisese eesmärgi täitmiseks).

Metoodika eesmärk on määratleda nende rollide õigused, kohustused ja vastutus selliselt, et oleks tagatud andmete õiguspärane ristkasutus, põhiõiguste kaitse ning *once-only* põhimõtte tõhus rakendamine.

1. Rollide määratlus

Primaarne andmekoguja on avaliku sektori asutus, kes kogub andmed ettevõtjalt või muult kohustatud isikult esmakordselt seadusest tuleneva ülesande täitmiseks.

Sekundaarne kasutaja on avaliku sektori asutus, kes kasutab primaarse andmekoguja poolt kogutud andmeid oma ülesannete täitmiseks ilma, et ta koguks neid andmeid uuesti ettevõtjalt.

2. Metoodika põhimõtted

Rollide määramisel ja õiguste-kohustuste jaotamisel lähtutakse järgmistest põhimõtetest:

1. **Seaduslikkuse põhimõte** – andmete kogumine ja kasutamine peab tuginema õiguslikule alusele;
2. **Eesmärgipiirangu põhimõte** – andmeid võib kasutada üksnes eesmärkidel, mis on kooskõlas algse kogumise eesmärgiga või milleks on olemas eraldi õiguslik alus;
3. **Proportsionaalsuse põhimõte** – andmete kasutamine peab olema vajalik ja mõõdukas;
4. **Tundlikkusepõhine lähenemine** – õigused ja kohustused sõltuvad andmete tundlikkusest;
5. **Läbipaistvuse ja jälgitavuse põhimõte** – andmete kasutamine peab olema logitav ja kontrollitav.

3. Primaarse andmekoguja õigused ja kohustused

Primaarne andmekoguja vastutab andmete esmakogumise õiguspärasuse ja kvaliteedi eest.

Õigused:

- koguda andmeid seadusest tuleneva ülesande täitmiseks;
- määrata andmete esmane töötlemise eesmärk;
- kehtestada andmete ligipääsupiirangud vastavalt õiguslikule režiimile;

Kohustused:

- kontrollida andmete kogumise **vajalikkust ja proportsionaalsust**;
- tagada andmete **õigsus, ajakohasus ja kvaliteet**;
- määrata iga andmeelemendi:
    - õiguslik alus,
    - töötlemise eesmärk,
    - tundlikkuse kategooria,
    - säilitamistähtaeg;

- tagada andmete **kirjeldatus (metaandmed)** viisil, mis võimaldab nende hilisemat ristkasutust;
- võimaldada andmete kättesaadavus teistele asutustele juhul, kui selleks on õiguslik alus;
- tagada andmete kasutamise **logimine ja jälgitavus**.

4. Sekundaarse kasutaja õigused ja kohustused

Sekundaarne kasutaja vastutab andmete teisese kasutuse õiguspärasuse eest.

Õigused:

- kasutada primaarse andmekoguja kogutud andmeid, kui:
    - selleks on seadusest tulenev õiguslik alus; või
    - see toimub nõusoleku alusel;
- saada andmeid keskse andmejagamise mehhanismi kaudu;

Kohustused:

- kontrollida enne andmete kasutamist:
    - õigusliku aluse olemasolu,
    - eesmärgipiirangu järgimist;
- kasutada andmeid üksnes ulatuses, mis on vajalik konkreetse ülesande täitmiseks;
- järgida andmete tundlikkusest tulenevaid piiranguid;
- tagada andmete kasutamise **läbipaistvus ja logimine**;
- mitte laiendada andmete kasutust uutele eesmärkidele ilma täiendava õigusliku aluseta;

5. Vastutuse jaotuse metoodika

Once-only põhimõtte rakendamisel jaotub vastutus järgmiselt:

- **Primaarne andmekoguja** vastutab:
    - andmete kogumise õiguspärasuse,
    - andmete kvaliteedi,
    - esialgse klassifitseerimise eest;
- **Sekundaarne kasutaja** vastutab:
    - andmete kasutamise õiguspärasuse,
    - eesmärgipiirangu järgimise,
    - konkreetse kasutusjuhtumi proportsionaalsuse eest;
- **Keskne andmejagamise mehhanism (kui olemas)** vastutab:
    - turvalise vahendamise,
    - ligipääsukontrolli,
    - logimise ja jälgitavuse eest.

6. Metoodika rakendamise tulemus

Metoodika võimaldab:

- vältida dubleerivat andmete kogumist;
- tagada selge vastutuse jaotus asutuste vahel;
- rakendada *once-only* põhimõtet kooskõlas andmekaitse ja põhiõigustega;
- luua eeldused automatiseeritud ja turvaliseks andmete ristkasutuseks.

1.4.1. Andmekategooriapõhine õiguste ja kohustuste metoodika

Andmepõhise aruandluse ja *once-only* põhimõtte rakendamisel ei ole primaarse andmekoguja ja sekundaarse kasutaja õigused ja kohustused universaalsed, vaid sõltuvad otseselt andmete liigist, nende tundlikkusest ning kasutuseesmärgist. Seetõttu on vajalik rakendada andmekategooriapõhist metoodikat, mis võimaldab diferentseerida õigusi, kohustusi ja piiranguid vastavalt konkreetse andmekategooria eripäradele.

Metoodika lähtub põhimõttest, et mida suurem on andmete tundlikkus ja potentsiaalne mõju isikute või ettevõtjate õigustele, seda rangemad peavad olema nii andmete kasutamise tingimused kui ka sekundaarse kasutaja kohustused.

1. Andmekategooriate jaotus

Käesolevas analüüsis eristatakse järgmisi peamisi andmekategooriaid:

- identifikaatorid;
- tehingu- ja operatiivandmed (kõrge granulaarsus);
- klassifikaatorid ja metaandmed;
- tuletatud ja koondandmed.

Iga nimetatud kategooria puhul tuleb eraldi hinnata andmete tundlikkust, kasutuseesmärki ning töötlemisega kaasnevaid riske.

2. Õiguste ja kohustuste diferentseerimise põhimõtted

Andmekategooriapõhine metoodika tugineb järgmistele üldpõhimõtetele:

1. **Tundlikkusepõhine diferentseerimine**

Madala tundlikkusega andmete puhul (nt klassifikaatorid) on õigused laiemad ja piirangud minimaalsed, samas kui kõrge tundlikkusega andmete (nt isikuandmed, ärisaladus) puhul kehtivad rangemad kasutus- ja ligipääsupiirangud.

2. **Eesmärgipõhine kasutus**

Sekundaarne kasutaja võib andmeid kasutada üksnes eesmärkidel, mis on kooskõlas algse kogumise eesmärgiga või milleks on olemas eraldi õiguslik alus.

3. **Minimaalsuse põhimõte**

Sekundaarne kasutaja tohib kasutada üksnes neid andmeid ja sellisel granulaarsusel, mis on konkreetse ülesande täitmiseks vajalik.

4. **Vastutuse eristamine**

Primaarne andmekoguja vastutab andmete kvaliteedi ja esmase klassifitseerimise eest, sekundaarne kasutaja aga andmete õiguspärase kasutamise eest.

3. Metoodika rakendamine andmekategooriate lõikes

Identifikaatorid

Identifikaatorite puhul on *once-only* põhimõtte rakendamine üldjuhul täielik. Primaarne andmekoguja peab tagama nende õigsuse ja keskse allika olemasolu, samas kui sekundaarne kasutaja võib neid kasutada laialdaselt tingimusel, et on tagatud nõuetekohane ligipääsukontroll.

Tehingu- ja operatiivandmed

Kõrge granulaarsusega andmete puhul on õigused ja kohustused rangelt piiratud. Primaarne andmekoguja peab tagama andmete täpse klassifitseerimise ja tundlikkuse määramise, samas kui sekundaarne kasutaja peab iga kasutusjuhtumi puhul eraldi hindama õigusliku aluse olemasolu, eesmärgipiirangu järgimist ning vajaduse korral kasutama agregeeritud andmeid.

Klassifikaatorid ja metaandmed

Kuna tegemist on üldjuhul avaliku teabega, on nii primaarse andmekoguja kui ka sekundaarse kasutaja õigused laiad ning piirangud minimaalsed. Peamine kohustus on tagada standardiseeritus ja ühtne kasutus.

Tuletatud ja koondandmed

Nende andmete puhul on võimalik rakendada laiemat ristkasutust, kuid tuleb arvestada, et need võivad mõjutada isikute või ettevõtjate õigusi. Sekundaarne kasutaja peab tagama kasutamise läbipaistvuse ning vajaduse korral selgitama andmete kujunemise aluseid.

4. Metoodika tähendus

Andmekategooriapõhine õiguste ja kohustuste metoodika võimaldab siduda andmete liigi, tundlikkuse ja kasutuseesmärgi konkreetsete õiguslike nõuetega. See loob eeldused diferentseeritud regulatsiooniks, kus *once-only* põhimõtet rakendatakse ulatuses, mis on kooskõlas andmekaitse, eesmärgipiirangu ja proportsionaalsuse põhimõtetega.

Metoodika rakendamine aitab vältida üleregulatsiooni madala riskiga andmete puhul ning samas tagada kõrgema kaitsetaseme tundlike andmete töötlemisel, luues tasakaalu andmete efektiivse kasutamise ja põhiõiguste kaitse vahel.

2. ÕIGUSLIKUD PIIRANGUD

2.1. Põhiseadusest tulenevad piirangud

Andmepõhise aruandluse rakendamisel tuleb arvestada põhiseadusest tulenevate põhiõiguste ja nende riive lubatavuse tingimustega. APA puudutab eeskätt õigust eraelu puutumatusele ja isikuandmete kaitsele (PS § 26, § 43), ettevõtlusvabadust ja omandiõigust (PS § 31, § 32), teabevabadust ja avaliku teabe kättesaadavust (PS § 44), samuti üldist proportsionaalsuse põhimõtet (PS § 11).

Põhiõiguste riive ei ole APA raames välditav, kuna andmete kogumine ja korduvkasutus eeldab paratamatult ettevõtjate ja tihti ka füüsiliste isikute kohta käiva teabe töötlemist. Õiguspäraseks saab seda pidada üksnes juhul, kui riivel on selge ja legitiimne eesmärk, see tugineb seadusele ning on sobiv, vajalik ja mõõdukas võrreldes taotletava eesmärgiga. (vt PS § 11, Riigikohtu praktika proportsionaalsuse testi kohta).

2.1.1. Ettevõtlusvabadus

Lisaks eraelu puutumatusele tuleb APA kavandamisel arvestada ettevõtlusvabaduse ja omandiõigusega. Ettevõtlusvabadus hõlmab mh õigust korraldada oma majandustegevust, kaitsta ärisaladusi ja konfidentsiaalset äriteavet ning prognoosida oma suhetest riigiga tulenevaid kohustusi mõistliku etteaimatavusega. (vt PS § 31, § 32)

Andmepõhine aruandlus puudutab ettevõtlusvabadust kahel tasandil:

1. **Andmete esitamise kohustus ja halduskoormus**

Iga uus aruandlus- või andmekogumiskohustus kujutab endast ettevõtjale koormust ja võib piirata ettevõtlusvabadust, kui sellest tulenevad kulud või riskid ei ole proportsionaalsed taotletava avaliku huviga. APA eesmärk on küll halduskoormust vähendada, kuid praktikas võib andmekorralduse muutmine tekitada üleminekuperioodil täiendavat koormust. Seetõttu tuleb iga uue APA-lahenduse puhul hinnata, kas:

- andmete kogumine on sisuliselt vajalik (minimaalsuse põhimõte);
- sama eesmärki ei saa saavutada ettevõtjat vähem koormavate vahenditega;
- koormus on põhjendatud, arvestades ettevõtja suurust ja tegevusala (nt VKE-de eripära). (vt PS § 31, § 11)

2. **Ärisaladus ja tundlik äriteave**

Ettevõtjate esitatud andmed sisaldavad sageli ärisaladust või teavet, mille avalikustamine või liiga lai andmejagamine võib kahjustada nende konkurentsipositsiooni (nt tootmismahud, hinnastamine, kliendistruktuur, palgastatistika teatud detailis). Ärisaladuse kaitse tuleneb nii põhiseaduslikust omandi- ja ettevõtlusvabadusest kui ka seadustest (nt äriseadustik, konkurentsiõigus, AvTS ärisaladuse normid). (vt PS § 31, § 32, AvTS ärisaladuse regulatsioon)

APA ja *once-only* põhimõtte rakendamisel ei tohi ärisaladuse kaitse „lahjeneda“ pelgalt seetõttu, et andmed liiguvad automaatselt mitme asutuse vahel. Kui andmeid kogutakse ühel konkreetsel eesmärgil, ei tohi neid ilma selge uue õigusliku aluseta ja proportsionaalsusanalüüsita kasutada teistel eesmärkidel, mis võivad ettevõtjat oluliselt kahjustada (nt andmete kasutamine teises valdkonnas järelevalve prioriteetide muutmiseks, riskiprofiilide loomiseks, millel on ettevõtja jaoks olulised majanduslikud tagajärjed).

Põhiseaduslikust proportsionaalsuse nõudest tulenevad APA jaoks eelkõige järgmised piirangud:

3. **Selge volitusnorm ja eesmärgipiirang**

Andmete kogumise ja korduvkasutuse tingimused peavad tulenema seadusest. Seadus peab andma selge volituse nii andmete kogumiseks kui ka nende andmete kasutamiseks konkreetsetel eesmärkidel. Ebamäärased volitused, mis lubavad „andmete kasutamist kõigi avalike ülesannete täitmiseks", ei ole proportsionaalsuse seisukohalt vastuvõetavad. (vt PS § 3, § 11, § 31)

4. **Eesmärgiga kooskõlas korduvkasutus**

Once-only põhimõte ei tohi muutuda üldiseks „once-collected, forever-used" loogikaks. Andmete korduvkasutus peab jääma kooskõlla algse või selgelt sätestatud teisese eesmärgiga; kui APA raames soovitakse andmeid kasutada uutel eesmärkidel, on vaja kas uut seaduslikku alust või selgelt piiritletud teisese kasutuse normi, mis läbib põhiseaduslikku proportsionaalsustesti.

5. **Ettevõtjate võrdne kohtlemine ja õiguspärane ootus**

APA lahendused ei tohi viia selleni, et üksikute sektorite või ettevõtjate gruppide suhtes tekivad ebaproportsionaalsed aruandluskoormused või järelevalveriskid võrreldes teistega, ilma et selleks oleks objektiivset ja põhjendatud alust. Samuti peavad andmekorralduse muudatused olema piisavalt etteaimatavad, et ettevõtja saaks oma tegevust ja investeeringuid vastavalt planeerida. (vt PS § 12, § 31)

Kokkuvõttes seab põhiseadus APA rakendamisele kahepoolsed piirid: ühelt poolt tuleb vältida ülemäärast sekkumist eraellu ja andmekaitsegarantiide õõnestamist (sh superandmebaasi keelu rikkumist), teiselt poolt ei tohi andmepõhine aruandlus muuta ettevõtlusvabaduse kasutamist tarbetult keerukaks või ebavõrdseks. APA õigusraamistik peab seetõttu olema üles ehitatud põhiõiguste kaitse ja proportsionaalsuse loogikast, mitte üksnes tehnoloogilisest teostatavusest lähtuvalt.

2.1.2. Superandmebaasi keeld

Eesti õiguskorras ei ole lubatud luua nn superandmebaasi, kuhu koondataks kõik isikuandmed või valdav osa neist ühte kesksesse andmekogusse. Selline lahendus tooks kaasa kvalitatiivselt uue taseme eraelu ja isikuandmete kaitse riives ning oleks raskesti ühitav põhiseadusliku proportsionaalsuse nõudega (PS § 11, § 26, § 43). Superandmebaasi keeld ei välista mitmest andmekogust pärit andmete ajutist koondamist konkreetse uuringu või analüüsi tarbeks, kui selleks on selge õiguslik alus ja piiratud eesmärk, kuid välistab püsiva üldotstarbelise „kõike ühendava" andmekogu loomise.

Sama põhimõte kehtib ka keskse andmejagamise platvormi kujundamisel: platvorm peab vahendama eesmärgipõhiseid päringuid eri andmekogudesse, mitte koondama kõik andmed ise püsivasse ühtsesse andmebaasi.

2.2. Andmete kasutamise piirangud süüteomenetluse eesmärgil

Õiguskaitsedirektiivi[36] artikli 2 lõike 1 ja artikli 1 lõike 1 kohaselt on selle kohaldumise materiaalseks kriteeriumiks, et isikuandmete töötlemine toimub "*süütegude tõkestamiseks, uurimiseks, avastamiseks,*

[36] 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. - ELT L 119, lk 89.

nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks".[37] Nähtub, et muuhulgas saab materiaalseks kriteeriumiks olla, et isikuandmeid töödeldakse (i) "süütegude tõkestamiseks" või (ii) "avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja ohtude ennetamiseks". Lähtudes analüüsi eesmärgist, on küsimuseks, mida hõlmab "süütegude tõkestamine" ja "avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja ohtude ennetamine".

Terminil "süütegude tõkestamine" on kaks elementi - süütegu ning tõkestamine.[38] Ükski õiguskaitsedirektiivi norm ei defineeri, mis on süütegu direktiivi tähenduses. Euroopa Komisjoni ekspertide grupp leidis, et iga liikmesriik võib lähtuda liikmesriigi õiguses sätestatud süütegude regulatsioonist.[39] Samuti ei defineeri õiguskaitsedirektiiv terminit tõkestamine. Õiguskirjanduses selgitatakse, et kui süütegude uurimine, avastamine, nende eest vastutusele võtmine ja karistuse täitmisele pööramine on seotud süütegudega, mis on juba toimunud, siis süütegude tõkestamine seondub selliste süütegudega, mis ei ole veel toimunud. Süütegude tõkestamine võib hõlmata väga erinevaid avaliku võimu tegevusi. Kindlasti on tõkestamisena käsitletavad erinevad "ennustavad politseitehnoloogiad", mille kasutamisega kaasnevad väga tõsised andmekaitse küsimused. Kuna liikmesriigid kasutavad süütegude tõkestamiseks väga erinevaid meetodeid, on termin "tõkestamine" üks ebaselgemaid õiguskaitsedirektiivi mõisteid.[40]

Termin "avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja ohtude ennetamine" on tähenduselt veel laiem, kui "süütegude tõkestamine". Tõlgendamisel tuleb arvestada õiguskaitsedirektiivi preambula punktiga 12, mis ütleb, et direktiivi reguleerimisalasse langeb tegevus, mis hõlmab *ka avaliku korra säilitamist /…/, et vajaduse korral kaitsta avalikku julgeolekut ja seadusega kaitstavaid ühiskonna põhihuve selliste ohtude eest ja hoida ära selliste ohtude teke avalikule julgeolekule ja seadusega kaitstavatele ühiskonna põhihuvidele, mis võivad viia süüteo toimepanemiseni*. Õiguskirjanduses juhitakse tähelepanu, et kirjeldatud avaliku võimu tegevus ei pea enam seonduma süütegudega. Seega hõlmab ohtude eest kaitsmine ja ohtude ennetamine märksa rohkemaid tegevusi, kui pelgalt süütegude tõkestamine.[41] Terminit "avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja ohtude ennetamine" on seetõttu palju kritiseeritud. Suurimad Euroopa andmekaitse institutsioonid, nagu näiteks *European Data Protection Supervisor* ja *WP29*, olid vastu sellele, et vaatlusalune termin üldse õiguskaitsedirektiivi lisatakse. Toodi esile, et "avalik julgeolek" on nii lai mõiste, et see hõlmab osades liikmesriikides ka rahvatervist ning toiduohutust.[42] Kokkuvõttes võimaldab hetkel kehtiv regulatsioon ning selle tõlgendused igal liikmesriigil ise määratleda, millised tegevused on selles liikmesriigis käsitletavad "avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja ohtude ennetamisena".

