

FinEst Centre
for Smart Cities

Personaalse andmeruumi teostatavusuuring

Lõppraport

2026



Rahastanud Euroopa Liit
NextGenerationEU



Eesti
tuleviku heaks

Teostaja: FinEst Targa Linna Tippkeskus, Tallinna Tehnikaülikool

Koostajad (tähestikulises järjekorras): Kärt Salumaa-Lepik, Ralf-Martin Soe, Sille Sepp, Taivo Kangilaski

Tellija: Justiits- ja Digiministeerium

Kuupäev: 31.03.2026

Projekt on rahastatud Euroopa Liidu NextGenerationEU vahenditest.



Tänu sõnad

Käesoleva uuringu tulemusteni on jõutud tänu intervjueeritud ekspertide panusele, seega autorid soovivad siiralt tänada kõiki kaasatud eksperte, sh iGrant.io (Lal Chandran), EdTech Estonia (Märt Aro), Cachet (Hedi Mardisoo, Kristjan Aruoja), Liikluskindlustusfond ning Eesti Kindlustusseltside Liit (Martti Merila ja Tuuli Pärenson) ning kõik teised anonüümseks jääda soovinud eksperdid järgnevatest organisatsioonidest – Athumi, CompensaLife, CreditInfo, ELIIS, Haridus- ja Teadusministeerium, Justiits- ja Digiministeerium, Kutsekoda, LHV, Majandus- ja Kommunikatsiooniministeerium, PZU, Riigi Infosüsteemi Amet, Tallinna Tehnikaülikool ja Töötukassa. Samuti soovivad autorid tänada uuringu tellija esindajaid (Kaarel Sepp ja Kuldar Aas) mitmekülgse toe eest.

Sisukord

Lühikokkuvõte	6
1. Sissejuhatus	9
1.1 Inimkeskne vaade andmemajandusele	11
1.2 Poliitiline tahe ja andmemajanduslik potentsiaal	13
1.3 Õiguslik vaade inimeste andmete korraldusele	15
2. Teostatavusuuringu läbiviimine	17
2.1 Uurimiseesmärk ja -küsimused	17
2.2 Uuringuprojekti ulatus ning piirangud	18
2.3 Metodoloogia ning sidusrühmade kaasamine	20
3. Mis on personaalne andmeruum?	22
4.1 Väärtuspakkumine inimesele	25
4.2 Väärtuspakkumine organisatsioonidele	28
4.3 Näiteid Eestist ja mujalt	29
4. Ärivajadused	32
3.1 Andmepõhiste toodete ja teenuste pakkumisest tulenevad vajadused	32
3.2 Tehnoloogiast ja andmetaristust tulenevad vajadused	34
3.3 Ärikeskkonnast ja ühiskondlikust nõudlusest tulenevad vajadused	35
5. Võimekused ja eeldused inimkeskse andmemajanduse toetamiseks	37
5.1 Ärilised aspektid, eeldused ja väljakutsed	37
5.2 Õiguslikud aspektid, eeldused ja väljakutsed	38
5.3 Funktsionaalsed võimekused	43
5.3.1 Kontrolli ja läbipaistvust võimaldavad teenused	43
5.3.2 Andmevahetust võimaldavad ja toetavad teenused	44
5.3.3 Lisaväärtusteenused	45
5.4 Tehnoloogilised komponendid ja nende rakendusarhitektuur	46
5.4.1 Identiteedihalduse komponent	46
5.4.2 Nõusoleku halduse komponent	47
5.4.3 Andmevahenduse komponent	47
5.4.4 Auditi ja logimise komponent	47
5.4.5 Personaalse andmeruumi vaate rakendusteenus	48
5.4.6 Komponentide koostöömudel ja päringu tüüpiline elutsükel	48
6. Rollimudel	50
6.1 Otseselt andmevahetuses osalevad rollid	50
6.2 Andmevahendust toetavad rollid	51
6.3 Andmeökosüsteemi kui terviku haldamise eest vastutavad rollid	52
7. Personaalse andmeruumi esialgsed kasutuslood	55
8. Valitud kasutusjuhtude teostatavusanalüüs	57
8.1 Elukindlustus	57
8.1.1 Elukindlustuslepingu sõlmimise <i>as-is</i> ja <i>to-be</i> analüüs	58
8.1.2 Rollimudel ja osapoolte kaardistus	63
8.1.3. Äriline vaade	63
8.1.4. Tehnoloogiline vaade	65
8.1.5. Õiguslik vaade	66
8.2 Oskuste ja haridusandmete põhine teenus	68
8.2.1 Värbamise ja tööleasumise protsessi <i>as-is</i> ja <i>to-be</i> analüüs	69
8.2.2 Rollimudel ja osapoolte kaardistus	76
8.2.3. Äriline vaade	77
8.2.4. Tehnoloogiline vaade	79
8.2.5. Õiguslik vaade	80
9. Personaalse andmeruumi arengu võimalused	83
9.1 Nõusolekupõhisus ja/või privaatsust kaitsvate tehnoloogiate laiem rakendamine	83

9.2 Alternatiivsed väärtusloome stsenaariumid	84
9.3 Andmealased koostöömudelid	86
9.4. Väljakutsed ja võimalused	86
10. Soovitused ja teekaart	90
10.1 Soovitused personaalse andmeruumi lahenduste arendamiseks	90
10.2 Teekaart personaalse andmeruumi rakendamiseks	94
11. Kasutatud kirjandus	96
Lisad	101
Lisa 1: Intervjueeritud organisatsioonid	101
Lisa 2: Intervjuu kava	102
Lisa 3: Intervjuu kava 2	103

Lühendid

AI – *Artificial Intelligence*, tehisintellekt

AKI – Andmekaitse Inspeksioon

AML-kontroll – *Anti-Money Laundering control*, rahapesu ja terrorismi rahastamise tõkestamisega seotud kontrollimeetmete kogum

B2B – *Business-to-Business*, äri-äri

B2C – *Business-to-Consumer*, äri-lõpptarbijale

B2G – *Business-to-Government*, äri-avaliku sektori asutustele (sh riigiasutused, kohalikud omavalitsused jt)

DA – *Data Act*, andmemäärus

DGA – *Data Governance Act*, andmehaldusmäärus

DMA – *Digital Markets Act*, digiturgude määrus

DSSC – *Data Spaces Support Centre*, andmeruumide tugikeskus

EDPB – *European Data Protection Board*, Euroopa Andmekaitse nõukogu

EHIS – Eesti Hariduse Infosüsteem

eID – elektrooniline identiteet, digiidentiteet

eIDAS – *Regulation on electronic identification and trust services*, Elektroonilise identifitseerimise ja usaldusteenuste määrus

EMTA – Maksu- ja Tolliamet

FiDA – *Framework for financial data access*, ELi raamistik finantsandmetele juurdepääsu soodustamiseks