Tehnoloogilised lahendused võimaldavad süütegusid uurida ja ennetada efektiivsemalt. Samas ei tohi uute tehnoloogiate ja funktsioonide kasutamine olla vastuolus kehtiva õiguse ja õigusriigi toimise

---

[37] Brewczyńska, M. A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation. – Research handbook on EU data protection law. Cheltenham: Edward Elgar Publishing Ltd 2022, lk 108.
[38] *Ibid.*, lk 108-110.
[39] Commission Expert Group. Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (4 May 2017). Para 1.
[40] Brewczyńska, M, lk 111-112.
[41] Brewczyńska, M, lk 112.
[42] Vogiatzoglou, P., Fantin, S. National and public security within and beyond the Police Directive. - Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. Cambridge, Antwerp, Chicago: Intersentia, 2019. Lk 31.

seisukohalt oluliste printsiipidega. Järelevalvemenetlus, haldusmenetlus ning süütegude uurimine peab toimuma vastavalt kehtivale õigusele. Iga uue tehnoloogia, funktsiooni või töömeetodi kasutuselevõtule peab eelnema mõjuhinnang ja õigusanalüüs hindamaks kehtiva õiguse asjakohasust ning võimalike põhiõiguste riivet. Massiline andmete analüüs ning automatiseeritud otsused süütegude ennetamise eesmärgil on nõnda suure põhiõiguste riivega, et sellise tegevuse lubatavust tuleb reeglina eitada.

Lisaks konkreetsetele õiguslikele piirangutele (nt põhiseaduslikud ja süüteomenetlusega seotud piirangud) kujundavad andmete töötlemise lubatavust ka töötlemistoimingute lõikes kehtivad üldised nõuded.

APA ja once-only põhimõtet ei saa süüteomenetluse ega avalikku julgeolekut puudutavate tegevuste puhul rakendada samal kujul nagu tavapärase haldus- või statistikatöötluse puhul. See tähendab eelkõige, et:

(i) süüteomenetluse või õiguskaitsedirektiivi reguleerimisalasse kuuluva tegevuse jaoks vajalikke andmeid ei tohi automaatselt ja üldistavalt „sisse kirjutada" APA tavapärasesse andmevahetusrežiimi;

(ii) massilist andmete ristkasutust ja profileerimist süütegude ennetamise eesmärgil tuleb käsitada erandlikult ja seda saab lubada üksnes selges seaduslikus raamistikus, mis läbib range põhiseadusliku proportsionaalsustesti;

(iii) *once-only* tehniline lahendus ei tohi viia olukorrani, kus süüteomenetluse või julgeolekuga seotud andmete kasutusala laieneb märkamatult, ilma et seda oleks seadusandlikult otsustatud ja läbipaistvalt põhjendatud.

Seega peab APA õigusraamistik süüteomenetluse ja avaliku julgeoleku valdkonnas ette nägema rangemad erisätted ja piirangud kui tavapärase haldusandmete korduvkasutuse puhul, vältimaks õigusriigi põhialuste ja põhiõiguste ebaproportsionaalset riivet.

2.3. Andmete töötlemistoimingute lõikes kehtivad piirangud

Käesoleva õigusanalüüsi raames on andmete töötlemisega seotud piirangud tuvastatud nii andmetüüpide, tundlikkuse kui ka töötlemistoimingute lõikes. Analüüs näitab, et andmete töötlemisele kehtivad piirangud ei tulene üksnes andmete liigist, vaid ka konkreetsest töötlemistoimingust (nt kogumine, säilitamine, edastamine), millele kohaldatakse erinevaid õiguslikke nõudeid. Seetõttu on APA rakendamisel vajalik käsitleda andmete töötlemist toimingupõhiselt.

Alljärgnev koondvaade toob välja peamised töötlemistoimingud ning nendega seotud õiguslikud piirangud.

Tabel nr 7. Töötlustoimingute ja õiguslike piirangute koondvaade

Töötlemistoimingud	Peamised piirangud ja nõuded
Andmete kogumine (vastuvõtmine)	Nõuab selget õiguslikku alust; kohaldub minimaalsuse ja proportsionaalsuse põhimõte; keelatud on dubleeriv kogumine, kui andmed on juba riigi valduses (*once-only* põhimõte).
Andmete salvestamine ja säilitamine	Tuleb määrata säilitamistähtaeg; andmeid ei tohi säilitada kauem kui vajalik; kohustus tagada andmete turvalisus ja terviklus.

Andmete kasutamine ja analüüs	Piiratud eesmärgipiirangu põhimõttega; andmeid ei tohi kasutada uuel eesmärgil ilma õigusliku aluseta; automatiseeritud otsuste puhul täiendavad nõuded (nt mõju isikule).
Andmete edastamine ja jagamine	Nõuab eraldi õiguslikku alust (seadus või nõusolek); kohaldatakse konfidentsiaalsuspiiranguid (nt isikuandmed, ärisaladus, maksusaladus); tuleb tagada ligipääsukontroll ja logimine.
Andmete avalikustamine	Lubatav üksnes avaliku teabe puhul; juurdepääsupiiranguga andmeid ei tohi avalikustada; tuleb hinnata avalikustamise mõju.
Andmete muutmine ja parandamine	Kohustus tagada andmete õigsus ja ajakohasus; muudatused peavad olema jälgitavad.
Andmete kustutamine või piiramine	Kohustus kustutada andmed säilitamistähtaja möödumisel; kustutamine ei ole lubatud, kui seadus nõuab säilitamist; tuleb tagada turvaline kustutamine.
Juurdepääsu võimaldamine	Tuleb lähtuda rollipõhisest ligipääsust; juurdepääs peab olema põhjendatud ja dokumenteeritud; andmete kasutamine peab olema jälgitav.

Analüüsi põhjal saab järeldada, et kõige rangemad piirangud kehtivad andmete kogumisele ja edastamisele, kuna need kujutavad endast andmete töötlemise kriitilisi etappe, kus määratakse andmete õiguspärasus ja kasutusulatus. Samas mõjutavad andmete säilitamine, analüüs ja kustutamine eelkõige andmete elutsükli hilisemaid etappe ning on seotud andmete kvaliteedi, turvalisuse ja põhiõiguste kaitsega.

APA rakendamise seisukohalt tähendab see, et *once-only* põhimõtte elluviimine ei sõltu üksnes andmete olemasolust, vaid ka sellest, millises töötlemisetapis ja millistel tingimustel andmeid kasutatakse. Seetõttu tuleb andmete ristkasutuse lubatavust hinnata alati koos konkreetse töötlemistoiminguga, arvestades nii andmete tundlikkust kui ka õiguslikku alust.

Eeltoodud töötlemistoimingute lõikes kehtivad piirangud loovad aluse andmete kasutamise õiguspärasuse hindamiseks. Nende piirangute praktiliseks rakendamiseks on vajalik täiendav metoodika, mis võimaldab otsustada, millistel juhtudel on andmete jagamine kohustuslik, lubatav või välistatud.

Andmete edastamisel ettevõtjalt riigile võib sõltuvalt õigusaktist olla nõutav andmete esitaja elektrooniline tuvastamine, eelkõige e-identimise ja usaldusteenuste määruse (eIDAS) ning riigisiseste autentimislahenduste alusel. Tuvastamise nõue sõltub andmete tundlikkusest ja kasutuseesmärgist ning on rangem eelkõige juhtudel, kus andmetel on õiguslikud tagajärjed.

2.4. Andmete jagamisest keeldumise ja kohustuslikkuse metoodika

Andmepõhise aruandluse ja *once-only* põhimõtte rakendamisel on keskseks küsimuseks, millistel juhtudel on andmete jagamine asutuste vahel kohustuslik, millal lubatav ning millal tuleb sellest keelduda. Käesolevas analüüsis on välja töötatud metoodika, mis võimaldab hinnata andmete jagamise õiguspärasust lähtudes andmete liigist, tundlikkusest, kasutuseesmärgist ning töötlemisega kaasnevatest riskidest.

Metoodika lähtub põhimõttest, et andmete jagamine ei ole eesmärk omaette, vaid peab olema õigustatud konkreetse avaliku ülesande täitmiseks ning kooskõlas seaduslikkuse, eesmärgipiirangu ja proportsionaalsuse põhimõtetega.

1. Otsustusmudel

Andmete jagamise lubatavus jaguneb kolme kategooriasse:

1.1. Kohustuslik jagamine

Andmete jagamine on kohustuslik, kui:

- teisel asutusel on **selge seadusest tulenev õiguslik alus** andmete kasutamiseks;
- andmete kasutus on **kooskõlas algse kogumise eesmärgiga** või seadus võimaldab teisest kasutust;
- andmete jagamine on **vajalik avaliku ülesande täitmiseks**;
- puuduvad õiguslikud piirangud, mis välistaksid jagamise.

Sellisel juhul ei tohi primaarne andmekoguja andmete jagamisest keelduda.

1.2. Tingimuslik jagamine

Andmete jagamine on lubatav tingimuslikult, kui:

- õiguslik alus on olemas, kuid andmed on **kõrge tundlikkusega** (nt isikuandmed, ärisaladus);
- on vajalik hinnata:
    - eesmärgipiirangu järgimist,
    - proportsionaalsust,
    - andmete minimaalsust (nt kas piisab agregeeritud andmetest);
- rakendatakse täiendavaid meetmeid, näiteks:
    - ligipääsupiirangud,
    - pseudonümiseerimine või agregeerimine,
    - nõusolekupõhine jagamine.

Sellisel juhul tuleb iga jagamisjuhtumit eraldi hinnata.

1.3. Keelatud jagamine (keeldumise kohustus)

Andmete jagamisest tuleb keelduda, kui:

- puudub **õiguslik alus** andmete teisese kasutuse jaoks;
- andmete kasutamine oleks vastuolus **eesmärgipiirangu põhimõttega**;
- andmete jagamine tooks kaasa **ebaproportsionaalse riive** isikute või ettevõtjate õigustele;
- andmed sisaldavad **konfidentsiaalset teavet**, mille jagamine ei ole seadusega lubatud (nt ärisaladus, maksusaladus);
- andmete kasutamise eesmärk ei ole piisavalt selgelt määratletud.

Sellisel juhul on primaarne andmekoguja kohustatud andmete jagamisest keelduma.

2. Metoodika rakendamise kriteeriumid

Andmete jagamise lubatavuse hindamisel tuleb arvestada järgmisi kriteeriume:

1. Andmete kategooria ja tundlikkus

   – mida tundlikumad andmed, seda rangemad on jagamise tingimused;

2. Kasutuse eesmärk

   – kas andmete kasutus on seotud avaliku ülesandega ning kooskõlas algse eesmärgiga;

3. Granulaarsus

   – kas eesmärgi saavutamiseks on vajalik detailandmete jagamine või piisab koondandmetest;

4. Õiguslik alus

   – kas andmete jagamine tuleneb seadusest, on lubatud nõusoleku alusel või puudub alus;

5. Riskitase

   – kas andmete jagamine võib kaasa tuua põhiõiguste riive või konfidentsiaalsuse rikkumise.

3. Metoodika tähendus

Metoodika võimaldab luua selge otsustusraamistiku, mille alusel avaliku sektori asutused saavad hinnata andmete jagamise lubatavust ja kohustuslikkust. See aitab vältida nii põhjendamatut andmete kinnihoidmist kui ka õigusvastast andmete jagamist, tagades tasakaalu andmete tõhusa kasutamise ja põhiõiguste kaitse vahel.

Metoodika toetab *once-only* põhimõtte rakendamist, kuna võimaldab selgelt eristada olukordi, kus andmete ristkasutus on kohustuslik, ning olukordi, kus see peab olema piiratud või välistatud.

2.5. Metoodika andmete jagamiseks piiratud õigusraamistikus

Andmepõhise aruandluse rakendamisel esineb sageli olukordi, kus andmete jagamiseks puudub otsene ja selgesõnaline õiguslik alus, kuid andmete kasutamine võiks olla põhjendatud avaliku ülesande täitmiseks või halduskoormuse vähendamiseks. Sellistes olukordades on vajalik metoodika, mis võimaldab hinnata andmete jagamise lubatavust piiratud õigusraamistiku tingimustes.

Käesolev metoodika lähtub astmelisest otsustusloogikast, mille eesmärk on tagada, et andmete jagamine toimub üksnes siis, kui see on õiguslikult põhjendatud ning kooskõlas andmekaitse, eesmärgipiirangu ja proportsionaalsuse põhimõtetega.

1. Otsustusloogika

Andmete jagamise lubatavust hinnatakse järgmise järjestikuse loogika alusel:

1.1. Otsene õiguslik alus

Esmalt tuleb hinnata, kas andmete jagamiseks on olemas otsene seadusest tulenev õiguslik alus.

- Kui jah → andmete jagamine on lubatud, eeldusel et järgitakse kehtivaid piiranguid (nt eesmärgipiirang, minimaalsus, turvameetmed);
- Kui ei → liikuda järgmise sammu juurde.

1.2. Anonümiseerimine või agregeerimine

Kui otsene õiguslik alus puudub, tuleb hinnata, kas andmeid on võimalik töödelda viisil, mis vähendab nende tundlikkust.

- Kui andmeid saab **anonümiseerida või agregeerida** selliselt, et andmesubjekti ei ole enam võimalik tuvastada → andmete jagamine on lubatud tingimuslikult;
- Kui see ei ole võimalik → liikuda järgmise sammu juurde.

1.3. Nõusolekupõhine jagamine

Järgmise sammuna tuleb hinnata, kas andmete jagamine on võimalik andmete omaniku nõusoleku alusel.

- Kui on võimalik saada **teadlik, vabatahtlik ja konkreetne nõusolek** → andmete jagamine on lubatud piiratud ulatuses;
- Kui nõusolekut ei ole võimalik kasutada → liikuda järgmise sammu juurde.

1.4. Jagamise keeld

Kui puudub nii otsene õiguslik alus, anonümiseerimise võimalus kui ka nõusolek, ei ole andmete jagamine lubatav.

Sellisel juhul tuleb:

- kas koguda vajalikud andmed eraldi õigusliku aluse alusel;
- või loobuda andmete kasutamisest vastaval eesmärgil.

2. Metoodika rakendamise piirid

Metoodika rakendamisel tuleb arvestada järgmisi piiranguid:

- **Eesmärgipiirang** – andmeid ei tohi kasutada eesmärkidel, mis ei ole kooskõlas algse kogumise eesmärgiga;
- **Andmete tundlikkus** – kõrgema tundlikkusega andmete puhul (nt isikuandmed, ärisaladus) on anonümiseerimise ja nõusoleku kasutamine piiratud;
- **Proportsionaalsus** – andmete jagamine peab olema vajalik ja mõõdukas;
- **Tõlgendusvastutus** – andmete kasutamise vastutus jääb jagavale ja kasutavale asutusele.

3. Metoodika tähendus

Käesolev metoodika võimaldab rakendada paindlikku, kuid õiguspärast lähenemist olukordades, kus andmete jagamiseks puudub otsene õiguslik alus. See aitab vältida nii põhjendamatut andmete kasutamist kui ka olukordi, kus andmete kasutamine jääb ebamõistlikult piiratuks üksnes formaalse õigusliku aluse puudumise tõttu.

Metoodika toetab *once-only* põhimõtte rakendamist ning võimaldab vähendada ettevõtjate halduskoormust, säilitades samal ajal andmekaitse ja põhiõiguste kaitse kõrge taseme.

3. ANDMETE OLEMUS

3.1. Andmete jaotus struktureerituse alusel

3.1.1. Struktureeritud andmed

Andmepõhise aruandluse keskmes on üleminek dokumendipõhiselt suhtluselt andmepõhisele. Selle protsessi edukus sõltub sellest, mil määral on andmed esitatud struktureeritud kujul. Struktureeritud andmed on informatsioon, mis on esitatud kindla formaadi ja andmestruktuuri alusel ning on seetõttu masintöödeldav. Struktureeritud andmete olemasolu on eelduseks automatiseeritud API-põhisele (rakendusliidese kaudu toimuvale) andmevahetusele ettevõtja infosüsteemide ja riiklike infosüsteemide vahel.

APA kontekstis hõlmavad struktureeritud andmed eeskätt majandustegevuse käigus tekkivaid standardiseeritavaid andmevälju. Tüüpilised näited on:

- Identifikaatorid. Näiteks registrikood või isikukood, mis võimaldavad andmeid üheselt subjektiga siduda;
- Finantsnäitajad. Näiteks brutopalk või arve kogusumma, mis on aluseks maksuarvestusele ja statistikale;
- Mõõdetavad kogused. Näiteks kütusekogus liitrites või töötundide arv.

Õiguslikust vaatepunktist on struktureeritud andmete ristkasutus ja korduvkasutus (*once-only*) oluliselt lihtsam mitmel põhjusel.

Esiteks tagavad struktureeritud andmed üheselt mõistetava semantilise tähenduse. Erinevalt vaba tekstist on struktureeritud andmeväljade sisu täpselt defineeritud, näiteks taksonoomiate, riiklike klassifikaatorite või muude andmemudelite abil. See vähendab riski, et erinevad ametiasutused tõlgendavad sama andmevälja erinevalt, ning suurendab andmete õiguslikku usaldusväärsust.

Teiseks võimaldab struktureeritud andmete selge sisu paremini hinnata andmete töötlemise eesmärgipärasust. Kuna andmevälja tähendus on määratletud, on andmekaitseõiguse seisukohalt lihtsam hinnata, kas andmete jagamine teise asutusega on kooskõlas algse kogumise eesmärgiga.

Kolmandaks võimaldavad struktureeritud andmed kasutada metaandmeid, mis kirjeldavad andmete päritolu, ajakohasust, tundlikkuse taset ja ligipääsupiiranguid. See on kooskõlas ettevalmistatava Avaliku teabe seaduse (AvTS) muutmise väljatöötamiskavatsusega (VTK), mille eesmärk on parandada riigi andmete leitavust ja kvaliteetseid andmekirjeldusi. Metaandmete olemasolu võimaldab rakendada ka nõusolekupõhiseid andmejagamise lahendusi, kus ettevõtja saab määrata, millistele andmeväljadele kolmandatel isikutel on ligipääs.

Neljandaks võimaldavad struktureeritud andmed kontrollida andmete granulaarsust. Riik saab juriidiliselt piirata ligipääsu detailsetele tehinguandmetele, võimaldades korduvkasutust vaid agregeeritud tasemel. Selline lähenemine aitab kaitsta ettevõtjate ärisaladusi ja vähendada liigse andmejagamise riski.

Kokkuvõttes on andmete struktureerimine üks keskseid eeldusi andmepõhise aruandluse rakendamiseks. Struktureeritud andmete kasutamine võimaldab vähendada aruandlusest tulenevat halduskoormust, toetab automatiseeritud andmevahetust ning aitab tagada andmete õigusselguse ja turvalise kasutamise.

3.1.2. *Struktureerimata andmed*

Eelmises alapeatükis käsitletud struktureeritud andmed moodustavad andmepõhise aruandluse tehnilise ja õigusliku vundamendi. Praktikas ei koosne riigile esitatav teave siiski üksnes standardiseeritud andmeväljadest. Oluline osa teabest esitatakse jätkuvalt struktureerimata kujul, st dokumentide või tekstina, mille sisu ei ole jagatud masinloetavateks andmeväljadeks ning mille tõlgendamine eeldab inimlikku hinnangut.

Struktureerimata andmed on seega teave, mis on esitatud vabas vormis ning mille sisu ei ole eelnevalt standardiseeritud andmestruktuuride või klassifikaatorite kaudu. Sellised andmed on küll digitaalsed, kuid ei ole automaatselt masintöödeldavad samal viisil nagu struktureeritud andmeväljad.

APA kontekstis on tüüpilised näited struktureerimata andmetest järgmised:

- Selgitavad dokumendid. Seletuskirjad, tegevusaruannete tekstilised osad ja arengukavad;
- Eksperthinnangud. Keskkonnamõjude hindamised, auditid ja tehnilised lisadokumendid;
- Vabatekstilised märkused. Majandustarkvara või aruandlusvormide selgitavad tekstid, mis kirjeldavad tehingute sisu või erisusi.

Erinevalt struktureeritud andmetest rakendub ühekordse küsimise (*once-only*) põhimõte struktureerimata andmete puhul piiratumalt ning teistsuguse metoodika alusel. Selle põhjuseks on mitmed tehnilised ja õiguslikud asjaolud.