G2C – *Government-to-Citizen*, avaliku sektori asutusele-kodanikule

IKS – isikuandmete kaitse seadus

IKÜM – isikuandmete kaitse üldmäärus

IoT – *Internet of Things*, asjade internet

JDM – Justiits- ja digiministeerium

KYC – *know your customer*, “tunne-oma klienti” printsiip

LKF – Eesti Liikluskindlustuse Fond

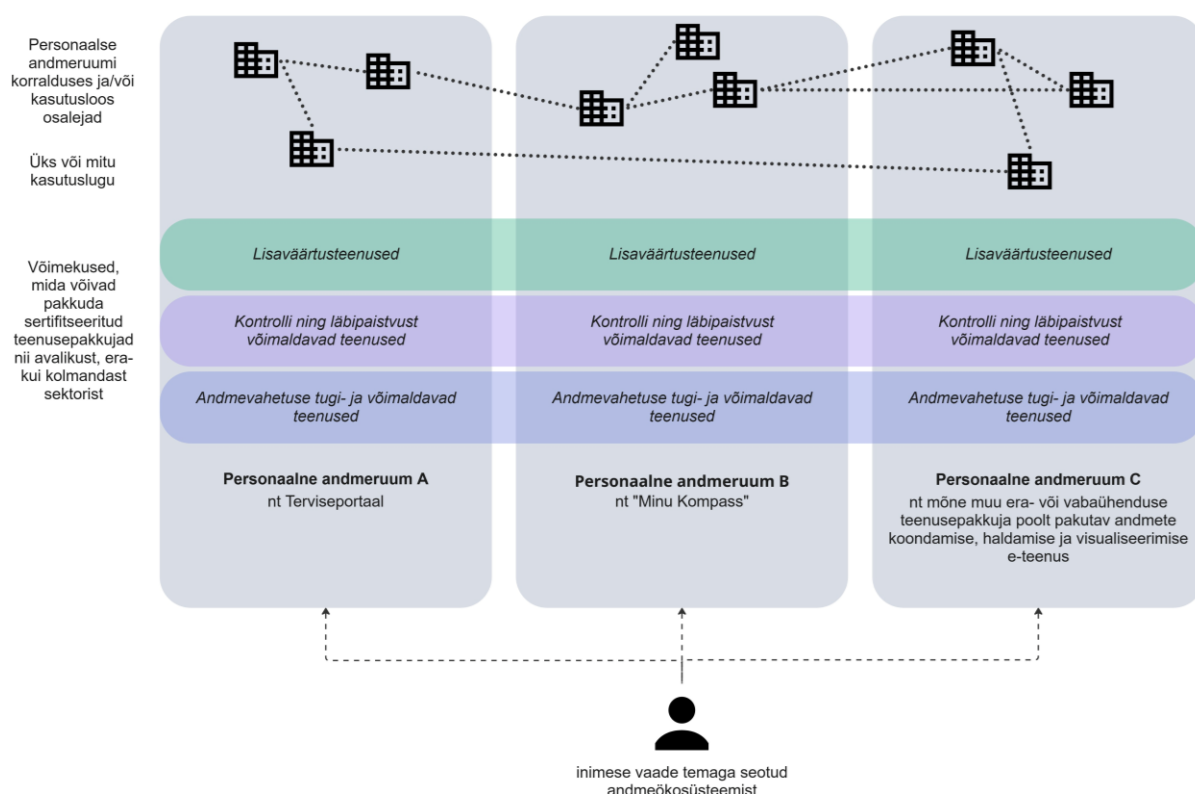
Lühikokkuvõte

Eesti digiühiskonna arengukava 2030 rõhutab inimkeskse lähenemise olulisust digiriigi arengus, sealhulgas andmekorralduses ja digiteenuste arengus nii avalikus kui erasektoris. Üheks lubaduseks ja eesmärgiks on seatud arengukavas järgmine - *“Digiriigis on inimeste põhiõigused kaitstud ning inimesel ja ettevõtjal on kontroll oma andmete üle ja võimalus neid päriselt jagada”*.

Käesoleva teostatavusuuring lähtub sellest lubadusest, eesmärgiga hinnata inimkeskse andmemajanduse edendamise võimalusi Eestis ning uurida, millist rolli võiks selles mängida personaalse andmeruumi kontseptsioon. Sealjuures keskendub uuring küsimusele, kuidas võimaldada **inimestel paremini mõista, hallata ja kasutada oma andmeid**, mis toetaksid samal ajal **uute andmepõhiste teenuste ja ärimudelite arengut**, ning millised on **ettevõtete äri vajadused** inimeste andmete laiemaks kasutamiseks. Sissevaade organisatsioonide äri vajadustesse, võimalikesse kasutuslugudesse ning personaalse andmeruumi potentsiaali andmemajanduse toetamisel on autorite hinnangul olulise väärtusega, et toetada avalikku diskussiooni inimkeskse andmekorralduse ümber ning toetada uudsete lähenemiste katsetamist ka teistes valdkondades.

Uuringu tulemused näitavad, et **Eesti andmeökosüsteem on tehnoloogiliselt arenenud, kuid inimkeskne lähenemine ei ole veel suuresti realiseerunud**. Avaliku sektori digitaristu loob tugeva aluse andmete turvaliseks vahetamiseks, kuid inimeste võimalused oma andmete kasutamist terviklikult hallata on endiselt piiratud. Praktikas tähendab see, et kuigi inimestel on seaduslikud õigused oma andmete üle otsustamiseks, puuduvad sageli lihtsad ja arusaadavad vahendid nende õiguste kasutamiseks.

Personaalse andmeruumi kontseptsioon ja rakendused pakuvad võimaliku lahenduse sellele probleemile. Uuringu põhjal ei ole tegemist ühe konkreetse tehnilise lahendusega, vaid **paindliku lähenemisega, mis võimaldaks inimesel koondada enda kohta käivaid andmeid (kas valdkondlikult või valdkonnaüleselt) ühte vaatesse ning otsustada nende kasutamise üle erinevates rakendustes**, soodustades seeläbi andmepõhiste toodete ja teenuste pakkumist. Personaalse andmeruumi eesmärk on tagada, et inimene ei oleks pelgalt andmete allikas ja subjekt, vaid **aktiivne osaleja nende kasutamises ja väärimises**.



Joonis 1. Hüpoteetiline stsenaarium, kus inimene saab paralleelselt kasutada ühte või mitut personaalse andmeruumi rakendust, mis võimaldab tal hallata, kontrollida ja jagada oma andmeid talle huvipakkuvate kasutuslugude võimaldamiseks. Iga personaalne andmeruum kätkeb endas konkreetseid osalejaid ja nende vahelist andmekoostööd.

Eesti kontekstis on personaalse andmeruumi arendamiseks olemas mitmed olulised eeldused. Riigi digitalistu, sealhulgas elektrooniline identiteet ja andmevahetuslahendused nagu X-tee, andmenõusolekuteenus jms, loovad tugeva vundamendi. Samuti toetab selle arengut Euroopa Liidu õigusraamistik, mis rõhutab inimeste õigusi oma andmete üle. Samas näitab uuring, et tehnoloogilised eeldused üksi ei ole piisavad. Suurimad väljakutsed on seotud **organisatsioonide motivatsiooni, selgete äriliste stiimulite, ärimudelite kujunemise ning erinevate osapoolte vahelise andmealase koostööga**. Ettevõtetel on küll huvi arendada andmepõhiseid teenuseid, kuid **piiratud ligipääs kvaliteetsetele andmetele, nõusolekupõhise andmetöötlemise ebakindlus, regulatiivne ja halduslik selgusetus ning kehtivate ärimudelite inertsus** vähendavad valmisolekut investeerida uutesse lahendustesse. Inimeste kui teenuste lõppkasutajate ja andmesubjektide vaatest on oluline, et andmete jagamine tooks neile selget kasu, näiteks paremate teenuste (sh personaliseeritud ning proaktiivsed teenused), suurema mugavuse, rahalise või ühiskondliku väärtuse kujul, **säilitades sealjuures kontrolli** selle üle, kes ja milleks nende andmeid kasutab.

Uuringu käigus analüüsitud kasutuslood, eelkõige finants- ja haridus ning töövaldkonnas, näitavad, et personaalse andmeruumi lahendused on põhimõtteliselt teostatavad. Tehnilised lahendused on enamasti olemas ning õiguslik raamistik võimaldab nende arendamist, kuid edukas rakendamine eeldab selgeid ärimudeleid ning osapoolte koostööd. Seetõttu ei ole peamised takistused tehnoloogilised, vaid institutsionaalsed ja majanduslikud. Oluliseks

uuringu järelduseks on sealjuures, et **personaalse andmeruumi arendamine ei tähenda uue keskse süsteemi või teenuste komponendi loomist**, vaid olemasolevate lahenduste sidumist viisil, mis annab inimesele suurema kontrolli ja parema ülevaate oma andmete kasutamisest. See eeldab ühtlasi uute rollide ja vastutuste kujunemist andmeökosüsteemis, sealhulgas andmevahendajate ja lisaväärtusteenuste pakkujate seas.

Uuringu põhjal on võimalik järeldada, et personaalse andmeruumi kontseptsioon on Eestis realistlikult rakendatav (ning mõningal juhul seda ka juba tehakse, mõeldes nt Eesti.ee, Terviseportaal, Oskuste Kompass lahendustele) ning sellel on potentsiaal toetada nii majanduslikku innovatsiooni kui ka inimeste suuremat autonoomiat digiteenuste korralduses. Küsimuseks on ettevõtete huvi ning võimekus ehitada uusi teenuseid olemasolevate komponentide peale, nagu andmenõusolekuteenus, arvestades nende majanduslikku positsiooni ning äristrateegiat skaleerida teenuseid ka Eestist väljapoole. Selle potentsiaali realiseerimine eeldab koordineeritud tegevust riigi, erasektori ja teiste sidusrühmade vahel, otsimaks **uusi ärimudeleid, mis lähtuvad organisatsioonide ülesest andmealasest koostööst**. Eesti ettevõtted nagu Cachet, Lyfery ja välismaised andmevahendusteenused nagu Athumi ja iGrant.io koos oma koostööpartneritega on käesoleva uuringu autorite hinnangul siinkohal suunanäitajaks.