Esiteks on struktureerimata andmete automaatne masintöötlus piiratud. Kuna sisu on esitatud vaba tekstina, ei suuda infosüsteemid seda ilma täiendavate tekstitöötluse või analüüsimeetoditeta automaatselt töödelda ega siduda teiste asutuste andmevajadustega. Seetõttu ei toimu struktureerimata andmete ristkasutus tavaliselt üksikute andmeväljade tasemel, vaid pigem dokumendi tasemel.

Teiseks on struktureerimata andmete puhul keerulisem hinnata andmete töötlemise eesmärgipärasust. Isikuandmete kaitse üldmääruse kohaselt peab andmete töötlemise eesmärk olema selgelt määratletud. Vaba teksti puhul ei ole aga alati võimalik ette näha, milliseid andmeid dokument sisaldab, mistõttu võib sama dokument sisaldada mitut erinevat andmeliiki ja eesmärki. See muudab asutustevahelise automaatse ristkasutuse õiguslikult keerukamaks.

Kolmandaks kaasneb struktureerimata dokumentidega suurem konfidentsiaalsus- ja ärisaladuse risk. Sellised dokumendid võivad sisaldada etteaimamatuid või kõrvalisi andmeid, näiteks kirjeldusi ettevõtte äriprotsessidest, koostööpartneritest või tehnoloogilistest lahendustest. Automaatne ja ulatuslik jagamine võib seetõttu suurendada riski, et konfidentsiaalne teave jõuab asutusteni, kellel puudub selle kasutamiseks tegelik vajadus.

Metoodiline lahendus ehk leitavusepõhine *once-only*

Eeltoodud piirangute tõttu ei rakendata struktureerimata andmete puhul APA raamistikus tavaliselt automatiseeritud andmevoogu, vaid nn leitavusepõhist andmete korduvkasutust. Selle mudeli eesmärk ei ole struktureerimata dokumentide automaatne levitamine, vaid nende olemasolu tuvastatavus ja vajaduse korral kontrollitud jagamine.

Selline lähenemine tugineb eelkõige kolmele sambale.

Esiteks tuleb struktureerimata dokumendid varustada masinloetavate metaandmetega, mis kirjeldavad dokumendi liiki, päritolu, ajaperioodi ja valdkonda. See võimaldab teistel asutustel tuvastada, et vajalik dokument on olemas, ilma et nad peaksid kohe ligipääsu selle sisule.

Teiseks toimub dokumentide jagamine pöörduspõhiselt. See tähendab, et teine asutus küsib õigusliku aluse olemasolul ligipääsu konkreetsele dokumendile esmaselt andmekogujalt, selle asemel et dokument liiguks automaatselt kõigi potentsiaalsete kasutajate vahel.

Kolmandaks tagatakse andmete kasutamise läbipaistvus andmete teabevärava ja nõusolekuteenuste kaudu, mille arendamist näeb ette avaliku teabe seaduse muutmise väljatöötamiskavatsus (VTK). Sellised lahendused võimaldavad ettevõtjal saada ülevaate, milliseid tema esitatud dokumente on erinevad asutused kasutanud.

Kokkuvõte

Struktureerimata andmete puhul ei seisne andmepõhise aruandluse eesmärk niivõrd andmete täielikus automatiseerimises, vaid dokumentide korduva küsimise vältimises. Selle saavutamiseks tuleb luua turvaline ja metaandmetel põhinev asutustevaheline jagamiskeskkond, mis võimaldab dokumentide olemasolu tuvastada ja vajaduse korral kontrollitud viisil jagada. Selline lähenemine asendab järk-järgult seni levinud e-kirja teel toimuvat dokumentide edastamist ning loob eelduse struktureerimata teabe tõhusamaks ja läbipaistvamaks kasutamiseks avalikus sektoris.

3.2. APA-spetsiifiline andmetüüpide kaardistus

Andmepõhise aruandluse rakendamine eeldab, et erinevaid andmeid ei käsitleta ühtse massina, vaid nende õiguslikke ja tehnilisi eripärasid arvestades diferentseeritult. Selleks on vajalik andmetüüpide süsteemne kaardistus, mis võimaldab hinnata nii andmete õiguslikku režiimi, nendega seotud riske kui ka nende sobivust *once-only* põhimõtte rakendamiseks.

Käesolevas peatükis esitatud kaardistus lähtub eeldusest, et andmete ristkasutuse võimalikkus sõltub kolmest omavahel seotud tegurist: andmete olemusest, nende õiguslikust kvalifikatsioonist ning nende töötlemisega kaasnevast riskist. Seetõttu on iga andmetüübi puhul eraldi hinnatud (i) õiguslik režiim, (ii) peamised piirangud ja riskid, (iii) sobivus *once-only* põhimõtte rakendamiseks ning (iv) vajalikud normitehnilised lahendused.

Oluline on rõhutada, et tabel ei käsitle andmetüüpe üksnes kirjeldavalt, vaid toimib analüütilise tööriistana. Selle eesmärk on näidata, millistel juhtudel on andmete ristkasutus koheselt võimalik, millistel juhtudel eeldab see täiendavaid õiguslikke tagatisi ning millistel juhtudel ei ole see ilma seadusandliku sekkumiseta põhjendatud. Selline lähenemine loob aluse diferentseeritud regulatsiooniks, mis võimaldab ühtaegu toetada andmete tõhusat kasutamist ning tagada põhiõiguste kaitse.

Alljärgnevas tabelis on esitatud APA kontekstis kesksemad andmetüübid koos nende õiguslike ja regulatiivsete tunnustega.

Tabel nr 8. Kesksed andmetüübid koos nende õiguslike ja regulatiivsete tunnustega

Nr	Tüüp	Näited	Õiguslik režiim	Piirangud	*Once-only* sobivus	Piirangud (*once-only kontekstis*)	Normitehniline soovitus
1.	**Identifikaatorid**	Näited: • registrikood • isikukood • kinnistu tunnus (nt katastritunnus)	• Kui seostatav füüsilise isikuga → isikuandmed • Kui juriidilise isikuga → mitte-isikuandmed (siiski tuleb arvestada teatud eranditega)	• identiteedivarguse risk, • vale seostamise risk.	Väga kõrge — identifikaatorid on põhiandmed	• järelevalverisk, • konkurentsirisk, • sanktsioonimõju	Seaduses tuleb sätestada identifikaatorite keskallika põhimõte
2.	**Tehingu- ja operatiivandmed (kõrge granulaarsus)**	• palgaväljamaksed • müügitehingud • kütuseostud	• isikuandmed • maksusaladus • ärisaladus	• minimaalsuse põhimõte (ei tohi koguda rohkem, kui eesmärgiks vajalik) • eesmärgipiirang (algne kogumise eesmärk seab ranged piirid teisesele kasutusele) • konfidentsiaalsus (ärisaladus,	Tingimuslik — vajab: • õiguslikku alust • turvameetmeid • eesmärgipiirangu lahendust	• Järelevalverisk • konkurentsirisk • sanktsioonimõju • suur andmemahu ja detailisuse tõttu kõrgem väärkasutuse risk • süüteomenetluse / järelevalve „funktsioonide	Seada seaduses eraldi reeglid tehinguandmete teisese kasutuse ja väärindatud kasutuse kohta (vt näited § 43[8], § 43[9]) Nõuda tehinguandmete käsitlemist kõrgema tundlikkuse kategooriana (nt T3–T4) ning siduda nende korduvkasutus

				maksusaladus, isikuandmete eriliigid) • säilitustähtaeg peab olema selgelt määratletud		hiiliv laienemine“ (*function creep*) • profileerimis- ja diskrimineerimisriskid, kui kasutatakse riskiskooride loomiseks	kohustusliku mõjuhindamisega
3.	**Klassifikaatorid ja metaandmed**	Klassifikaatorid kirjeldavad teisi andmeid. Näited: • EMTAK • valuutakood • mõõtühikud	Üldjuhul avalik teave.	• üldjuhul madal tundlikkus, kuid • valede või ebaühtlaste klassifikaatorite kasutamisel tekib andmete tõlgendusrisk • metaandmed võivad kaudselt paljastada tundliku teabe (nt skeemid, mida saab kombineerida muude andmetega)	Täielik	• risk, et erinevad asutused kasutavad eri versioone klassifikaatoritest (versioonihaldus) • semantilise mittekoosvõime risk (kui metaandmete struktuurid erinevad)	• kehtestada seaduses kohustus kasutada keskset klassifikaatorite ja metaandmete registrit (§ 43[11] + eraldi klassifikaatoriregister) • sätestada, et klassifikaatorite ja metaandmete muudatused avaldatakse ühtse mehhanismi kaudu ja versioonid on jälgitavad

4.	**Tuletatud- ja koondandmed**	Arvutuslikud näitajad. Näited: • keskmine palk, • maksukohustus, • ESG indeks.	• sõltuvad sisendandmete režiimist, • võivad mõjutada õigusi	• kui tuletatud andmed võimaldavad üksikettevõtjat või isikut tuvastada või mõjutada, tuleb neid käsitleda vähemalt sama tundlikena kui sisendandmeid • eksitava metoodika või vigaste eelduste korral võib tekkida oluline mõju õigustele (vale riskiskoor, vale „punane lipp“) • statistika puhul kehtivad erireeglid: üksnes statistiline kasutus, mitte haldus- või järelevalveotsused.	Keskmine — once-only sobiv, kui: • tuletatud näitajal on selge keskne looja (keskallikas), • metoodika on läbipaistev ja dokumenteeritud • kasutatakse peamiselt mitte-isiku- või anonüümseid koondandmeid	• ei tohi luua olukorda, kus sama tuletatud näitaja korduv arvutamine eri • asutustes muutub põhjendamatult vajalikuks, kuid samas • peab lubama erinevaid mudeleid, kui eesmärgid ja metoodika on sisuliselt erinevad • automatiseeritud otsuste tegemine üksnes tuletatud näitajate alusel vajab selget seaduslikku alust (IKÜM art 22 analoogia)	• sätestada väärindatud andmete eriregulatsioon (§ 43[9]), mis nõuab metoodika läbipaistvust, vastutava asutuse määramist ja mõjuhindamist, kui andmetel on otsene mõju õigustele; • kehtestada, et tuletatud andmeid ei tohi ilma selge seadusliku aluseta kasutada automaatsete otsuste tegemiseks ega süüteomenetluse ennetavaks profileerimiseks.

Eeltoodud andmetüüpide kaardistus näitab, et andmepõhise aruandluse kontekstis ei ole andmete ristkasutuse võimalikkus ühtlane, vaid sõltub otseselt andmete liigist, nende õiguslikust režiimist ning nendega seotud riskidest. Andmetüüpide diferentseerimine võimaldab hinnata, millises ulatuses on võimalik rakendada *once-only* põhimõtet ning millistel juhtudel on vajalik täiendav õiguslik või tehniline regulatsioon.

Esiteks moodustavad identifikaatorid andmepõhise aruandluse tuumiku, kuna need võimaldavad erinevate andmekogude vahel andmeid üheselt siduda. Nende kõrge *once-only* sobivus tuleneb asjaolust, et tegemist on põhiandmetega, mille puhul on võimalik rakendada keskallika põhimõtet[43]. Samas kaasnevad identifikaatoritega olulised riskid, eelkõige identiteedivarguse ja vale seostamise risk, mistõttu eeldab nende ristkasutus selget õiguslikku raamistikku ning ranget ligipääsukontrolli.

Teiseks, tehingu- ja operatiivandmed on oma olemuselt kõrge granulaarsusega ning sisaldavad sageli isikuandmeid, maksusaladust või ärisaladust. Selliste andmete ristkasutus ei ole välistatud, kuid on tingimuslik ning eeldab selget õiguslikku alust, piisavaid turvameetmeid ning eesmärgipiirangu põhimõtte järgimist. Nende andmete puhul on riskid märkimisväärsed, hõlmates nii järelevalve- kui ka konkurentsiriski ning võimalikku mõju sanktsioonimenetlustele. Seetõttu ei saa nende andmete puhul lähtuda pelgalt tehnilisest võimalikkusest, vaid vajalik on diferentseeritud regulatiivne lähenemine.

Kolmandaks, klassifikaatorid ja metaandmed on oma olemuselt toetavad andmed, mille peamine eesmärk on tagada teiste andmete mõistetavus ja ühtne tõlgendamine. Kuna tegemist on üldjuhul avaliku teabega, on nende ristkasutus praktiliselt piiranguteta ning nende puhul on *once-only* põhimõtte rakendamine täielik. Õiguslikus plaanis on keskseks küsimuseks pigem standardiseerimine ja keskse klassifikaatorite registri olemasolu, mis tagaks semantilise koosvõime.

Neljandaks hõlmavad tuletatud- ja koondandmed andmeid, mis on saadud teiste andmete töötlemise tulemusena. Nende õiguslik režiim sõltub sisendandmetest, kuid lisandub ka eraldi risk, mis tuleneb nende võimalikust mõjust isikute õigustele ja kohustustele, näiteks maksukohustuse või riskihinnangu kujunemisel. Seetõttu on nende andmete *once-only* sobivus keskmine ning nende kasutamine eeldab täiendavat tähelepanu läbipaistvuse ja vastutuse küsimustele.

Kokkuvõttes näitab andmetüüpide kaardistus, et andmepõhise aruandluse rakendamine eeldab diferentseeritud lähenemist, kus erinevatele andmeliikidele kohaldatakse erinevaid õiguslikke ja tehnilisi nõudeid. Ühtne regulatsioon ei ole piisav, vaid vajalik on mitmetasandiline raamistik, mis arvestab nii andmete tundlikkust, kasutuseesmärki kui ka võimalikku mõju isikute ja ettevõtjate õigustele. Selline lähenemine võimaldab tasakaalustada andmete efektiivset kasutamist ja põhiõiguste kaitset.

[43] Käesoleva analüüsi kontekstis tuleb keskallikana käsitleda ametlikku (üldjuhul seadusega määratud) andmekogu, mis on konkreetse andmeelemendi kohta esmane ja autoriteetne allikas. Kui mõni andmeväli on ühes andmekogus määratud põhiandmeteks ja see andmekogu on selle andmeelemendi keskallikas, siis teised andmekogud võivad seda andmeväärtust kasutada, nad ei tohi sama andmeelementi uuesti koguda oma põhiandmetena, ning õige andmeväärtus loetakse põhimõtteliselt keskallika andmetest.

Eeltoodud andmetüüpide kaardistus näitab, et andmete ristkasutuse võimalikkus ei sõltu üksnes andmete liigist, vaid ka nende detailiastmest. Seetõttu on vajalik eraldi käsitleda andmete granulaarsuse küsimust ning määratleda, millisel tasemel on andmete kogumine ja jagamine õiguslikult põhjendatud.

3.2.1. Metoodika andmete granulaarsuse piiramiseks

Andmepõhise aruandluse rakendamisel on keskseks küsimuseks, millisel detailitasemel (granulaarsusel) on õiguspärane andmeid riigile koguda. Kehtiv õigus ei sätesta granulaarsust otseselt, kuid see tuleneb kaudselt andmekaitse, proportsionaalsuse ja eesmärgipiirangu põhimõtetest. Sellest lähtuvalt on käesolevas analüüsis välja töötatud metoodika, mis võimaldab hinnata, millistel juhtudel ei ole algandmete kogumine õiguspärane ning eelistada tuleb agregeeritud või tuletatud näitajaid.

Metoodika lähtub põhimõttest, et andmete kogumise detailiaste peab olema proportsionaalne nende kasutamise eesmärgiga ning ei tohi tekitada ebaproportsionaalseid riske andmesubjektide või ettevõtjate õigustele.

Granulaarsuse piirangu otsustusreegel

Riik ei tohiks koguda algandmeid (kõrge granulaarsusega detailandmeid), kui on täidetud vähemalt üks järgmistest tingimustest:

1. **Andmete kõrge tundlikkus**

Kui andmed sisaldavad isikuandmeid, ärisaladust või maksusaladust, mille detailne kogumine suurendab oluliselt privaatsus- või konfidentsiaalsusriski.

2. **Eesmärgi saavutatavus madalama granulaarsusega**

Kui andmete töötlemise eesmärki (nt statistika, analüüs, seire) on võimalik saavutada agregeeritud või tuletatud andmete alusel ilma detailandmeid kogumata.

3. **Ebaproportsionaalne risk**

Kui detailandmete kogumine suurendab ebaproportsionaalselt:

   - andmete väärkasutuse riski,
   - järelevalveriski,
   - konkurentsi- või ärisaladuse lekke riski.

4. **Kasutuse analüütiline või statistiline iseloom**

Kui andmeid kasutatakse üksnes koondatud järelduste tegemiseks ning individuaalne otsustamine ei ole vajalik.

Metoodika rakendamise tähendus

Metoodika rakendamine võimaldab diferentseerida andmete kogumise taset vastavalt nende tundlikkusele ja kasutuseesmärgile. Selle tulemusel:

- väheneb ettevõtjate halduskoormus, kuna ei nõuta liigseid detailandmeid;
- suureneb andmete kasutamise õiguspärasus ja proportsionaalsus;
- väheneb andmekaitse ja konfidentsiaalsusega seotud risk.

APA kontekstis tähendab see, et *once-only* põhimõtte rakendamine ei eelda alati algandmete kogumist ja jagamist, vaid võib toimida ka agregeeritud või tuletatud andmete tasemel, kui see on õiguslikult ja sisuliselt piisav.

3.3. Andmetüübi miinimumkirjelduse nõuded

Andmepõhise aruandluse toimimiseks ei piisa üksnes andmete struktureerimisest, vaid iga andmetüüp peab olema varustatud ühtse ja arusaadava kirjeldusega. Andmetüübi miinimumkirjeldus tagab, et andmeväljade tähendus, kasutusviis ja õiguslik staatus on üheselt mõistetavad nii andmeid koguvatele kui ka neid kasutavatele asutustele. Selline kirjeldus on eelduseks andmete automatiseeritud töötlemisele, ristkasutusele ning *once-only* põhimõtte rakendamisele. Miinimumkirjeldus hõlmab kolme omavahel seotud tasandit: semantilist ja tehnilist tasandit, õiguslikku tasandit ning dünaamilist tasandit.

3.3.1. Semantiline ja tehnilise tasand

Semantiline ja tehniline tasand määrab andmevälja sisulise tähenduse ning selle tehnilise kuju. Iga andmeväli peab olema varustatud selge nimetuse ja definitsiooniga, mis kirjeldab üheselt, millist teavet konkreetne andmeelement esitab. Lisaks tuleb määratleda andmetüüp, näiteks kas tegemist on arvulise väärtuse, tekstilise kirje või kuupäevaga. Semantilise ühtsuse tagamiseks on vajalik viidata ka kasutatavale standardile või klassifikaatorile, näiteks riiklikele klassifikaatoritele või rahvusvahelistele andmemudelitele. Selline kirjeldus võimaldab eri infosüsteemidel mõista andmete sisu samal viisil ning tagab andmete tehnilise koosvõime.

3.3.2. Õiguslik tasand

Õiguslik tasand määratleb andmete töötlemise lubatavuse ning piirangud. Iga andmevälja puhul tuleb hinnata selle tundlikkust, näiteks kas tegemist on avaliku teabe, isikuandmete või ärisaladust sisaldava teabega. Samuti tuleb määrata andmete kogumise ja töötlemise õiguslik alus, mis tuleneb kas seadusest või muust õigustloovast aktist. Õiguslik kirjeldus peab hõlmama ka ligipääsupiiranguid, mis määravad, millised asutused või isikud võivad andmeid kasutada, ning säilitamistähtaega, mis piirab andmete hoidmise kestust. Selline lähenemine aitab tagada, et andmete ristkasutus ja automatiseeritud töötlemine toimuvad kooskõlas kehtivate andmekaitse- ja konfidentsiaalsusnõuetega.

3.3.3. Dünaamiline tasand

Lisaks semantilisele ja õiguslikule kirjeldusele on oluline kirjeldada ka andmete dünaamilisi omadusi. Dünaamiline tasand hõlmab andmete värskust, uuendussagedust ning versioonihaldust. Andmete värskus näitab, kui ajakohased on andmed nende kasutamise hetkel, samas kui uuendussagedus kirjeldab, kui tihti andmeid uuendatakse või täiendatakse. Versioonihaldus võimaldab jälgida andmete muutumist ajas ning tagab, et erinevad infosüsteemid kasutavad sama andmevälja puhul ühtset ja ajakohast versiooni. Need aspektid on eriti olulised olukorras, kus andmeid kasutatakse mitmes avaliku sektori infosüsteemis ning nende alusel tehakse haldusotsuseid.