Käesolev uuring esitab seetõttu järgmised **põhilised soovitud**:

- Tõsta nii Eesti elanike teadlikkust digiriigi ning andmemajanduse toimimisest kui ka soosida digipädevuste arendamist;
- Tagada toimiv ja prognoositav õigus- ning haldusraamistik;
- Suurendada andmete kättesaadavust ning vahetust tuginedes toimivale digitalistule ning usaldusväärsetele andmevahendusteenustele;
- Toetada andmealast koostööd erasektoris;
- Siduda personaalse andmeruumi raamistik ettevõtte äristrateegiaga ning tagada tugev strateegiline juhtimine.

Lisaks esitavad uuringu autorid ka ettepaneku konkreetseteks tegevusteks, mida järgmistel aastatel ellu viia.

Kokkuvõttes näitab uuring, et küsimus ei ole niivõrd selles, kas personaalsed andmeruumid on võimalikud, vaid selles, kuidas kujundada nende rakendamine viisil, mis loob väärtust nii inimestele, ettevõtetele kui ka ühiskonnale tervikuna. Personaalse andmeruumi raamistikus toimivaid teenuseid pole võimalik arendada "tavapärase" IT-teenusena, millega katta vaid konkreetse organisatsiooni või kasutaja vajadust ning ootusi. Personaalse andmeruumi arendamine eeldab **sektoriülest innovatsiooni**, millega toetada inimeste andmete taaskasutamist erinevate osapoolte ning teenuste poolt, pakkudes samal ajal inimestele terviklikku ülevaadet ning mugavat hallatavust. Samuti sõltuvad kaasuspõhised arengud laiemast **ökosüsteemi andmeküpsusest**, mille arengu toetamiseks on vaja mitmetasandilist poliitikakujundust, andmepõhise ning inimkeskse ettevõtluse toetamist ning koostöötava andmehalduspraktikate juurutamist.

1. Sissejuhatus

Digitaliseerumise ning uute tehnoloogiate nagu Asjade Interneti (*Internet of Things, IoT*), pilveteenuste ja privaatsuskaitsetehnoloogiate laialdane levik on muutnud andmed üheks olulisemaks majanduslikuks ja ühiskondlikuks ressursiks. Andmete maht kasvab kiiresti ning üha rohkem ühiskondlikke nähtusi on võimalik analüüsida ja juhtida andmepõhiselt. Sellest tulenevalt nähakse andmemajanduses olulist potentsiaali nii majanduskasvu kui ka avalike teenuste kvaliteedi parandamiseks^{1,2}.

Samas on andmemajanduse areng toonud esile uusi väljakutseid. Märkimisväärne osa digitaalsest väärtusloome protsessist põhineb inimeste kohta kogutud andmetel, mida kasutatakse teenuste arendamiseks, turunduseks ja otsuste tegemiseks. Praktikas on aga üksikisikute võimalused nende andmete kasutamist mõista, suunata või kontrollida sageli piiratud. See on tekitanud olukorra, kus andmemajanduse majanduslik väärtus koondub peamiselt organisatsioonide kätte, samal ajal kui inimeste roll andmepõhistes väärtusvoogudes on olla pigem passiivsed teenuste lõppkasutajad. Samal ajal on nii teadlased, huvikaitseorganisatsioonid kui ka poliitikakujundajad Eestis ja mujal seisnud inimkesksete põhimõtete eest digisfääri kujundamisel, et tagada nii inimeste põhiõiguste (nagu õigus eraelu puutumatusele, õigus vabale eneseteostusele, sh informatsioonilisele enesemääramisele) kaitsmine kui ka võimestada inimesi enda kohta käivaid andmeid soovi kohaselt vääridama.

Euroopa Liidus on isikuandmete kaitse üldmäärus (IKÜM) loonud olulise õigusliku raamistiku, mis tagab üksikisikutele mitmeid õigusi oma andmete kaitseks ja kontrollimiseks. Praktikas on aga ilmnenud, et pelgalt regulatsioonidest ei piisa, et tagada inimestele sisuline kontroll nende andmete üle või muuta andmete kasutamine läbipaistvamaks. Seetõttu on hakatud üha enam otsima lahendusi, mis ühendaksid õiguslikud põhimõtted tehnoloogiliste ja institutsionaalsete mehhanismidega.

Üheks võimalikuks lahenduseks on personaalse andmeruumi³ kontseptsioon, mille eesmärk on võimaldada üksikisikutel hallata ja jagada oma andmeid turvaliselt ning läbipaistvalt, võimaldades samal ajal organisatsioonidel kasutada andmeid kokkulepitud tingimustel uute teenuste, toodete ja innovatsiooni arendamiseks. Selline lähenemine püüab ühendada kaks seni sageli vastandatud eesmärki: isikuandmete⁴ kaitse ning nende majanduslik ja ühiskondlik väärtustamine. Käesolev uuring panustab laiemasse eesmärki edendada inimkesket

¹ Andmete ja tehisintellekti valge raamat 2024–2030, Justiits- ja Digiministeerium, 2024.

² Andmeühiskonna tulevik. Stsenaariumid aastani 2035. Arenguseire Keskus, 2022

³ Andmeruume on defineeritud kui juhtimis-, toimimis- ja korraldusmudeliga määratletud hajutatud süsteemid, mis võimaldavad andmetehinguid erinevate osapoolte vahel. See tähendab, et andmeruumid on olemuselt laiapõhjalist andmemajanduse ökosüsteemi toetavad kontseptuaalsed ja tehnilised raamistikud, mille toimimiseks on kriitiline nende rajamine äri vajadustest lähtuvalt. ([JDM 2025](#)) Antud uuringu huviorbiidis on paremini mõista, mida tähendab see inimese jaoks ning kuidas sobitub antud definitsiooniga kokku personaalse andmeruumi kontseptsioon.

⁴ Isikuandmed (inimeste andmed) on igasugune teave tuvastatud või tuvastatava füüsilise isiku („andmesubjekti“) kohta; tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada, eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal (IKÜM art 4 p 1 definitsioon).

andmekorraldust ühiskonnas ning toetada andmemajanduse arengut Eestis. Sealjuures on antud projekti raames eesmärgiks selgitada, mida tähendab personaalne andmeruum nii teoorias kui praktikas, kirjeldada organisatsioonide ärivajadusi inimeste andmete kasutamisel ning uurida võimalikke kasutuslugusid, et hinnata personaalse andmeruumi potentsiaalset rolli inimkeskse andmemajanduse arendamisel Eestis.

Käesolev dokument koosneb järgnevatest osadest:

1. esimeses peatükis antakse ülevaade inimkeskse andmemajanduse põhimõtetest, poliitilisest ja majanduslikust kontekstist ning õiguslikust raamistikust, mis mõjutab inimeste andmete kasutamist ja jagamist;
2. seejärel avaneb teises peatükis uuringu teostamise kontekst – selle eesmärk, uurimisküsimused, metodoloogia ning kaasatud sidusrühmad;
3. kolmas peatükk avab personaalse andmeruumi kontseptsiooni, põhimõtted ning selle väärtuspakkumise inimestele ja organisatsioonidele;
4. neljas peatükk annab ülevaate uuringu käigus kaasatud organisatsioonide ärivajadustest andmepõhiste toodete ja teenuste arendamiseks;
5. viies peatükk esitab ärilised, õiguslikud, funktsionaalsed ja tehnoloogilised võimekused, eeldused ja väljakutsed inimkeskse andmemajanduse arendamiseks ning personaalse andmeruumi kontseptsiooni rakendamiseks.
6. kuues peatükk annab ülevaate personaalse andmeruumi kontseptuaalsest rollimudelitest, mis määratleb osapoolte vastutused ja suhted inimeste andmete vahetuse ja väärimdamise kontekstis.
7. seitsmes peatükk kirjeldab uuringu jooksul tuvastatud esialgseid kasutusjuhud; ning seejärel esitatakse
8. kaheksandas peatükis kahe süvitsi uuritud kasutusloos – elukindlustuse ja tööleasumist soodustava oskuste ja haridusandmete põhise teenuse – teostatavuse analüüs.
9. Üheksas peatükk avab laiemalt personaalse andmeruumi arendamise võimalusi ning olulisemaid väljakutseid; ning
10. kümnes peatükk esitab uuringumeeskonna peamised soovitusel ja teekaardi personaalse andmeruumi arendamiseks Eestis.