Kokkuvõttes võimaldab andmetüübi miinimumkirjeldus tagada, et andmeväljad on üheselt mõistetavad nii tehnilisest kui ka õiguslikust perspektiivist. Semantiline ja tehniline tasand loob aluse andmete koosvõimele, õiguslik tasand tagab andmete õiguspärase kasutamise ning dünaamiline tasand toetab andmete ajakohasust ja usaldusväärsust. Koos moodustavad need tasandid raamistiku, mis võimaldab andmepõhise aruandluse lahenduste toimimist ning andmete turvalist ristkasutust avalikus sektoris.

3.3.4. *Töötlemistoimingupõhiste metaandmete metoodika*

Andmepõhise aruandluse rakendamisel ei piisa üksnes andmeelementide kirjeldamisest, vaid vajalik on ka andmete töötlemistoimingute kirjeldamine metaandmete kaudu. Töötlemistoimingupõhine metaandmete metoodika võimaldab siduda iga andmetöötluse etapi konkreetsete õiguslike ja tehniliste nõuetega ning tagada andmete kasutamise läbipaistvus, jälgitavus ja õiguspärasus.

Metoodika lähtub põhimõttest, et iga andmetöötluse toiming (nt kogumine, salvestamine, edastamine, kasutamine) peab olema varustatud metaandmetega, mis kirjeldavad selle toimingu õiguslikku alust, eesmärki, ulatust ning rakendatavaid piiranguid.

1. Metoodika põhimõtted

Töötlemistoimingute metaandmete kirjeldamisel lähtutakse järgmistest põhimõtetest:

(i) Toimingupõhisus – metaandmed ei seondu üksnes andmeelemendiga, vaid iga konkreetse töötlemistoiminguga;

(ii) Õiguslik sidusus – iga toiming peab olema seotud õigusliku aluse ja eesmärgiga;

(iii) Jälgitavus – kõik toimingud peavad olema logitavad ja auditeeritavad;

(iv) Minimaalsus ja proportsionaalsus – metaandmed peavad võimaldama hinnata, kas konkreetne toiming on vajalik ja lubatav;

(v) Koosvõime – metaandmed peavad olema standardiseeritud ja masinloetavad.

2. Töötlemistoimingute ja metaandmete seos

Iga töötlemistoimingu puhul tuleb määratleda minimaalsed metaandmed, mis võimaldavad hinnata toimingu õiguspärasust:

Andmete kogumine (vastuvõtmine)

- õiguslik alus;
- kogumise eesmärk;
- andmete allikas;
- kogumise ulatus (granulaarsus);

Andmete salvestamine ja säilitamine

- säilitamistähtaeg;
- säilitamise eesmärk;
- turvameetmed;

Andmete kasutamine ja analüüs

- kasutuse eesmärk;
- kasutusjuhtum (nt järelevalve, statistika);
- mõju andmesubjektile;

Andmete edastamine ja jagamine

- õiguslik alus (seadus / nõusolek);
- vastuvõtja;
- ligipääsupiirangud;
- jagamise ulatus (nt täisandmed[44] vs agregeeritud);

Andmete avalikustamine

- avalikustamise alus;
- avalikustamise ulatus;

Andmete muutmine ja parandamine

- muudatuse alus;
- muudatuse tegija;
- versioonihaldus;

Andmete kustutamine või piiramine

- kustutamise alus;
- kustutamise aeg;
- säilitamiskohustuse olemasolu;

Juurdepääsu võimaldamine

- juurdepääsuõiguse alus;
- kasutaja roll;
- juurdepääsu ulatus.

3. Metoodika tähendus

Töötlemistoimingupõhiste metaandmete metoodika võimaldab siduda andmete elutsükli kõik etapid selgete õiguslike ja tehniliste kirjeldustega. See loob eeldused andmete õiguspäraseks ristkasutuseks, võimaldab automatiseeritud kontrolli andmete kasutamise üle ning toetab *once-only* põhimõtte rakendamist, tagades samal ajal andmekaitse ja läbipaistvuse.

3.3.5. Metaandmete avaldamise metoodika

Lisaks metaandmete loomisele on andmepõhise aruandluse rakendamisel keskse tähtsusega nende süstemaatiline ja õiguspärane avaldamine. Metaandmete avaldamise metoodika eesmärk on tagada

[44] Täisandmed käesoleva analüüsi kontekstis on andmed kõige detailsemas kogutavas vormis, mille puhul ükski sisuline element ei ole koondatud, üldistatud ega anonüümseks muudetud. Täisandmed võimaldavad taastada üksiktehingu, üksikobjekti või üksikisiku tasandi (nt iga arve, iga väljamakse, iga töötaja palgarida), mistõttu on nende töötlemise risk ja mõju õigustele oluliselt kõrgem kui koond- või tuletatud andmetel. Täisandmeid kasutatakse üldjuhul üksnes siis, kui eesmärki ei ole võimalik saavutada koond- või tuletatud andmete abil ning seadus annab selleks selge volitusnormi.

andmete töötlemise läbipaistvus, toetada andmete leitavust ning võimaldada andmete kontrollitavat ristkasutust avaliku sektori asutuste vahel.

Metoodika lähtub põhimõttest, et metaandmeid tuleb avaldada ulatuses, mis võimaldab hinnata andmete olemasolu, tähendust ja kasutustingimusi, kahjustamata seejuures andmete konfidentsiaalsust ega rikkumata õigusaktidest tulenevaid piiranguid.

1. Avaldamise põhimõtted

Metaandmete avaldamisel lähtutakse järgmistest põhimõtetest:

1. Läbipaistvus – metaandmed peavad võimaldama saada ülevaate, milliseid andmeid riik töötleb, millisel eesmärgil ja millistel tingimustel;
2. Leitavus – metaandmed peavad olema kättesaadavad viisil, mis võimaldab teistel asutustel tuvastada olemasolevaid andmeid;
3. Masinloetavus – metaandmed peavad olema standardiseeritud ja masinloetavas vormis, et toetada automatiseeritud andmevahetust;
4. Proportsionaalsus – avaldatavate metaandmete ulatus peab olema kooskõlas andmete tundlikkusega;
5. Turvalisus – metaandmete avaldamine ei tohi võimaldada juurdepääsu andmetele, mille kasutamine on piiratud.

2. Avaldamise kihid

Metaandmete avaldamine toimub kihiliselt, sõltuvalt andmete tundlikkusest ja kasutusotstarbest:

- Avalik kiht

Sisaldab üldist infot andmekogude ja andmetüüpide kohta (nt andmevälja nimetus, kirjeldus, üldine eesmärk), mis on kättesaadav kõigile.

- Piiratud juurdepääsuga kiht

Sisaldab täpsemaid metaandmeid (nt ligipääsutingimused, kasutuspiirangud, andmete granulaarsus), mis on kättesaadavad üksnes õigustatud asutustele.

- Sisemine kiht

Sisaldab detailset infot andmete töötlemise kohta (nt logid, kasutusjuhtumid, riskihinnangud), mis on kättesaadav üksnes andmekogu pidajale või järelevalveasutustele.

3. Metaandmete avaldamise sisu

Avaldatavad metaandmed peavad hõlmama eelkõige:

- andmete kirjeldust ja tähendust;
- töötlemise eesmärki;
- õiguslikku alust;
- andmete tundlikkuse kategooriat;
- ligipääsutingimusi;
- andmete kasutamise ja jagamise piiranguid.

Selline kirjeldus võimaldab teistel asutustel hinnata, kas andmete kasutamine on vajalik ja lubatav ilma, et nad peaksid esmalt taotlema ligipääsu andmete sisule.

4. Metoodika tähendus

Metaandmete avaldamise metoodika loob eelduse andmete paremale leitavusele ja koosvõimele ning toetab *once-only* põhimõtte rakendamist, võimaldades asutustel tuvastada juba olemasolevad andmed ja vältida nende korduvat küsimist ettevõtjalt. Samal ajal tagab kihiline avaldamine, et tundlike andmete kaitse ja konfidentsiaalsus on säilitatud.

3.4. Struktureerimata andmete erikäsitlus

Kuigi andmepõhise aruandluse eesmärk on võimalikult suur andmete struktureeritus ja automatiseeritud ristkasutus, ei ole praktikas võimalik kogu riigile edastatavat teavet esitada struktureeritud andmeväljadena. Paljudes valdkondades, näiteks järelevalve-, keskkonna- või analüütiliste dokumentide puhul, esitatakse oluline teave jätkuvalt struktureerimata kujul. Sellised andmed esinevad eelkõige dokumentide, aruannete, selgituste või ekspert-, mõju-, ja riskihinnangutena, mille sisu ei ole jagatud masinloetavateks andmeelementideks ning mille tõlgendamine eeldab sageli inimlikku hinnangut ja analüüsi.

Seetõttu tuleb struktureerimata andmete käsitlemisel rakendada andmepõhise aruandluse raamistikus eraldi metoodikat, mis erineb struktureeritud andmete automatiseeritud ristkasutusest. Struktureerimata andmete puhul ei ole realistlik ega alati ka õiguspärane rakendada täielikult automatiseeritud andmevoogu, kuna sellised dokumendid võivad sisaldada mitmesuguseid andmeliike, sealhulgas isikuandmeid, ärisaladust või muid konfidentsiaalseid andmeid, mille terviklik jagamine ei või olla lubatud. Sellest tulenevalt on vajalik eraldi käsitlus, mis võimaldab vältida dokumentide korduvat küsimist ettevõtjalt, kuid tagab samal ajal andmete kontrollitud ja õiguspärase kasutamise.

3.4.1. Once-only rakendamine

Struktureerimata andmete puhul ei rakendu *once-only* põhimõte tavapäraselt üksikute andmeväljade tasandil, vaid pigem dokumentide tasandil. Sellisel juhul ei tähenda andmete korduvkasutus automaatset andmevoogu erinevate infosüsteemide vahel, vaid mehhanismi, mis võimaldab tuvastada juba esitatud dokumentide olemasolu ning vajaduse korral neid kontrollitud viisil jagada.

Selline lähenemine põhineb eelkõige kolmel omavahel seotud mehhanismil.

Esiteks rakendub *once-only* põhimõte struktureerimata andmete puhul metaandmete kaudu. Iga dokument tuleb varustada masinloetavate metaandmetega, mis kirjeldavad dokumendi liiki, päritolu, ajaperioodi, valdkonda ning vajaduse korral ka tundlikkuse taset. Metaandmete olemasolu võimaldab teistel asutustel tuvastada, et vajalik dokument on juba riigi infosüsteemides olemas, ilma et nad peaksid koheselt ligipääsu dokumendi sisule.

Teiseks võimaldab *once-only* põhimõtte rakendamist dokumentide leitavus. Kui dokument on metaandmete abil tuvastatav, saab teine asutus hinnata, kas selle dokumendi kasutamine on vajalik ja õiguslikult põhjendatud. Selline lahendus vähendab vajadust küsida ettevõtjalt sama dokumenti korduvalt ning aitab vältida dubleerivat aruandluskoormust.

Kolmandaks võib struktureerimata dokumentide jagamine toimuda nõusolekupõhiselt, eriti juhtudel, kus dokument sisaldab andmeid, mille jagamine ei tulene otseselt seadusest. Nõusolekupõhine jagamine võimaldab ettevõtjal kontrollida, millised asutused võivad tema esitatud dokumentidele ligipääsu saada, ning tagab andmete kasutamise suurema läbipaistvuse.

Kokkuvõttes tähendab *once-only* põhimõtte rakendamine struktureerimata andmete puhul eelkõige dokumentide korduva küsimise vältimist. Selle saavutamiseks tuleb luua mehhanismid, mis võimaldavad dokumentide olemasolu tuvastada, hinnata nende kasutamise õiguspärasust ning tagada vajaduse korral kontrollitud ligipääs. Selline lähenemine võimaldab ühendada andmepõhise aruandluse eesmärgid ning andmekaitse- ja konfidentsiaalsusnõuded olukorras, kus täielikult automatiseeritud andmevahetus ei ole võimalik.

3.4.2. Õiguslikud riskid

Struktureerimata andmete kasutamine ja jagamine avaliku sektori infosüsteemides toob kaasa mitmeid õiguslikke riske, mis erinevad oma olemuselt struktureeritud andmete töötlemisega seotud riskidest. Kuna sellised andmed esinevad sageli vabas tekstis või dokumentides ning ei ole eelnevalt standardiseeritud andmeelementideks, võib nende sisu olla mitmetähenduslik ning sisaldada erinevaid andmeliike. Seetõttu tuleb struktureerimata andmete ristkasutuse ja jagamise puhul arvestada eelkõige konfidentsiaalsuse, eesmärgipiirangu ning tõlgendusvastutuse küsimustega.

Esiteks on oluline konfidentsiaalsuse risk. Struktureerimata dokumendid võivad sisaldada teavet, mis ei ole otseselt seotud dokumendi algse eesmärgiga, kuid mis võib siiski olla käsitatav konfidentsiaalse teabena, näiteks ärisaladusena või isikuandmetena. Sellised andmed võivad dokumendis esineda kontekstipõhiselt ning neid ei ole võimalik automaatselt eristada või filtreerida. Seetõttu võib dokumentide automaatne või laialdane jagamine asutuste vahel suurendada riski, et konfidentsiaalne teave jõuab asutusteni, kellel puudub selle kasutamiseks tegelik õiguslik alus või vajadus.

Teiseks tuleb arvestada eesmärgipiirangu põhimõttega. IKÜM art 5 lg 1 p b kohaselt peab andmete töötlemine olema seotud selgelt määratletud eesmärgiga ning andmeid ei tohi kasutada viisil, mis on selle eesmärgiga vastuolus. Struktureerimata andmete puhul võib olla keeruline hinnata, kas dokumendis sisalduva teabe kasutamine teise asutuse poolt vastab algsele töötlemise eesmärgile, kuna dokument võib sisaldada mitut eri liiki teavet. Sellest tulenevalt on vajalik hinnata iga dokumenti ja selle kasutamist eraldi, et tagada töötlemise kooskõla eesmärgipiirangu põhimõttega.

Kolmandaks kaasneb struktureerimata andmete kasutamisega tõlgendusvastutuse küsimus. Kuna selliste dokumentide sisu ei ole esitatud standardiseeritud andmeväljadena, võib nende tõlgendamine eri asutustes erineda. Kui dokumentide põhjal tehakse haldusotsuseid või kasutatakse neid analüütiliste järelduste tegemiseks, võib tekkida küsimus, milline asutus vastutab dokumendi sisu tõlgendamise eest ning millisel määral saab sellele tugineda õiguslikult siduvate otsuste tegemisel. See risk on eriti oluline olukordades, kus dokument sisaldab hinnangulist või eksperditeavet.

Kokkuvõttes eeldab struktureerimata andmete kasutamine avaliku sektori andmevahetuses ettevaatlikku ja kontrollitud lähenemist. Konfidentsiaalsuse kaitse, eesmärgipiirangu järgimine ning tõlgendusvastutuse selge määratlemine on keskse tähtsusega tingimused, mis võimaldavad struktureerimata andmete kasutamist kooskõlas kehtiva õigusega ning vähendavad riski, et andmete ristkasutus toob kaasa õiguskindluse või andmekaitsega seotud probleeme.

4. JUHTUMIPÕHINE ANALÜÜS

4.1. Andmete kogumise ja jagamise viisid

Käesolevas õigusanalüüsis käsitletakse andmete kogumise ja jagamise erinevaid mudeleid juhtumipõhiselt. Selline lähenemine võimaldab hinnata iga mudeli puhul andmete kogumise õiguslikku alust, töötlemise eesmärki, osapoolte rolle, andmete edastamise mehhanismi, ning *once-only* põhimõtte kohaldatavust.

Alljärgnevalt eristatakse kolme tüüpilist juhtumit:

(i) Juhtum I – Otsene andmete esitamine ettevõtjalt asutusele (nn traditsiooniline andmete kogumismudel);

(ii) Juhtum II - Andmete esitamine keskse andmejagamise punkti kaudu (nn keskse andmevärava või vahendusteenuse mudel);

(iii) Juhtum III – Asutustevaheline andmete jagamine ja väärindatud andmete edastamine (nn ristkasutuse ja väärindamise mudel).

4.2. Juhtum I – Otsene andmete esitamine ettevõtjalt asutusele (Traditsiooniline kogumismudel)

Kirjeldus

Ettevõtja või muu kohustatud isik esitab andmed otse konkreetsele avaliku sektori asutusele, kes on seaduse alusel õigustatud ja kohustatud neid andmeid koguma. Andmete esitamine võib toimuda taotluse alusel, aruandluskohustuse täitmiseks, järelevalve eesmärgil, loamenetluse käigus vms. Andmete edastamine toimub kas elektroonilise vormi kaudu, majandustarkvarast edastatava failina, API kaudu või dokumentaalsel kujul.

Õiguslik iseloomustus

Andmete kogumise õiguslik alus tuleneb tavaliselt eriseadusest (nt maksukorralduse seadus, keskkonnaseadustik, tööõigusaktid). Andmeid koguv asutus on üldjuhul vastutav töötleja. Ettevõtja on andmete esitamise kohustatud subjekt.

Õiguslikud küsimused

(i) Kas andmete kogumise ulatus vastab minimaalsuse põhimõttele?

(ii) Kas andmete esitamine toimub üksnes seaduses sätestatud eesmärgil?

(iii) Kas sama andmestik on juba mõne teise asutuse valduses?

Once-only kontekst

Selles mudelis ei rakendu *once-only* automaatselt, sest andmed liiguvad ainult ühe asutuse ja ettevõtja vahel. *Once-only* küsimus tekib hiljem, kui mõni teine asutus vajab samu andmeid või andmeid soovitakse teisese eesmärgi täitmiseks kasutada.

Õiguslik hinnang

Esmasel andmete kogumisel ettevõtjalt avaliku sektori asutuse poolt on tegemist klassikalise haldusõigusliku suhtega, kus andmete kogumise alus peab tulenema seadusest. Õiguslikult on keskne küsimus andmete kogumise ulatus ja eesmärk. Siin tuleb hinnata kolme põhimõtet:

(i) Seaduslikkuse põhimõte – andmete kogumine peab põhinema selgele volitusnormile.

(ii) Proportsionaalsus ja minimaalsus – koguda tohib üksnes neid andmeid, mis on eesmärgi saavutamiseks vajalikud.

(iii) Eesmärgipiirang – andmeid ei või kasutada muul eesmärgil ilma täiendava õigusliku aluseta.

APA kontekstis muutub esmane kogumine eriti oluliseks, sest see määrab:

(i) millised andmed muutuvad potentsiaalselt ristkasutatavaks,

(ii) millise kvaliteediga andmestik riigi infosüsteemi siseneb,

(iii) kas andmed kvalifitseeruvad põhiandmeteks.

Kui esmane kogumine on õiguslikult või sisuliselt liiga lai, kandub see probleem edasi kogu ristkasutuse ahelasse.

Regulatsioonivajadus

Kehtivas õiguses on esmane kogumine üldjuhul reguleeritud eriseadustes, kuid puuduvad:

- ühtsed andmekirjelduse miinimumnõuded,
- põhiandmete kvaliteedinõuded,
- selge kohustus hinnata, kas kogutavad andmed juba eksisteerivad mõnes teises andmekogus.

Regulatsioonivajadus seisneb eelkõige:

(i) Kohustuses kontrollida enne andmete kogumist, kas need on juba riigi valduses (*once-only* eelhindamine);

(ii) Kohustuses kirjeldada iga kogutava andmevälja:

- õiguslik alus,
- tundlikkus,
- säilitamistähtaeg,
- ristkasutuse lubatavus;

(iii) Põhiandmete keskallika määramise mehhanismi tugevdamises.

Ilma selliste nõueteta tekib risk, et *once-only* põhimõte jääb deklaratiivseks ning dubleeriv kogumine jätkub.

4.3. Juhtum II – Andmete esitamine keskse andmejagamise punkti kaudu (Keskse andmevärava või vahendusteenuse mudel)

Kirjeldus

Ettevõtja esitab andmed üks kord keskse andmejagamise punkti kaudu (nt andmete teabevärav, andmevahetusplatvorm). Kohustatud isiku vaates (nt ettevõtja, füüsiline isik) on parem, kui ühesuguseid andmeid antakse üks kord.

Seejärel on kõigil õigustatud asutustel võimalus neid andmeid kasutada vastavalt seaduses sätestatud tingimustele.

Olulised tunnused on, et:

- andmete esitamine toimub ühekordselt;
- keskne süsteem vahendab andmeid õigustatud asutustele;
- ettevõtja ei esita samu andmeid mitmele asutusele eraldi;
- andmete vahetuskeskkond ise ei tohi andmeid töödelda.

Õiguslik iseloomustus

Keskne süsteem võib olla tehniline vahendaja, volitatud töötleja või teatud juhtudel iseseisev vastutav töötleja. Õigustatud asutused peavad omama õiguslikku alust andmete kasutamiseks. Andmete vastutava töötleja roll (sh nõusolek) võib olla asjakohane, kui andmete jagamine ei toimu otseselt seaduse alusel.

Õiguslikud küsimused

- Millisel alusel saavad teised asutused andmeid kasutada?
- Kas andmete edastamine on kooskõlas eesmärgipiirangu põhimõttega?
- Kas keskne süsteem tagab andmete kasutuslogid ja läbipaistvuse?
- Kuidas tagatakse andmete kvaliteet ja ajakohasus?

Once-only kontekst

See mudel realiseerib *once-only* põhimõtte kõige otsesemalt. Vajalik on:

- selge volitusnorm seaduses,
- andmete tundlikkuse diferentseerimine,
- rollide ja vastutuse täpne määratlus,
- nõusolekuteenuse regulatsioon, kui jagamine ei põhine otseselt seadusel.

Õiguslik hinnang

See mudel realiseerib *once-only* põhimõtte kõige otsesemalt. Samas on tegemist kõige keerukama õigusliku konfiguratsiooniga, sest rollijaotus ei ole lineaarne.

Olulised küsimused:

- Kas keskne süsteem on vastutav või volitatud töötleja?
- Kas teistel asutustel on iseseisev õiguslik alus andmete kasutamiseks?
- Kas andmete edastamine toimub seaduse alusel või nõusolekupõhiselt?
- Kuidas tagatakse andmete kasutuslogid ja läbipaistvus?

Õiguslik risk seisneb eelkõige selles, et:

- andmeid hakatakse kasutama laiemalt, kui algne kogumise eesmärk lubab;
- keskne süsteem muutub de facto universaalseks andmehoidlaks ilma piisava õigusliku raamita;
- vastutus hajub ning andmesubjektil puudub selge ülevaade, kes tema andmeid töötleb.

Kui keskse andmejagamise mudel ei ole seaduse tasandil piisavalt normeeritud, võib see olla vastuolus nii eesmärgipiirangu kui ka õigusselguse põhimõttega.

Regulatsioonivajadus

See mudel eeldab selget volitusnormi seaduses, mis määratleb:

1. Keskse andmejagamise süsteemi õigusliku staatuse.
2. Õigustatud kasutajate ringi ja nende volituse aluse.
3. Andmete tundlikkuse alusel diferentseeritud ligipääsutingimused.
4. Kohustuse pidada andmete kasutuslogi (andmejälgija mehhanism).
5. Nõusolekupõhise jagamise korra, kui jagamine ei toimu otseselt seaduse alusel.

Ilma sellise regulatsioonita tekib põhiseaduslik risk, et riik kogub ja jagab andmeid üldvolituse alusel, mis ei vasta piisava määratletuse nõudele.

4.4. Juhtum III – Asutustevaheline andmete jagamine ja väärindatud andmete edastamine (Ristkasutuse ja väärindamise mudel)

Kirjeldus

Ühel avaliku sektori asutusel (asutus A) on kas:

1. algandmed, mis on saadud ettevõtjalt; või
2. väärindatud andmed, mis on saadud näiteks arvutuste, analüüsi, koondamise või järelevalvemenetluse tulemusena.

Teisel asutusel (asutus B) tekib vajadus kasutada neid andmeid oma avaliku ülesande täitmiseks.

Õiguslik iseloomustus

Siin tuleb eristada algandmete jagamist, tuletatud või väärindatud andmete jagamist ja otsustusliku tähendusega andmete edastamist.

Asutus A võib olla algne vastutav töötleja või andmete teisese töötlemise tulemusel tekkinud uute andmete vastutav töötleja.

Õiguslikud küsimused

- Kas andmete teisene kasutamine on kooskõlas esialgse kogumise eesmärgiga?
- Kas seadus näeb ette andmete jagamise kohustuse või õiguse?
- Kas väärindatud andmed kujutavad endast uut andmekogumit?
- Kas andmete jagamine võib mõjutada andmesubjekti õigusi?

Väärindatud andmete eripära

Väärindatud andmed võivad omada otsustuslikku tähendust (nt maksukohustus, sanktsioon), olla suurema mõjuga kui algandmed ning sisaldada täiendavat hinnangulist elementi.

Seetõttu on väärindatud andmete jagamine sageli suurema õigusliku riskiga kui algandmete jagamine.

Once-only kontekst

Siin ei ole tegemist klassikalise *once-only* olukorraga, vaid:

- teisese kasutuse ja ristkasutuse mudeliga,
- kus keskne küsimus on eesmärgipiirang ja õiguslik alus.

Õiguslik hinnang

Asutustevaheline andmete jagamine on *once-only* põhimõtte praktiline tuum, kuid just siin ilmnevad suurimad õiguslikud riskid.

Eristada tuleb:

- algandmete jagamist;
- tuletatud või väärindatud andmete jagamist;
- otsustusliku tähendusega andmete edastamist.

Väärindatud andmed võivad sisaldada:

- hinnanguid,
- arvutusi,
- riskisooritusi,
- järeldusi, mis mõjutavad isiku või ettevõtte õigusi.

Selliste andmete jagamine ei ole neutraalne tehniline toiming, vaid võib omada otsest õiguslikku mõju.

Oluline on hinnata:

- kas teisene kasutus on kooskõlas esialgse kogumise eesmärgiga;
- kas väärindatud andmed kujutavad endast uut andmekogumit;
- kas andmete edastamine võib viia kaudse automatiseeritud otsustuseni.

Õiguslikult on tegemist kõrgeima riskitasemega mudeliga.

Regulatsioonivajadus

Kehtivas õiguses puudub üldnorm, mis reguleeriks mitte-isikuandmete teisest kasutust, väärindatud andmete jagamist ning ristkasutuse mõju hindamist.

Seega andmepõhist aruandlust ja *once-o*nly põhimõtte rakendamist toetav regulatsioon peab sisaldama:

(i) selget teisese kasutuse üldnormi;

(ii) väärindatud andmete jagamise erisätet, kui andmetel on otsustuslik mõju;

(iii) mõjuhindamise kohustust kõrgema tundlikkusega andmete puhul;

(iv) kohustust teavitada andmesubjekti või ettevõtjat, kui andmeid kasutatakse uuel eesmärgil;

(v) vastutuse selget määratlust (milline asutus vastutab jagatud andmete õigsuse eest).

Ilma sellise raamistikuta võib ristkasutus viia olukorrani, kus ettevõtja või muu isiku suhtes tehakse otsuseid mitme asutuse koostalitlusel, kuid õiguslik vastutus ja läbipaistvus on hajutatud.

4.5. Mudelite võrdlus

Andmete kogumise ja jagamise mudelite analüüs näitab, et ettevõtjalt andmete esmane kogumine, keskne andmejagamine ning asutustevaheline ristkasutus ei ole alternatiivsed, vaid komplementaarsed mehhanismid. Nende paralleelne eksisteerimine on vältimatu nii andmete tekke loogika, õiguslike aluste kui ka töötlemise eesmärkide erinevuse tõttu. Andmepõhise aruandluse rakendamisel tuleb seega kujundada diferentseeritud regulatsiooniraamistik, mis võimaldab mudelite koostoimet, kuid määratleb selgelt nende kohaldamisala ja prioriteetsuse.

Tabel nr 9. Juhtumite põhiselt *once-only* sobivus

Juhtum	Andmevoog	*Once-only* sobivus	Õiguslik risk
I	Ettevõtja → üks asutus	Madal (esmasel kogumisel)	Madal–keskmine
II	Ettevõtja → keskne punkt → mitmed asutused	Väga kõrge	Sõltub regulatsioonist
III	Asutus A → Asutus B	Tingimuslik	Kõrge, kui tegemist väärindatud andmetega

Normitehniline järeldus

Juhtumipõhine analüüs näitab, et andmete kogumise ja jagamise erinevad mudelid eeldavad erinevat õiguslikku käsitlust. Kolme käsitletud juhtumi võrdlusest ilmneb, et esmane andmete kogumine on eeskätt normatiivse kvaliteedi küsimus, kus keskne roll on andmete selgel määratlemisel ja kogumisõiguse ja -kohustuse õigusselgusel. Seevastu keskse andmejagamise mehhanismi kaudu toimuv andmete vahendamine on eelkõige volitusnormi ja vastutuse küsimus, kuna selline mudel eeldab selget õiguslikku alust andmete edastamiseks ning üheselt määratletud rolle ja kohustusi erinevate osapoolte vahel. Asutustevahelise väärindatud andmete jagamise puhul kerkivad esile eeskätt eesmärgipiirangu ning põhiõiguste kaitsega seotud küsimused, kuna tegemist on andmete teisese kasutusega, millel võib olla oluline mõju isikute ja ettevõtjate õigustele.

Sellest tulenevalt eeldab *once-only* põhimõtte tõhus ja õiguspärane rakendamine, et seadus eristab selgelt andmete esmast kogumist, keskset vahendatud jagamist ning asutustevahelist teisest kasutust. Ühtlasi tuleb kehtestada nendele olukordadele diferentseeritud õiguslikud reeglid ning siduda andmete kasutamine nende tundlikkusest lähtuva riskijuhtimise mudeliga.

Normitehniliselt tähendab see, et seadus peab esiteks selgelt eristama andmete esmast kogumist, keskse mehhanismi kaudu toimuvat jagamist ning asutustevahelist ristkasutust. Teiseks eeldab keskse andmejagamise mudel selge volitusnormi kehtestamist, andmete tundlikkuse diferentseerimist, nõusolekuteenuse õiguslikku alust ning andmete vahendamisega seotud vastutuse ja rollide täpset määratlemist. Kolmandaks on asutustevahelise väärindatud andmete jagamise puhul vajalik kehtestada andmete teisese kasutuse üldnorm, näha ette mõjuhindamise kohustus kõrgema tundlikkusega andmete puhul ning tagada andmete kasutamise läbipaistvus ja jälgitavus.

Selline diferentseeritud ja süsteemne lähenemine võimaldab luua õigusliku raamistiku, mis toetab andmepõhise aruandluse eesmärke, tagades samal ajal andmete õiguspärase kasutamise ning põhiõiguste kaitse.

Riiklik statistika ja nõusolekupõhine andmejagamine

Käesolev analüüs käsitleb nõusolekupõhist andmejagamist eelkõige APA kontekstis üldiselt ning ei paku ammendavat lahendust riikliku statistika eripäradele. Statistikaameti vaates võib kaaluda, kas ja millises ulatuses peaks statistilistel eesmärkidel andmete kogumisel ja kasutamisel kehtima rangemad nõusolekunõuded või selgemad teavitamisstandardid kui teiste avaliku sektori andmetöötluste puhul.

Põhimõtteliselt eeldab see selgeid kriteeriume, millal Statistikaamet tegutseb andmekogujana (nt küsitluste või otseküsitluse kaudu) ja millal üksnes andmete kasutajana (tuginedes administratiivandmetele). Nende rollide eristamine ja nõusoleku rolli täpsem määratlemine ületab käesoleva analüüsi fookuse, kuid APA edasisel kujundamisel on vajalik see koostöös Statistikaameti ja teiste asutustega välja töötada.

4.6. Teise asutuse eest andmete kogumise metoodika

Andmepõhise aruandluse ja *once-only* põhimõtte rakendamisel tekib küsimus, kas ja millistel tingimustel võib üks avaliku sektori asutus koguda andmeid teise asutuse eest olukorras, kus andmeid koguval või vastu võtval asutusel ei pruugi olla otsest õiguslikku alust nende andmete töötlemiseks. Käesolevas analüüsis on välja töötatud metoodika, mis võimaldab hinnata sellise andmekogumise lubatavust ning määratleda vastavad piirangud.

1. Põhireegel

Üldreeglina ei ole lubatud koguda andmeid teise asutuse eest ilma selge õigusliku aluseta. Andmete kogumine peab tuginema seadusest tulenevale volitusnormile ning olema seotud konkreetse avaliku ülesande täitmisega. Õigusliku aluse puudumisel ei ole lubatav laiendada andmete kogumise ulatust teise asutuse vajadustest lähtudes.

2. Lubatav kogumine (tingimuslik)

Andmete kogumine teise asutuse eest võib olla lubatav, kui on täidetud järgmised tingimused:

- olemas on **selge õiguslik alus või volitusnorm**, mis võimaldab andmete kogumist ja vahendamist;
- andmete kogumise ja kasutamise eesmärgid on **omavahel kooskõlas**;
- andmete kogumine on **vajalik halduskoormuse vähendamiseks** ja proportsionaalne;
- rakendatakse **andmete minimaalsuse põhimõtet** (kogutakse vaid vajalikud andmeväljad);
- on tagatud **läbipaistvus ja jälgitavus**, sh andmete kasutamise logimine;
- vajaduse korral kasutatakse **nõusolekupõhist jagamist**, kui seadusest tulenev alus puudub.

Selline mudel on kõige selgemalt rakendatav keskse andmejagamise mehhanismi (andmevärava) kaudu.

3. *Statistikaamet kui esmane kontaktasutus*

APA raames tuleb eristada olukordi, kus Statistikaamet tegutseb:

(i) andmekoguja rollis, kogudes andmeid üksnes statistilisel eesmärgil, ning

(ii) andmete kasutaja rollis, tuginedes teiste asutuste administratiivandmetele.

Juhtudel, kus Statistikaamet on ettevõtja peamine kontakt samal teemal, on oluline, et andmeesitajale oleks selgelt arusaadav, millisel õiguslikul alusel ja millisel eesmärgil andmeid kogutakse ning kas andmeid kasutatakse üksnes statistika tootmiseks või ka teiste avalike ülesannete täitmiseks. Riikliku statistika eripäraks on, et teatud tundlikes valdkondades (nt ümbrikupalk, perevägivald) võib andmete

edasijagamine teistele asutustele olla kas õiguslikult välistatud või praktikas usaldussuhte seisukohalt ebasoovitav.

Seetõttu peab APA õigusraamistik võimaldama olukordi, kus Statistikaamet kogub andmeid üksnes statistilisel eesmärgil ning neid andmeid ei kasutata teiste asutuste haldus-, menetlus- või järelevalveotsusteks, isegi juhul, kui tehniliselt oleks andmete edasijagamine võimalik. Selliste piirangute ja erandite läbipaistev fikseerimine on oluline nii ettevõtjate usalduse kui ka statistika regulatiivse eristaatuse säilitamiseks.

4. Keelatud kogumine

Andmete kogumine teise asutuse eest ei ole lubatav eelkõige järgmistel juhtudel:

- puudub **õiguslik alus** või volitusnorm;
- andmete kasutamine oleks vastuolus **eesmärgipiirangu põhimõttega**;
- andmed on **kõrge tundlikkusega**, sealhulgas:
    - isikuandmed (eriti eriliigilised andmed),
    - ärisaladus,
    - maksusaladus;
- andmete kogumine on seotud **järelevalve- või sanktsioonimenetlusega**, kus andmete kogumise alus peab olema selgelt määratletud;
- andmete kogumine tooks kaasa **ebaproportsionaalse riive** isikute või ettevõtjate õigustele.

5. Andmekategooriapõhine eristus

Andmete kogumise lubatavus sõltub otseselt andmekategooriast:

- **Identifikaatorid**
  – üldjuhul lubatav keskse kogumise mudelis, eeldusel et on tagatud keskallika põhimõte;
- **Klassifikaatorid ja metaandmed**

  – lubatav ja soovitatav tsentraliseeritud kogumine;
- **Tehingu- ja operatiivandmed (kõrge granulaarsus)**

  – tingimuslik; eeldab tugevat õiguslikku alust, piiranguid ja turvameetmeid;
- **Tuletatud ja koondandmed**

  – eelistatud lahendus juhtudel, kus detailandmete kogumine ei ole vajalik.

6. Normitehniline järeldus

Kehtiv õigusraamistik ei anna piisavalt selget alust olukordadeks, kus üks asutus kogub andmeid teise eest. Sellise mudeli õiguspäraseks rakendamiseks on vajalik:

- kehtestada **selge volitusnorm** andmete vahendatud kogumiseks;
- määratleda **primaarse koguja ja sekundaarse kasutaja rollid ja vastutus**;
- sätestada **andmete tundlikkusel põhinevad piirangud**;
- luua **nõusolekuteenuse õiguslik alus**, kus seadusest tulenev alus puudub;
- tagada **läbipaistvus ja kontrollitavus**, sh logimine ja auditeeritavus.

7. Metoodika tähendus

Käesolev metoodika võimaldab hinnata, millistel juhtudel on andmete kogumine teise asutuse eest õiguspärane ning millistel juhtudel tuleb seda piirata või välistada. See loob aluse halduskoormuse vähendamiseks ilma, et kahjustataks andmekaitset, konfidentsiaalsust või põhiõigusi, ning toetab *once-only* põhimõtte praktilist rakendamist.

5. APA RAKENDAMINE PRAKTIKAS

5.1. Andmete klassifikatsioon APA kontekstis

APA rakendamine eeldab, et andmed on süstemaatiliselt klassifitseeritud vähemalt tundlikkuse, kasutuseesmärgi ja riskitaseme alusel. Klassifikatsioon ei ole pelgalt tehniline (IT) tegevus, vaid sisuline juhtimisotsus.

Vastutus

Andmekogu tasandil lasub esmase klassifitseerimise vastutus andmekogu vastutaval töötlejal. Ettevõtja klassifitseerib oma tasandil andmed, mida ta riigile esitab (nt millised andmed on ärisaladus, millised avalikud). Keskne koordineeriv asutus (nt andmehalduse kesküksus) kehtestab ühtse klassifikatsioonimetoodika ja kontrollib selle rakendamist, kuid ei tee igapäevast üksikandmete käsitsi liigitamist.

Aeg

Klassifikatsioon tehakse:

(i) uue andmekogu loomisel (andmekogu asutamisel on klassifikatsioon kohustuslik osa eelanalüüsist),
(ii) andmekogu olulisel muutmisel (uued andmekategooriad, uued kasutuseesmärgid või ristkasutus),
(iii) perioodiliselt, nt õiguslike muudatuste või uute riskide ilmnemisel.

Kriteeriumid

Andmete tundlikkus ja riskitase määratakse kombinatsioonis järgmiste kriteeriumidega:

(iii) õiguslik alus (seadusest tulenev kohustus, nõusolek, leping),
(iv) kasutuseesmärk (otsustamine, järelevalve, aruandlus, teenuse osutamine),
(v) andmete ristkasutuse ulatus (üks asutus, mitu asutust, avalikkus),
(vi) järelevalve- ja põhiõiguste risk (potentsiaalne mõju ettevõtjale või andmesubjektile).

Mitu kategooriat ühes andmekogus

Ühes ja samas andmekogus võivad koos esineda vabalt ristkasutatavad, piiratud ja rangelt kaitstavad andmed. Seetõttu tuleb klassifitseerida andmeid andmetüübi või andmeelemendi tasandil, mitte ainult andmekogu tervikuna. APA ja once-only põhimõtted rakenduvad eelkõige nendele andmetele, mille klassifikatsioon lubab korduvkasutust; sama andmekogu sees olevate kõrgema tundlikkusega andmete puhul tuleb ette näha rangemad juurdepääsupiirangud ja järelevalvemehhanismid.

Näide

Oletame, et Asutus A peab andmekogu BC, kuhu ettevõtjad esitavad kord kvartalis aruandeid. Andmekogus BC on kolm peamist andmeelementi:

- F – ettevõtte üldandmed (nimi, registrikood, kontaktandmed);
- C – majandusnäitajad (käive, töötajate arv, palgafond);
- D – järelevalvega seotud märkused ja hinnangud (riskihinnang, rikkumiste kirjeldused, kohaldatud meetmed).

Vastutus

Andmekogu BC vastutav töötleja on Asutus A. Tema ülesanne on määrata iga andmeelemendi F, C ja D tundlikkuse, kasutuseesmärgi ja riskitaseme klassifikatsioon. Ettevõtja klassifitseerib oma tasandil, milliseid C-andmeid ta käsitleb ärisaladusena ja millised võivad olla avalikud. Andmehalduse kesküksus annab ette üldise metoodika (tundlikkuse skaala, kriteeriumid), mille järgi Asutus A klassifitseerimise otsuseid teeb.

Aeg

Esmaklassifikatsioon tehakse andmekogu BC loomisel. Näiteks määratakse, et:

(i) F-andmed on üldjuhul madala tundlikkusega ja võivad olla laialdasemalt korduvkasutatavad;

(ii) C-andmed on keskmise tundlikkusega (ärisaladuse risk) ja nende korduvkasutus eeldab täiendavaid piiranguid;

(iii) D-andmed on kõrge tundlikkusega (järelevalvemeetmete ja rikkumiste info). Hiljem, kui lisatakse uus andmeväli (nt detailne palgajaotus), tuleb Asutusel A andmekogu BC klassifikatsioon uuesti üle vaadata. Samuti tehakse klassifikatsiooni perioodiline ülevaatus, kui muutuvad õiguslikud alused või ristkasutuse ulatus.

Kriteeriumid

Asutus A määrab F, C ja D klassifikatsiooni, võttes arvesse:

(i) õiguslikku alust (nt C-andmed kogutakse seadusest tuleneva aruandluskohustuse alusel);

(ii) kasutuseesmärki (F-andmeid kasutatakse kontaktiks ja identifitseerimiseks, C-andmeid statistiliseks aruandluseks ja otsustamiseks, D-andmeid järelevalveks);

(iii) ristkasutuse ulatust (F-andmeid jagatakse ka teistele asutustele identifitseerimise eesmärgil, C-andmete jagamine on piiratud, D-andmed jäävad valdavalt Asutus A-siseseks);

(iv) mõju ettevõtjale (nt D-andmete vale kasutus võib oluliselt kahjustada ettevõtja mainet ja õigusi).

Mitu kategooriat ühes andmekogus

Andmekogus BC on seega koos vähemalt kolm erinevat kategooriat:

(i) F-andmed on valdavalt vabalt ristkasutatavad (APA ja once-only rakenduvad laialt);

(ii) C-andmed on piiratud korduvkasutatavusega (vajalik täpsem õiguslik alus ja juurdepääsukontroll);

(iii) D-andmed on rangelt kaitstavad (kitsas juurdepääs, detailne logimine, eraldi järelevalve).

See tähendab, et Asutus A ei saa käsitleda andmekogu BC tervikuna kas „avatud“ või „suletuna“. Klassifikatsioon tehakse andmeelemendi tasandil ning APA lahendusi (once-only päringuid, automaatset aruandlust) saab rakendada eelkõige F- ja osaliselt C-andmete suhtes, samal ajal kui D-andmete puhul tuleb ette näha rangemad juurdepääsupiirangud ja tugevamad järelevalvemehhanismid.

5.2. Tuletatud andmed APA kontekstis

APA raames ei töödelda üksnes ettevõtjate esitatud algandmeid, vaid ka nendest tuletatud andmeid (näiteks koondnäitajad, indeksid, riskiskoorid, ennustused). Tuletatud andmed ei ole automaatselt avalikud ega vabalt ristkasutatavad; nende õiguslik käsitlus sõltub nii lähteandmetest kui ka tuletatud andmete kasutuseesmärgist.

Õiguslik iseloom

Üldjuhul on tuletatud andmete töötlemine osa algandmete töötlemise ahelast, mitte uus iseseisev töötlemistoiming, kui see toimub algsete eesmärkide ja õigusliku aluse raames. Kui tuletatud andmed muutuvad iseseisvaks andmestikuks (näiteks riskiskooride register), tuleb nende loomist ja kasutust käsitleda eraldi töötlemisena, millel on oma õiguslik alus ja eesmärk.

Vastutav töötleja

Tuletatud andmete vastutav töötleja on asutus, kes otsustab tuletatud andmete loomise eesmärgi, metoodika ja kasutamise ulatuse. See võib olla erinev algandmete vastutavast töötlejast, kuid tuletatud andmeid ei tohi luua ega kasutada viisil, mis on vastuolus algandmete kogumise õigusliku aluse või eesmärgiga.

APA ja *once-only* põhimõtted

Once-only põhimõte tähendab, et:

(i) ettevõtja ei pea esitama mitu korda sama algandmestikku ainult selleks, et eri asutused saaksid sama tuletatud näitajat arvutada;

(ii) võimaluse korral tuleks määrata tuletatud andmete keskne looja (keskallikas), kelle arvutatud näitajat teised asutused kasutavad;

(iii) sama tuletatud näitaja korduv loomine mitmes asutuses võib olla põhjendatud ainult siis, kui eesmärgid ja metoodika on sisuliselt erinevad.

Tuletatud andmed ei saa olla vaikimisi käsitatavad madalama tundlikkusega andmetena. Kui tuletatud näitajad mõjutavad ettevõtja õigusi või võimalusi (näiteks riskiprofiilid, skoorid, hinnangud), tuleb nende töötlemisele kohaldada samu või rangemaid põhimõtteid kui algandmete töötlemisel.

Järelevalve

Tuletatud andmete järelevalve hõlmab lisaks tavapärasele järelevalvele (õiguslik alus, minimaalsus, turvalisus) ka:

(i) läbipaistvust selle kohta, milliseid tuletatud näitajaid luuakse ja kuidas neid kasutatakse;

(ii) võimalust ettevõtjale saada sisuline selgitus teda mõjutavate tuletatud näitajate kohta ning vajadusel neid vaidlustada;

(iii) modelleerimise ja profileerimisega seotud riskide hindamist, sh võimalikke süsteemseid kallutatusi või diskrimineerimisriske.

Näide

Jätkates eelmise näitega eeldame, et Asutus A peab andmekogu BC, kuhu ettevõtjad esitavad algandmeid C (käive, töötajate arv, palgafond). Nende andmete põhjal loob Asutus A kaks tüüpi tuletatud andmeid:

- T1 – sektoriülesed koondnäitajad (näiteks keskmine käive ja palgatase majandussektori kaupa);
- T2 – ettevõttepõhine riskiskoor (näiteks maksukäitumise riskihinnang skaalal 1–5).

Õiguslik iseloom

T1 koondnäitajad on klassikaline statistiline tuletatud andmestik: neid kasutatakse poliitikakujunduseks ja üldiseks aruandluseks, üksikettevõtjat nende põhjal tuvastada ei saa. T1 töötlemine on seega osa algandmete C töötlemisest sama avaliku ülesande raames. T2 riskiskoorid seevastu moodustavad eraldi andmestiku, mille eesmärk on suunata järelevalvemeetmeid üksikute ettevõtjate suhtes. T2 puhul tuleb defineerida eraldi õiguslik alus, eesmärk ja säilitustähtaeg ning käsitleda seda iseseisva töötlemisena.

Vastutav töötleja

Algandmete C vastutav töötleja on Asutus A, kes kogub aruandeid andmekogusse BC. Ka T1 koondnäitajate loomise otsustab Asutus A, mistõttu on ta ka nende tuletatud andmete vastutav töötleja. T2 riskiskooride loomises osaleb aga teine asutus D, kes määrab, milliseid muutujaid riskimudelisse kaasatakse ja kuidas skoori kasutatakse järelevalve kavandamisel. Sellisel juhul on riskiskooride andmestiku vastutav töötleja Asutus D, isegi kui osa sisendandmeid pärineb Asutuse A andmekogust BC. Asutus D peab tagama, et riskiskooride loomine ei ole vastuolus Asutus A algse kogumise eesmärkide ja õigusliku alusega.

APA ja once-only põhimõtted

Ettevõtja ei pea esitama sama C-andmestikku eraldi nii Asutusele A kui Asutusele D üksnes selleks, et mõlemad saaksid luua identse T2 riskiskoori. Võimaliku lahendusena määratakse, et riskiskoori T2 keskne looja (keskallikas) on Asutus D, kes arvutab skoori, tuginedes Asutuselt A saadud C-andmetele, ning edastab skoori vajaduse korral tagasi Asutusele A. Kui Asutus A soovib luua teistsuguse, näiteks üksnes statistilise jälgimise eesmärgil kasutatava „pehme“ riskinäitaja, võib see olla põhjendatud eraldi tuletatud andmestikuna, eeldusel et eesmärk ja metoodika erinevad sisuliselt Asutuse D skoorist.

Tundlikkus ja järelevalve

T1 koondnäitajad on üldjuhul madala tundlikkusega, kui neist ei ole võimalik üksikettevõtjat järeldada. Need võivad sobida laiemaks avalikustamiseks ja APA rakendamiseks (näiteks automaatne aruandlus avalikkusele). T2 riskiskoorid on seevastu kõrge tundlikkusega tuletatud andmed, mis mõjutavad otseselt ettevõtja õigusi ja võimalusi (näiteks kontrolli tõenäosust). Nende töötlemisel tuleb järgida samu või rangemaid põhimõtteid kui algandmete C töötlemisel:

(i) ettevõtjal peab olema võimalik saada selgitus teda mõjutava skoori olemuse ja peamiste tegurite kohta,

(ii) järelevalveasutused peavad hindama skoorimudeli võimalikke süsteemseid kallutatusi või diskrimineerimisriske,

(iii) juurdepääsu skooridele logitakse ja piiratakse selgemalt kui üldstatistika T1 puhul.

Selline eristamine aitab APA raames vältida olukorda, kus tuletatud andmeid käsitletakse automaatselt „kahjutu statistikuna“, kuigi nad võivad tegelikkuses omada ettevõtjate jaoks suuremat õiguslikku ja majanduslikku mõju kui algandmed ise.

6. ÕIGUSKESKKOND JA SEOS AvTS MUUTMISE VTK-GA KAVANDATUD LAHENDUSTEGA

Andmepõhise aruandluse rakendamist takistavad mitmed kehtivast õigusraamistikust tulenevad kitsaskohad, mis on seotud eeskätt andmete leitavuse, kirjeldatuse, jagatavuse ning andmesubjekti kontrolliga oma andmete kasutamise üle. Justiitsministeeriumi koostatud avaliku teabe seaduse muutmise väljatöötamiskavatsus (VTK) adresseerib mitmeid neist probleemidest ning loob eeldused APA visiooni realiseerimiseks.

Muudatuspaketi eesmärk on:

(i) normeerida andmete kogumise ja jagamise kolm põhistsenaariumi;

(ii) rakendada *once-only* põhimõte diferentseeritult;

(iii) kehtestada teisese kasutuse üldnorm;

(iv) sätestada keskse andmejagamise mehhanismi õiguslik alus;

(v) reguleerida väärindatud andmete jagamist;

(vi) tugevdada põhiandmete kvaliteedi- ja vastutuskohustust.

6.1. Andmete teabevärav kui keskne ligipääsu- ja halduskiht

VTK kohaselt nähakse ette andmete teabevärava kui keskse teenuse õiguslik raamistik, mille eesmärk on võimaldada isikul — sh juriidilisel isikul — hallata oma andmete kasutamist ning saada ülevaade sellest, milliseid andmeid riik tema kohta töötleb ja millised asutused neid kasutavad.

Selle funktsionaalsuse olulisteks komponentideks on:

- **nõusolekuteenus**, mis loob õigusliku ja tehnilise aluse andmete jagamiseks juhtudel, kus jagamine ei tulene otseselt seadusest;
- **andmejälgija**, mis võimaldab andmesubjektil saada ülevaate oma andmete kasutamisest;
- **kasutuslogid**, mis tagavad andmetöötluse läbipaistvuse ja auditeeritavuse.

Selline lahendus on otseselt seotud APA *once-only* põhimõtte rakendamisega, kuna võimaldab andmete korduvkasutust kombineerida andmesubjekti kontrolli ja teadlikkusega.

6.2. Andmekirjelduste reform ja semantiline koosvõime

VTK teine keskne suund on andmekirjelduste kvaliteedi ja sisulisuse tõstmine. Kavandatavad muudatused liiguvad formaalsest andmekogude registreerimisest sisulise andmekirjelduse suunas.

Reformi põhielemendid on:

- **masinloetavus**, mis võimaldab andmete automaatset töötlemist ja ristkasutust;
- **metaandmete standardiseerimine**, mis tagab andmeväljade üheselt mõistetavuse;
- **andmete leitavuse parandamine**, mis võimaldab asutustel tuvastada olemasolevad andmeallikad enne uute andmete kogumist.

Need muudatused loovad tehnilis-õigusliku eelduse *once-only* põhimõtte rakendamiseks, kuna ilma semantiliselt võrreldavate ja kirjeldatud andmeteta ei ole ristkasutus praktiliselt teostatav.

6.3. Andmekogude asutamise paindlikkuse suurendamine

VTK käsitleb ka andmekogude asutamise regulatsiooni jäikust kui olulist takistust andmete rist- ja taaskasutusele. Kehtiv kord, mille kohaselt eeldab andmekogu asutamine sageli Vabariigi Valitsuse määrust, on ajamahukas ning ei võimalda piisavat paindlikkust andmepõhiste teenuste arendamisel.

Kavandatavate muudatuste eesmärk on:

- muuta andmekogude asutamine ja ümberkujundamine kontrollitumaks, kuid menetluslikult lihtsustatumaks;
- võimaldada andmekoosseisude paindlikumat kohandamist;
- soodustada andmete ristkasutust ja taaskasutust uute teenuste ja analüütiliste lahenduste arendamisel.

Selline lähenemine toetab APA visiooni, kuna vähendab institutsionaalseid ja normitehnilisi barjääre andmete liikumisel.

6.4. Sünteetiline hinnang

Kokkuvõtvalt võib hinnata, et VTK-s kavandatud muudatused loovad kolm kriitilist eeltingimust andmepõhise aruandluse rakendamiseks:

- Õiguslikult ja tehniliselt toimiv andmete jagamise taristu (andmete teabevärav, nõusolekuteenused, jälgitavusmehhanismid);
- Semantiliselt kirjeldatud ja masinloetav andmeruum, mis võimaldab andmete automatiseeritud ristkasutust;
- Paindlikum institutsionaalne andmekorraldus, mis võimaldab andmekogude ja andmevoogude dünaamilist kujundamist.

Seetõttu võib järeldada, et VTK ei käsitle üksnes avaliku teabe kättesaadavust, vaid loob laiemas tähenduses õigusliku ja haldusliku vundamendi andmepõhise riigi ning APA-lahenduste süsteemseks rakendamiseks.

6.5. Kriitiline hinnang VTK piisavusele andmepõhise aruandluse vaates

Kuigi VTK-s kavandatud muudatused loovad olulise institutsionaalse ja tehnilise eelduse andmepõhise aruandluse rakendamiseks, ei kata need täielikult kõiki APA visiooni realiseerimiseks vajalikke õiguslikke küsimusi. Alljärgnevalt on välja toodud peamised regulatiivsed lüngad ja arendusvajadused APA perspektiivist.

1. Andmete teisese kasutuse üldnormi puudumine

VTK käsitleb andmete jagamist tehnilise ja korraldusliku probleemina, kuid ei loo piisavalt selget õiguslikku raamistikku andmete teisese kasutuse lubatavuse hindamiseks.

APA kontekstis on keskne küsimus, kas ühel eesmärgil kogutud andmeid võib kasutada teisel avalikul eesmärgil ilma täiendava õigusliku aluseta. Kehtiv regulatsioon käsitleb seda killustatult:

- isikuandmete puhul IKÜM eesmärgipiirangu kaudu;
- mitte-isikuandmete puhul valdavalt eriseaduste tasandil.

Puudub horisontaalne üldnorm, mis määratleks:

- millal on teisene kasutus lubatav;
- millal on vajalik seadusandlik täpsustus;
- millal tuleb rakendada mõjuhindamist.

Ilma sellise normita jääb *once-only* põhimõtte laiem rakendamine õiguslikult ebakindlaks.

2. Väärindatud andmete jagamise regulatsiooni puudujääk

VTK keskendub eeskätt algandmete jagamisele, kuid APA kontekstis on üha olulisem väärindatud andmete liikumine.

Väärindatud andmed hõlmavad:

- arvutuslikke näitajaid,
- riskihinnanguid,
- koondanalüüse,
- järelevalve tulemusi.

Selliste andmete jagamine võib mõjutada ettevõtja õigusi ja kohustusi, mistõttu nende edastamine ei ole neutraalne tehniline toiming.

VTK ei käsitle piisavalt:

- kas väärindatud andmed on uus andmekogum;
- milline asutus vastutab nende õigsuse eest;
- millal on vajalik metoodika avalikustamine;
- millal tuleb välistada automatiseeritud otsustus.

See on oluline regulatsioonilünk APA analüütilise ja järelevalvelise kasutuse vaates.

3. Andmete tundlikkuse klassifikatsiooni puudumine

Kuigi VTK käsitleb juurdepääsupiiranguid ja avaandmeid, ei loo see süsteemset tundlikkuse klassifikatsiooni, mis võimaldaks diferentseerida:

- ristkasutuse lubatavust,
- säilitamistähtaegu,
- ligipääsu tasemeid,
- turvameetmeid.

APA toimimiseks on vajalik mitmetasandiline tundlikkuse mudel, sest *once-only* rakendatavus sõltub otseselt andmete riskiprofiilist.

Ilma klassifikatsioonita jääb jagamisraamistik kas liiga piiravaks (pidurdab ristkasutust) või liiga lahtiseks (tekitab põhiõiguste riske).

4. Põhiandmete kvaliteedi- ja vastutuskohustuse ebapiisav käsitlus

VTK rõhutab andmekirjelduste kvaliteeti, kuid ei käsitle piisavalt põhiandmete sisulist kvaliteeti.

APA eeldab, et ristkasutatavad andmed on õiged, ajakohased ja semantiliselt üheselt mõistetavad.

Puudub selge norm, mis sätestaks põhiandmete kvaliteedikohustuse, vigade parandamise vastutuse ja keskallika andmete prioriteetsuse. Ilma selleta võib ristkasutus suurendada vigade süsteemset levikut.

5. *Once-only* põhimõtte siduva regulatsiooni puudumine

VTK toetab ristkasutust, kuid ei sätesta siduvat kohustust vältida dubleerivat kogumist. APA visiooni realiseerimiseks oleks vajalik:

- norm, mis keelab dubleeriva andmekogumise;
- kohustus kontrollida andmete olemasolu teistes andmekogudes;
- prioriteet ristkasutusele esmase kogumise ees.

Praegu jääb *once-only* pigem poliitikapõhimõtteks kui õiguslikuks kohustuseks.

6. Struktureerimata andmete (vaba tekst) käsitluse piiratus

VTK keskendub struktureeritud andmekirjeldustele, kuid APA praktikas moodustavad olulise osa ka nn struktureerimata andmed nagu näiteks seletuskirjad, hinnangud, analüütilised lisad. Eeltoodu osas puudub terviklik käsitlus kuidas neid metaandmetega kirjeldada, tagada nende leitavus ja rakendada *once-only* põhimõtet dokumentide tasandil.

Kokkuvõte

Kokkuvõtvalt võib hinnata, et VTK loob tugeva aluse andmete tehnilisele jagamisele, andmekirjelduste standardiseerimisele ning nõusolekupõhisele andmehaldusele.

Samas jäävad APA vaates ebapiisavalt reguleerituks:

- Andmete teisese kasutuse üldnorm;
- Väärindatud andmete jagamise raamistik;
- Andmete tundlikkuse klassifikatsioon;
- Põhiandmete kvaliteedi- ja vastutuskohustus;
- *Once-only* siduv rakendusmehhanism;
- Struktureerimata andmete ristkasutus.

Sellest tulenevalt on vajalik käsitleda VTK-d kui olulist, kuid mitte ammendavat sammu andmepõhise aruandluse õigusliku raamistikku kujundamisel.

Allpool on iga juhtumi juurde lisatud vastav normitehniline lahendus.

7. NORMITEHNILISED MUUDATUSETTEPANEKUD

Ettepanek on täiendada avaliku teabe seadust järgmiste regulatsioonidega:

1. Andmete tundlikkuse kategooriad (T1–T5).
2. Andmete ühekordse küsimise ja dubleerimise vältimise kohustus.
3. Andmete teisese kasutuse üldnorm.
4. Põhiandmete kvaliteedi ja jagamiskohustus ning vastutus.
5. Andmekirjelduste miinimumnõuded.
6. Nõusolekupõhise andmejagamise selge volitusnorm.
7. Andmete teabevärava (ATV) seaduslik raamistik.
8. Väärindatud andmete jagamise erisätted.

Need muudatused loovad õigusliku aluse APA diferentseeritud rakendamiseks.

7.1. Avaliku teabe seaduse üldpõhimõtete täiendamine

Kehtiv õigus ei sisalda selget ja siduvat kohustust vältida andmete dubleerivat kogumist olukorras, kus vajalik teave on juba riigi infosüsteemis olemas. Praktikas tähendab see, et ettevõtjatelt nõutakse sageli samu andmeid korduvalt erinevate asutuste poolt, mis suurendab halduskoormust ning ei ole kooskõlas andmepõhise aruandluse eesmärkidega. Lisaks puudub ühtne kohustus kontrollida enne andmete küsimist nende olemasolu teistes andmekogudes ning andmekirjelduse miinimumnõuded ei ole piisavalt selgelt reguleeritud.

Kavandatav säte loob selge õigusliku kohustuse vältida andmete korduvat küsimist ning kehtestab asutustele eelkontrolli kohustuse andmete olemasolu osas. See võimaldab rakendada *once-only* põhimõtet ka esmase andmete kogumise etapis, tagades, et andmeid küsitakse ettevõtjalt vaid siis, kui see on põhjendatud. Samal ajal sätestab see erandid, mis võimaldavad tagada andmete õigsuse, ajakohasuse ning eesmärgipärase kasutamise. Selline regulatsioon vähendab halduskoormust, suurendab andmekasutuse efektiivsust ning loob eelduse ühtsemaks ja läbipaistvamaks andmekorralduseks avalikus sektoris.

Juhtum 1

Ettevõtja annab andmeid konkreetsele asutusele

Probleem:

- Dubleeriv kogumine.
- Puudub kohustus kontrollida, kas andmed on juba riigi valduses.
- Andmekirjelduse miinimumnõuded ei ole seaduse tasandil.

Tabel nr 10. Normitehniline lahendus. Andmete ühekordse küsimise kohustus ehk andmete dubleeriva esitamise vältimine

§ 43². Andmete ühekordse küsimise kohustus

(1) Avaliku sektori asutus ei või nõuda ettevõtjalt või muult kohustatud isikult andmeid, mis on juba riigi infosüsteemis olemas, välja arvatud juhul, kui:

1. andmete õigsus või ajakohasus ei ole tagatud;
2. seadus näeb ette andmete korduva esitamise;
3. andmete kasutamine teisel eesmärgil ei ole õiguslikult lubatud.

(2) Enne andmete nõudmist on asutus kohustatud hindama, kas vajalikud andmed on kättesaadavad mõnes teises andmekogus.

Andmevälja õigusliku kirjelduse kohustus

Kehtivas õiguses puudub ühtne nõue määratleda andmekogusse kogutavate üksikute andmeelementide õiguslikud ja sisulised tunnused, mistõttu on andmete tähendus, kasutusulatus ja jagamise tingimused sageli ebaselged või dokumenteerimata. See raskendab andmete ristkasutust, suurendab õiguslikku ebakindlust ning takistab *once-only* põhimõtte rakendamist, kuna ei ole võimalik üheselt hinnata, millistel tingimustel konkreetset andmevälja võib kasutada või edastada.

Käesolevas õigusanalüüsis on käsitletud, et seaduses peab olema kehtestatud kohustus määrata iga andmeelemendi kohta selle õiguslik alus, töötlemise eesmärk, tundlikkuse kategooria, säilitamistähtaeg ning ristkasutuse lubatavus. Selline lähenemine loob aluse andmete ühtseks ja masinloetavaks kirjeldamiseks, mis võimaldab automatiseeritud ja õiguspärast andmevahetust. Ühtlasi toetab see andmete tundlikkusel põhinevat riskijuhtimist ning suurendab andmete kasutamise läbipaistvust ja kontrollitavust avalikus sektoris.

Tabel nr 11. Andmevälja õigusliku kirjelduse kohustus

Täiendus § 43[3]. (andmekogu regulatsiooni juurde)

(X) Andmekogusse kogutava iga andmeelemendi kohta tuleb määrata:

1. õiguslik alus;
2. töötlemise eesmärk;
3. tundlikkuse kategooria;
4. säilitamistähtaeg;
5. ristkasutuse lubatavus.

Tabel nr 12. Andmete ühekordse küsimise põhimõte

§ 43[4]. Andmete ühekordse küsimise laiendatud põhimõte

(1) Avaliku sektori asutus ei või nõuda ettevõtjalt või muult kohustatud isikult andmeid, mis on juba kogutud mõne teise avaliku sektori asutuse andmekogusse, välja arvatud käesoleva paragrahvi lõikes 4 sätestatud juhtudel.

(2) Avaliku sektori asutused on kohustatud tagama andmete ristkasutuse tehnilised ja õiguslikud eeldused.

(3) Andmete ristkasutus peab toimuma kooskõlas andmete töötlemise eesmärgi, andmete tundlikkuse ning käesolevas seaduses sätestatud piirangutega.

(4) Andmete korduv küsimine on lubatud, kui:

1. see tuleneb seadusest;
2. andmete õigsus ei ole tagatud;
3. andmete kasutamine teisel eesmärgil ei ole õiguslikult lubatud.

Eeltoodud normide näidiste eesmärk on siduda *once-only* põhimõte reaalse jagamiskohustusega.

7.2. Andmete kategoriseerimise õiguslik raamistik

Juhtum 2 ehk keskse andmejagamise punkti toetav regulatsioon

Kehtiv õiguslik raamistik ei reguleeri piisavalt selgelt keskse andmejagamise mehhanismi (teabeevärava) rolli ja toimimist riigi infosüsteemis. Kuigi praktikas liigub areng kesksete andmevahetuse lahenduste suunas, puudub selge õiguslik määratlus, milline on sellise mehhanismi staatus, ülesanded ja piirid. Sellest tulenevalt võib andmete vahendamisega seotud vastutus hajuda erinevate osapoolte vahel, eelkõige küsimuses, kes vastutab andmete õiguspärase edastamise, kasutamise ja turvalisuse eest.

Lisaks puudub kehtivas õiguses selge volitusnorm, mis võimaldaks andmete süstemaatilist ristkasutust läbi keskse mehhanismi. See tekitab õigusliku ebakindluse olukorras, kus andmete taaskasutus võib olla tehniliselt võimalik, kuid õiguslikult vaieldav. Selline ebamäärasus piirab *once-only* põhimõtte rakendamist ning võib viia kas põhjendamatute piiranguteni andmete kasutamisel või vastupidi – riskini, et andmeid kasutatakse ilma piisava õigusliku aluseta.

Seetõttu on vajalik kehtestada selge õiguslik raamistik, mis määratleb keskse andmejagamise mehhanismi rolli, vastutuse ja andmete ristkasutuse alused, tagades ühtaegu nii andmete tõhusa kasutamise kui ka õiguspärasuse ja põhiõiguste kaitse.

Avaliku teabe seaduses (AvTS) puudub selge õiguslik alus andmepõhise aruandluse kesksele toimemehhanismile, mille kaudu ettevõtja saab täita oma andmete esitamise kohustuse ühekordselt. Kehtivas õiguses puudub ühtne regulatsioon, mis võimaldaks andmete süstemaatilist ja turvalist vahendamist erinevate asutuste vahel, mistõttu toimub andmete kogumine killustatult ning dubleerivalt. Avaliku teabe seadusesse tuleb lisada säte, mis võimaldab rakendada *once-only* põhimõtet, tagades samal ajal, et andmete kasutamine on piiratud seadusest tuleneva õigusliku alusega ning et andmete töötlemisel järgitakse läbipaistvuse, turvalisuse ja kontrollitavuse nõudeid. Keskne mehhanism ei või kujuneda iseseisvaks „superandmebaasiks“, vaid peab toimima üksnes vahendina eesmärgipõhiste päringute tegemiseks eri andmekogudesse. Lisaks looks säte vajaliku raamistiku vastutuse selgeks määratlemiseks andmete vahendamisel, mis on eelduseks õiguspärasele ja usaldusväärsele andmevahetusele avalikus sektoris.

Eeltoodust tulenevalt tuleb AvTS täiendada. Järgnevalt on koostatud näidisnorm, mille sarnasega peab AvTS täiendada.

Tabel nr 13. Keskse andmejagamise mehhanismi regulatsioon

§ 43[5]. Keskne andmejagamise mehhanism

(1) Riigi infosüsteemi koosseisus võib toimida keskne andmejagamise mehhanism, mille kaudu ettevõtja esitab andmed ühekordselt.

(2) Keskne andmejagamise mehhanism vahendab andmeid üksnes nendele asutustele, millel on seadusest tulenev õiguslik alus andmete kasutamiseks.

(3) Andmete vahendamisel tuleb tagada:

1. kasutuslogide pidamine;
2. andmete kasutuse läbipaistvus;
3. andmete tundlikkusele vastav ligipääsukontroll.

(4) Keskse mehhanismi vastutava või volitatud töötleja roll määratakse seaduses või selle alusel kehtestatud määruses.

Andmete tundlikkus

Kehtivas õiguses puudub ühtne ja süsteemne raamistik avaliku sektori andmete tundlikkuse hindamiseks, mistõttu käsitletakse andmete töötlemise ja jagamise tingimusi killustatult ning sageli juhtumipõhiselt. Selline lähenemine ei võimalda tagada ühtset praktikat andmete ristkasutuse puhul ning tekitab õiguslikku ebakindlust nii andmeid töötlevatele asutustele kui ka andmesubjektidele. Eelkõige puudub selge alus eristada, millised andmed on sobivad laiemaks ristkasutuseks ning milliste puhul tuleb kohaldada rangemaid piiranguid.

Kavandatav säte loob aluse andmete tundlikkuse süsteemseks kategoriseerimiseks, sidudes andmete töötlemise ja jagamise tingimused nende riskiprofiiliga. See võimaldab rakendada diferentseeritud lähenemist, kus kõrgema tundlikkusega andmete puhul kehtivad rangemad juurdepääsu- ja kasutusreeglid, samas kui madalama riskiga andmete ristkasutus on lihtsustatud. Ühtlasi loob säte aluse detailsemate reeglite kehtestamiseks määruse tasandil, tagades paindlikkuse ning võimaluse arvestada erinevate andmeliikide eripärasid. Selline lähenemine toetab *once-only* põhimõtte rakendamist, vähendades halduskoormust, kuid säilitades samal ajal andmekaitse ja konfidentsiaalsuse nõuete järgimise.

Tabel nr 14. Andmete tundlikkuse kategooriad

§ 43[6]. Avaliku sektori andmete tundlikkuse kategooriad

(1) Avaliku sektori andmed jaotatakse nende töötlemise, jagamise ja avalikustamise tingimuste määramiseks tundlikkuse kategooriatesse.

(2) Andmete tundlikkuse hindamisel võetakse arvesse eelkõige:

1. isikuandmete sisaldumist;
2. ärisaladuse või maksusaladuse olemasolu;
3. mõju andmesubjekti või ettevõtja õigustele ja kohustustele;
4. avalikustamisest tulenevat võimalikku kahju.

(3) Andmete tundlikkuse kategooriad ning nendele vastavad töötlemise ja jagamise tingimused kehtestatakse Vabariigi Valitsuse määrusega.

Nõusolekupõhine jagamine

Kehtiv õiguslik raamistik ei kata piisavalt olukordi, kus andmete jagamiseks puudub otsene seaduslik alus, kuid andmete ristkasutus oleks sisuliselt põhjendatud ja vajalik. Sellistel juhtudel puudub selge

mehhanism, mis võimaldaks andmete õiguspärast edastamist, mistõttu jääb potentsiaalne andmete taaskasutus kasutamata või toimub õiguslikult ebakindlal alusel. See piirab andmepõhise aruandluse rakendamist ning takistab paindlike ja kasutajakesksete lahenduste kujundamist.

Kavandatav säte loob õigusliku aluse nõusolekupõhisele andmete jagamisele, võimaldades ettevõtjal ise otsustada oma andmete kasutamise üle olukordades, kus seadusest tulenevat kohustust ei ole. Nõusoleku sisulised nõuded – teadlikkus, vabatahtlikkus ja eesmärgipõhisus – tagavad, et andmete jagamine toimub kooskõlas andmekaitse põhimõtetega ning ei riiva ebaproportsionaalselt andmesubjekti õigusi. Riikliku nõusolekuteenuse kasutamise võimalus loob omakorda tehnilise ja organisatsioonilise raamistiku nõusolekute haldamiseks, suurendades läbipaistvust ja kontrollitavust. Selline lähenemine toetab andmete turvalist ristkasutust ning võimaldab laiendada *once-only* põhimõtte rakendamist ka juhtumitele, kus seaduslik alus puudub.

Tabel nr 15. Nõusolekupõhine andmete jagamine

§ 43[7]. Nõusolekupõhine andmete jagamine
(1) Kui andmete jagamine ei tulene otseselt seadusest, võib andmeid edastada ettevõtja nõusoleku alusel. (2) Nõusolek peab olema: 1. teadlik; 2. vabatahtlik; 3. eristatav ja konkreetse eesmärgiga seotud. (3) Nõusoleku haldamiseks võib kasutada riiklikku nõusolekuteenust.

7.3. Ristkasutuse ja teisese töötlemise regulatsioon

Juhtum 3 ehk asutustevaheline väärindatud andmete jagamine

Teisese kasutuse ja väärindatud andmete jagamise regulatsiooni vajadus

Juhtumipõhine analüüs näitab, et andmepõhise aruandluse kontekstis kujutab endast eraldi ja õiguslikult keerukamat kategooriat asutustevaheline väärindatud andmete jagamine (Juhtum III). Erinevalt esmase kogumise või tehnilise vahendamise mudelitest ei seisne see mudel andmete pelgalt edastamises, vaid nende edasises töötlemises, analüüsimises ja tõlgendamises. Sellise tegevuse tulemusena tekivad väärindatud andmed, millel võib olla otsene mõju isikute või ettevõtjate õigustele ja kohustustele.

Kehtiv õigusraamistik ei käsitle piisava selgusega andmete teisest kasutust ega väärindatud andmete jagamist. Eelkõige puudub üldnorm, mis määratleks, millistel tingimustel võib üks asutus kasutada teise asutuse kogutud andmeid uuel eesmärgil. Samuti ei ole selgelt reguleeritud, millised täiendavad nõuded kohalduvad olukorras, kus andmete töötlemise tulemusel tekivad uued, otsustusliku tähendusega andmed. See loob õigusselgusetuse ning võib kaasa tuua nii põhiõiguste riive kui ka vastutuse hajumise.

Sellest tulenevalt on vajalik kehtestada eraldi normid, mis reguleerivad (i) andmete teisest kasutust ning (ii) väärindatud andmete jagamist.

Teisese kasutuse üldnorm

Ettepaneku kohaselt täiendatakse avaliku teabe seadust uue paragrahviga, mis sätestab andmete teisese kasutuse üldpõhimõtted. Selle sätte eesmärk on luua selge õiguslik alus olukordadeks, kus avaliku sektori asutus soovib kasutada teise asutuse kogutud andmeid oma ülesannete täitmiseks.

Kavandatav regulatsioon lähtub kahest põhimõttest. Esiteks on teisene kasutus lubatav juhul, kui see on kooskõlas andmete esialgse kogumise eesmärgiga. See tagab kooskõla eesmärgipiirangu põhimõttega ning välistab andmete kasutamist viisil, mis oleks andmesubjekti jaoks ettenägematu. Teiseks võimaldab säte seadusandjal ette näha erijuhud, kus teisene kasutus on lubatud ka algsest eesmärgist erinevalt, kui see on õiguspoliitiliselt põhjendatud.

Lisaks eristab säte isikuandmete ja mitte-isikuandmete teisest kasutust. Isikuandmete puhul tuleb alati järgida isikuandmete kaitse üldmääruse nõudeid, samas kui mitte-isikuandmete puhul on lähenemine paindlikum, eeldusel et seadusest ei tulene piiranguid. Selline diferentseerimine võimaldab tasakaalustada andmete kasutamise efektiivsust ja põhiõiguste kaitset.

Tabel nr 16. Andmete teisene kasutamine

§ 43[8]. Andmete teisene kasutamine
(1) Avaliku sektori asutus võib kasutada teise asutuse kogutud andmeid oma avaliku ülesande täitmiseks, kui: 1. töötlemine on kooskõlas andmete esialgse kogumise eesmärgiga; või 2. teisene kasutus on sätestatud seaduses. (2) Isikuandmete teisene kasutamine peab vastama isikuandmete kaitse üldmääruse nõuetele. (3) Mitte-isikuandmete teisene kasutamine on lubatud, kui seadusest ei tulene teisiti.

<u>Väärindatud andmete eriregulatsioon</u>

Juhtumi III puhul ei piisa üksnes teisese kasutuse lubatavuse määratlemisest. Kui andmete töötlemise tulemusena tekivad väärindatud andmed (nt riskihinnangud, koondnäitajad või analüütilised järeldused), võib nende kasutamine mõjutada otseselt isikute või ettevõtjate õigusi.

Seetõttu on ettepanek täiendada seadust uue paragrahviga, mis sätestab väärindatud andmete jagamise eritingimused. Sätte keskne eesmärk on tagada, et selliste andmete kasutamine oleks läbipaistev, kontrollitav ja allutatud õiguslikule vastutusele.

Eelkõige nähakse ette kohustus hinnata, kas väärindatud andmetel on otsene mõju õigustele või kohustustele. Mõju olemasolu korral tuleb tagada andmete töötlemise metoodika läbipaistvus, määratleda vastutav asutus ning vajaduse korral viia läbi mõjuhindamine. See on oluline, et vältida olukordi, kus otsused põhinevad ebaselgetel või kontrollimatutel algoritmidel või analüüsidel.

Samuti sätestatakse, et väärindatud andmete kasutamine ei või viia automaatsete otsusteni ilma selgesõnalise seadusliku aluseta. See on kooskõlas nii põhiseaduslike põhiõiguste kaitse nõuetega kui ka isikuandmete kaitse üldmääruse regulatsiooniga.

Tabel nr 17. Väärindatud andmete jagamine

§ 43[9]. Väärindatud andmete jagamine

(1) Väärindatud andmete jagamisel tuleb hinnata, kas andmetel on otsene mõju isiku või ettevõtja õigustele või kohustustele.

(2) Kui väärindatud andmed omavad otsest mõju, tuleb tagada:

1. andmete metoodika läbipaistvus;
2. vastutava asutuse määratlemine;
3. vajaduse korral mõjuhindamine.

(3) Väärindatud andmete jagamine ei või viia automaatse otsustuseni ilma seaduses sätestatud aluseta.

Andmete tundlikkusel põhinev riskijuhtimine

Teisese kasutuse ja väärindatud andmete regulatsiooni täiendamiseks on vajalik ka ühtne riskijuhtimise raamistik. Selleks nähakse ette uus paragrahv, mis kehtestab andmete tundlikkuse kategooriad ning seob need andmete kasutamise ja jagamise tingimustega.

Sätte kohaselt jaotatakse avaliku sektori andmed tundlikkuse kategooriatesse, lähtudes nende mõjust isikute või ettevõtjate õigustele ja huvidele. Tundlikkuse kategooria määrab, millistel tingimustel on andmete jagamine ja teisene kasutus lubatav, ning võimaldab rakendada diferentseeritud lähenemist erinevatele andmeliikidele.

Selline lahendus loob sidusa seose andmetüüpide kaardistuse, riskihindamise ning normitehniliste piirangute vahel. Ühtlasi võimaldab see rakendada *once-only* põhimõtet viisil, mis arvestab nii andmete kasutamise efektiivsust kui ka sellega kaasnevaid riske.

Tabel nr 18. Andmete tundlikkuse diferentseeritud käsitlus

§ 43[10]. Andmete tundlikkuse diferentseeritud käsitlus
(1) Avaliku sektori andmed jaotatakse tundlikkuse kategooriatesse vastavalt nende mõjule isiku või ettevõtja õigustele ja huvidele. (2) Tundlikkuse kategooria määrab andmete jagamise ja teisese kasutuse tingimused. (3) Tundlikkuse klassifikaator kehtestatakse Vabariigi Valitsuse määrusega.

Kokkuvõte

Kokkuvõttes on teisese kasutuse üldnormi, väärindatud andmete eriregulatsiooni ning tundlikkusepõhise riskijuhtimise kehtestamine vajalik, et võimaldada asutustevahelist andmete ristkasutust õiguspärasel ja läbipaistval viisil. Kavandatavad muudatused loovad õigusliku selguse, vähendavad vastutuse hajumist ning tagavad, et andmete kasutamine ei tooks kaasa põhjendamatut põhiõiguste riivet. Samal ajal loovad need eeldused andmepõhise aruandluse ja *once-only* põhimõtte tõhusaks rakendamiseks avalikus sektoris.

7.4. Andmekirjelduse ja kvaliteedi nõuded

Käesoleva õigusanalüüsi üks keskseid järeldusi on, et andmepõhise aruandluse toimimine eeldab lisaks andmete kogumise ja jagamise õiguslikele alustele ka andmete ühtset ja piisavalt detailset kirjeldamist. Avaliku teabe seaduse muutmise väljatöötamiskavatsuses (VTK) on ühe olulise suunana rõhutatud andmekirjelduste kvaliteedi ja masinloetavuse parandamist, kuid kehtivas õiguses puuduvad selged ja siduvad miinimumnõuded andmeelementide kirjeldamiseks.

Praegune olukord, kus andmekogude andmekirjeldused on ebaühtlased või osaliselt määratletud, takistab andmete semantilist koosvõimet ning piirab oluliselt andmete ristkasutust. Kui andmeelemendi sisu, päritolu või kasutustingimused ei ole üheselt arusaadavad, ei ole võimalik hinnata andmete kasutamise õiguspärasust ega rakendada automatiseeritud andmevahetust. See omakorda piirab once-only põhimõtte rakendamist ning suurendab vajadust andmete korduvaks küsimiseks ettevõtjatelt.

Sellest tulenevalt on vajalik kehtestada seaduse tasandil andmekirjelduste miinimumnõuded, mis loovad ühtse aluse andmete tähenduse, kasutuspiirangute ja kvaliteedi hindamiseks. Kavandatav uus paragrahv sätestab kohustuse kirjeldada kõik avaliku sektori andmekogude andmeelemendid masinloetaval kujul, mis on eelduseks automatiseeritud andmevahetusele ning infosüsteemide koosvõimele.

Sätte lõikes 2 loetletud miinimumandmed täidavad mitut omavahel seotud eesmärki. Andmeelemendi nimetus ja andmesubjekti või objekti kategooria tagavad semantilise selguse, võimaldades erinevatel asutustel mõista andmete sisu ühtemoodi. Õigusliku aluse, tundlikkuse taseme ning jagamise tingimuste kirjeldamine võimaldab hinnata andmete töötlemise lubatavust ja piiranguid, mis on eriti oluline andmete teisese kasutuse ja asutustevahelise jagamise kontekstis. Andmete allika ja säilitustähtaja määratlemine toetab andmete kvaliteedi ja ajakohasuse kontrolli ning võimaldab tagada vastavuse andmekaitse põhimõtetega.

Tabel nr 19. Andmekirjelduste koostamise nõuded

§ 43[11]. Andmekirjelduste koostamise nõuded

(1) Avaliku sektori andmekogude andmeelemendid peavad olema kirjeldatud masinloetaval kujul.

(2) Andmekirjeldus peab sisaldama vähemalt:

1. andmeelemendi nimetust;
2. õiguslikku alust kogumiseks;
3. andmesubjekti või objekti kategooriat;
4. andmete tundlikkuse taset;
5. andmete allikat;
6. jagamise tingimusi;
7. säilitustähtaega.

(3) Täpsemad tehnilised nõuded kehtestatakse määrusega.

Seaduse tasandil kehtestatud miinimumnõudeid täiendavad määruse tasandil sätestatavad tehnilised standardid, mis võimaldavad ühtlustada andmekirjelduste vormingut, klassifikaatoreid ja metaandmete struktuuri. Selline kahetasandiline regulatsioon (seadus + määrus) tagab ühtaegu piisava õigusliku selguse ja vajaliku paindlikkuse tehniliste lahenduste arendamisel.

Kokkuvõttes loob andmekirjelduste miinimumnõuete kehtestamine eelduse andmete kvaliteedi paranemiseks, semantilise koosvõime saavutamiseks ning andmete õiguspäraseks ja tõhusaks ristkasutuseks. Ilma sellise regulatsioonita ei ole võimalik realiseerida andmepõhise aruandluse keskseid eesmärke ega vähendada ettevõtjate halduskoormust süsteemselt.

7.5. Põhiandmete kvaliteedikohustus

Andmepõhise aruandluse rakendamise üks keskseid eeldusi on andmete kvaliteet. Once-only põhimõtte toimimine eeldab, et riigi infosüsteemides olemasolevad andmed on usaldusväärsed, ajakohased ning tehniliselt kasutatavad erinevate asutuste poolt. Kui andmete kvaliteet ei ole tagatud, ei ole võimalik andmeid korduvkasutada ning asutused on sunnitud andmeid ettevõtjatelt uuesti küsima, mis suurendab halduskoormust ja vähendab usaldust riigi andmekorralduse vastu.

Kehtivas õiguses puudub siiski ühtne ja selgesõnaline kohustus, mis määratleks põhiandmete kvaliteedi tagamise nõuded ning vastutuse nende täitmise eest. Kuigi andmekogude põhimäärustes võib olla sätestatud üksikuid kvaliteedinõudeid, ei ole need süsteemsed ega ühtlustatud. See loob olukorra, kus andmete kvaliteet varieerub andmekogude lõikes ning andmete ristkasutus muutub õiguslikult ja tehniliselt ebakindlaks.

Sellest tulenevalt on vajalik kehtestada Avaliku teabe seaduses eraldi säte, mis määratleb põhiandmete kvaliteedi tagamise kohustuse ning seob selle andmete jagamise ja kasutamise võimalikkusega. Kavandatav uus norm paneb põhiandmeid sisaldava andmekogu vastutavale töötlejale selgesõnalise kohustuse tagada andmete õigsus, ajakohasus, tehniline koosvõime ning jagatavus teistele õigustatud isikutele.

Andmete õigsuse ja ajakohasuse nõue on eelduseks, et andmeid saab kasutada haldusotsuste tegemisel ja muudes avaliku võimu tegevustes ilma täiendava kontrollita. Tehnilise koosvõime nõue tagab, et andmed on kasutatavad erinevates infosüsteemides ning vastavad ühtsetele standarditele. Jagatavuse nõue seob andmete kvaliteedi otseselt once-only põhimõttega, kuna ainult kvaliteetseid andmeid on võimalik turvaliselt ja õiguspäraselt teistele asutustele edastada.

Lisaks nähakse ette, et põhiandmete jagamise teenus peab vastama kehtestatud miinimumnõuetele. See tähendab, et andmete kvaliteet ei ole üksnes andmekogu sisemine küsimus, vaid peab olema tagatud ka andmete edastamise tasandil, sealhulgas ligipääsutingimuste, tehniliste standardite ja teenuse töökindluse osas.

Tabel nr 20. Põhiandmete kvaliteedi tagamine

§ 43[12]. Põhiandmete kvaliteedi tagamine
(1) Põhiandmeid sisaldava andmekogu vastutav töötleja on kohustatud tagama: 1. andmete õigsuse; 2. ajakohasuse; 3. tehnilise koosvõime;

4. jagatavuse teistele õigustatud isikutele.

(2) Põhiandmete jagamise teenus peab vastama kehtestatud miinimumnõuetele.

Kokkuvõttes loob põhiandmete kvaliteedikohustuse kehtestamine eelduse usaldusväärseks andmekorralduseks, kus andmeid saab kasutada korduvkasutatava ressursina. Ilma sellise kohustuseta ei ole võimalik realiseerida andmepõhise aruandluse eesmärke ega tagada, et once-only põhimõte toimib praktikas, mitte üksnes deklaratiivse põhimõttena.

7.6. Rakendusmääruste vajadus ja roll

Käesoleva õigusanalüüsi tulemused näitavad, et andmepõhise aruandluse rakendamine ei ole saavutatav üksnes seaduse tasandil kehtestatud üldpõhimõtete kaudu, vaid eeldab nende täpsustamist ja operatsionaliseerimist määruste tasandil. Seadus loob õigusliku raamistiku ja põhimõtted, kuid andmete tegelik kasutamine, jagamine ja haldamine avalikus sektoris sõltub suurel määral ühtsetest tehnilistest ja korralduslikest standarditest.

Eelkõige on määruste tasandil vajalik täpsustada andmete kirjeldamise, jagamise ja kasutamise praktilised nõuded, et tagada andmete semantiline koosvõime, tehniline ühilduvus ning õiguspärane kasutamine erinevate asutuste vahel. Ilma selliste täpsustavate regulatsioonideta jäävad seaduses sätestatud põhimõtted deklaratiivseks ning ei võimalda realiseerida once-only põhimõtet ega vähendada ettevõtjate halduskoormust.

Sellest tulenevalt on vajalik kehtestada vähemalt järgmised rakendusmäärused.

Esiteks on vajalik andmete tundlikkuse klassifikaator, mis võimaldab jaotada andmed ühtsetesse kategooriatesse ning siduda need konkreetsete töötlemise ja jagamise tingimustega. See loob aluse riskipõhisele lähenemisele ning võimaldab diferentseerida andmete kasutamise reegleid vastavalt nende mõjule isikute ja ettevõtjate õigustele.

Teiseks on vajalik andmekirjelduste tehniline standard, mis määratleb andmeelementide kirjeldamise ühtse vormingu, kasutatavad klassifikaatorid ning metaandmete struktuuri. See on eelduseks andmete semantilisele koosvõimele ja automatiseeritud andmevahetusele.

Kolmandaks tuleb kehtestada põhiandmete jagamise teenuse nõuded, mis tagavad, et andmete edastamine toimub turvaliselt, usaldusväärselt ning kooskõlas kehtivate õiguslike piirangutega. See hõlmab muu hulgas ligipääsukontrolli, logimise, töökindluse ja teenuse kvaliteedi nõudeid.

Neljandaks on vajalik once-only põhimõtte rakendamise juhend, mis annab asutustele praktilised suunised andmete korduvkasutuse korraldamiseks ning aitab ühtlustada praktikat erinevate asutuste vahel. Selline juhend on oluline eelkõige olukordades, kus õiguslik raamistik võimaldab mitut tõlgendust.

Viiendaks tuleb kehtestada nõusolekuteenuse tehnilised reeglid, mis määratlevad nõusoleku andmise, haldamise ja kontrollimise mehhanismid. See on vajalik, et tagada nõusolekupõhise andmejagamise läbipaistvus, jälgitavus ning vastavus kehtivatele andmekaitsenõuetele.

Kokkuvõttes moodustavad nimetatud määrused koos seaduse tasandil kehtestatud normidega tervikliku regulatiivse raamistiku, mis võimaldab andmepõhise aruandluse lahenduste praktilist rakendamist ning tagab andmete turvalise ja õiguspärase kasutamise avalikus sektoris.

7.7. Lõppjäreldus

Käesoleva õigusanalüüsi põhjal järeldub, et andmepõhise aruandluse edukas rakendamine eeldab terviklikku ja süsteemset lähenemist andmete õiguslikule ja tehnilisele korraldusele. APA ei ole käsitatav üksnes tehnilise lahendusena, vaid kujutab endast õiguslikult struktureeritud andmekorralduse mudelit, mille toimimine sõltub selgetest normidest, standarditest ja rollijaotusest.

Analüüs näitab, et APA rakendamise eelduseks on eelkõige:

- andmete õiguslik kategoriseerimine;
- andmete tundlikkuse diferentseeritud hindamine;
- andmete rist- ja teisese kasutuse selge normeerimine;
- metaandmete standardiseerimine;
- ning nõusolekupõhise andmejagamise võimaldamine.

Seejuures ei ole once-only põhimõte universaalne ega automaatselt kõigile andmetele kohaldatav. Selle rakendatavus sõltub otseselt andmete liigist, nende tundlikkusest ning töötlemise eesmärgist. Once-only ei ole seega pelgalt tehniline funktsioon, vaid õiguslik konstruktsioon, mille kohaldamine eeldab riskipõhist lähenemist ja selget regulatiivset raamistikku.

Täiendavalt kinnitab analüüs, et APA toimimine eeldab:

- andmete semantilist standardiseerimist;
- tundlikkusepõhist riskijuhtimist;
- teisese kasutuse üldnormi kehtestamist;
- põhiandmete kvaliteedikohustust;
- ning kontrollitud, sealhulgas nõusolekupõhist andmejagamise mudelit.

<u>Metaandmete (andmekirjelduse) miinimumnõuded</u>

Analüüsi tulemusel on võimalik sõnastada ka andmete kirjeldamise miinimumnõuded, mis on eelduseks andmete õiguspäraseks kasutamiseks ja ristkasutuseks. Käesolevas analüüsis kasutatakse peamiselt läbivalt terminit metaandmed, mille all mõistetakse andmevälja või andmeelemendi kirjeldust (st nn andmekirjeldust). Terminoloogilise ühtsuse huvides käsitletakse mõisteid „andmekirjeldus“ ja „andmevälja kirjeldus“ metaandmete osana. Käesolevas alajaotuses esitatud 13-elementi metaandmete miinimumkoosseis on analüütiline raamistik. Seaduse tasandil kehtestatav § 43^{10} hõlmab sellest kohustuslikud elemendid, ülejäänud detailsemad nõuded saab sätestada määruste ja tehniliste standarditega.

Iga andmeväli peab olema varustatud vähemalt järgmiste metaandmetega:

1. andme nimetus;
2. õiguslik alus töötlemiseks (sh kogumiseks ja jagamiseks);
3. andmesubjekti või objekti kategooria;
4. andme omanik;
5. andmete allikas;
6. teave selle kohta, kas tegemist on põhiandmetega;

7. andmete tundlikkuse tase;
8. andmete jagamise piirangud;
9. säilitustähtaeg;
10. andmete granulaarsus;
11. kasutatavad klassifikaatorid või standardid;
12. masinloetavuse tase;
13. andmete õigsuse kontrollimise ja uuendamise põhimõtted.

Selline metaandmete miinimumkoosseis võimaldab ühtlustada andmete kirjeldamist, tagada nende semantilise koosvõime ning hinnata andmete kasutamise õiguspärasust erinevates töötlemisstsenaariumides.

Kokkuvõte

Kokkuvõttes näitab analüüs, et andmepõhise aruandluse rakendamine ei sõltu üksnes tehnoloogilistest lahendustest, vaid eeldab selget ja diferentseeritud õiguslikku raamistikku. Keskseks muutub andmete käsitlemine struktureeritud ja kirjeldatud ressursina, mille kasutamine on seotud nii õiguslike piirangute kui ka kvaliteedinõuetega.

Selline lähenemine võimaldab ühtaegu vähendada ettevõtjate halduskoormust ning tagada andmete turvalise, läbipaistva ja õiguspärase kasutamise avalikus sektoris.

Kasutatud allikad

Kasutatud kirjandus

1. Andmekaitse Inspektsioon. Andmekogude juhend. 2013. – https://www.aki.ee/sites/default/files/dokumendid/andmekogude_juhend.pdf (30.03.2026).
2. Andmekaitse Inspektsioon. Andmeladude seire kokkuvõte. – https://www.aki.ee/sites/default/files/seired/andmeladude_seire_kokkuvote.pdf (30.03.2026).
3. Brewczyńska, M. A critical reflection on the material scope of the application of the Law Enforcement Directive and its boundaries with the General Data Protection Regulation. – Research handbook on EU data protection law. Cheltenham: Edward Elgar Publishing Ltd 2022.
4. Commission Expert Group. Minutes of the meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 (4 May 2017).
5. Majandus- ja Kommunikatsiooniministeerium. Andmeladude olemus ja selle funktsioonid. Selgitav juhis. 2023. – https://www.kratid.ee/_files/ugd/980182_5b9c740580a543c0ab48480b07c7ce5f.pdf (30.03.2026).
6. Mikiver, M. Analüüs. Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile. Justiitsministeerium 2021. – https://www.just.ee/media/3193/download (30.03.2026).
7. Vogiatzoglou, P., Fantin, S. National and public security within and beyond the Police Directive.- Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. Cambridge, Antwerp, Chicago: Intersentia, 2019. Lk 27-62.
8. Värk, K. Isikuandmete vastutava ja volitatud töötleja kontseptsiooni rakendamine andmekogudes. Magistritöö. Juhendajad Julia Antonova, Paloma Krõõt Tupay. Tartu: TÜ õigusteaduskond 2021.

Kasutatud euroopa liidu õigusaktid

9. 13. detsembri 2023. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2023/2854, ühtlustatud õigusnormide kohta, millega reguleeritakse õiglast juurdepääsu andmetele ja andmete kasutamist, millega muudetakse määrust (EL) 2017/2394 ja direktiivi (EL) 2020/1828 (andmemäärus). – ELT L.
10. 14. detsembri 2022. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2464, millega muudetakse määrust (EL) nr 537/2014, direktiivi 2004/109/EÜ, direktiivi 2006/43/EÜ ja direktiivi 2013/34/EL seoses äriühingute kestlikkusaruandlusega. – ELT L 322, lk 15.
11. 20. juuni 2019. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2019/1024, avaandmete ja avaliku sektori valduses oleva teabe taaskasutamise kohta (uuesti sõnastatud). – ELT L 172, lk 56–83.
12. 23. juuli 2014. aasta Euroopa Parlamendi ja nõukogu määrus (EL) nr 910/2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. – ELT L 257, lk 73.
13. 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/679, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).- ELT L 119, lk 1.

14. 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK.- ELT L 119, lk 89.
15. 30. mai 2022. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2022/868, Euroopa andmehalduse kohta ning millega muudetakse määrust (EL) 2018/1724 (andmehalduse määrus). – ELT L 152, lk 1–44.

Kasutatud eesti õigusaktid

16. Avaliku teabe seadus.- RT I, 06.03.2026, 3.
17. Eesti Vabariigi põhiseadus.- RT I, 11.04.2025, 3.
18. E-identimise ja e-tehingute usaldusteenuste seadus, RT I, 30.12.2025, 16.
19. Haldusmenetluse seadus.- RT I, 06.07.2023, 31.
20. Isikuandmete kaitse seadus.- RT I, 06.03.2026, 10.
21. Isikut tõendavate dokumentide seadus.- RT I, 26.06.2025, 6.
22. Küberturvalisuse seadus.- RT I, 30.12.2025, 15.
23. Maksukorralduse seadus.- RT I, 02.10.2025, 4.
24. Raamatupidamise seadus.- RT I, 10.07.2025, 3.
25. Riikliku statistika seadus.- RT I, 11.03.2022, 2.
26. Tsiviilseadustiku üldosa seadus.- RT I, 31.12.2024, 48.
27. Infosüsteemide andmevahetuskiht.- RT I, 06.08.2019, 17.
28. Klassifikaatorite süsteem.- RT I 2008, 4, 27.
29. Riigi infosüsteemi haldussüsteem.- RT I, 29.12.2024, 15.
30. Tervise infosüsteemi põhimäärus.- RT I, 10.12.2025, 3.