Uuringu lõpus on esitatud ka kasutatud kirjandus ning lisad.

1.1 Inimkeskne vaade andmemajandusele

Andmepõhised äriprotsessid lähtuvad enamasti organisatsioonide strateegilistest eesmärkidest ning kontekstist, mis viitab organisatsioonide suuremale jõupositsioonile andmekorralduses. Euroopa õigusruumis kohaldunud normid ja reeglid tõstavad küll esile üksikisiku õigusi ja vabadusi oma andmete ning privaatsuse kaitsmiseks, kuid vähe on pööratud tähelepanu inimese aktiivsele majanduslikule rollile⁵ andmete kasutamise ning organisatsioonide vaheliste andmekoostööde arendamise toetamisel. Inimkeskne lähenemine andmemajandusele püüab seda perspektiivi muuta. Selle lähenemise keskmeks on arusaam, et andmetega seotud protsesside kujundamisel tuleb arvestada üksikisikute vajaduste, eelistuste, õiguste ja eesmärkidega⁶. Inimkeskne andmekorraldus tähendab seega mitte ainult andmete kaitset, vaid ka võimalust kasutada andmeid viisil, mis toetab inimeste heaolu ja enesemääramist, vastates samal ajal ka organisatsioonide ärihuvidele.

Inimkeskse lähenemise põhimõtteid on kirjeldatud nii teaduslikus ja poliitikakujunduslikus raamistikus⁷. Üldjoontes võib need Lähteenoja jt (2021) järgi koondada järgmiselt⁸:

1. **Inimene kui keskne ühenduspunkt** lähtub organisatsioonide (ja nende üleses) andmekorralduses inimesest kui tervikust, võimaldades läbi vastutustundliku integreerimise tõsta andmete kvaliteeti ning väärtust;
2. **Inimese võimestamine andmetega** viitab inimeste loomupärasele agentsusele⁹ ning kontrollile oma andmete üle, võimaldades kasutada andmeid teadlikult oma elu parandamiseks, selmet olla pelgalt passiivsed kaitsmist vajavad osalejad digiühiskonnas;
3. **Ökosüsteemne lähenemine** viitab eesmärgile tagada koostalitlusvõime¹⁰ tehnoloogiate, poliitikate ja ärimudelite vahel, võimaldades erinevate osapoolte koostööd ja juurdepääsu andmetele;
4. **Pluralism** viitab erinevate kultuuride ja poliitikate kooseksisteerimise võimaldamist ühises, koostööd võimaldavas raamistikus;
5. **Proportsionaalsus ja õiglus** viitab vastutuste, vabaduste, riskide ning võimaluste õiglasele ja tasakaalustatud jaotamisele andmeökosüsteemides.

Selline lähenemine eeldab süsteemseid muutusi nii tehnoloogias, institutsioonides kui ka ühiskondlikes normides. Inimkeskse andmemajanduse toimimine sõltub muu hulgas inimeste andmekirjaoskusest, õigusruumi järjepidevast arengust, kestlike ärimudelite soosimisest,

⁵ Laufi jt sõnul võib ka IKÜM eirata Euroopa kodanike majanduslikke huve ning võib piirata seetõttu isikuandmete kasutamisest tulenevat majanduslikku potentsiaali, vt Lauf et al., 2022 Linking Data Sovereignty and Data Economy: Arising Areas of Tension

⁶ vt nt Digiühiskonna arengukava 2030 ja Andmete ning Tehisintellekti valge raamat

⁷ Vt nt Aguerre ja Hasselbalch 2025; Norman 2019; MyData Global 2017

⁸ On the importance of human centrality. Lähteenoja, V., Flanagan, A. J., & Warren, S. (2021)

⁹ Agentsus on inimese kui sotsiaalse toimija võime teha iseseisvaid otsuseid ja nende kaudu mõjutada oma elukeskkonda (Sõnaveeb 2025; Raud 2013)

¹⁰ Koostoime / koostalitlusvõime (*interoperability*) on süsteemide või komponentide võime läbipaistvalt vahetada teavet ja seda teavet kasutada. ([Cybernetica 2025](#))

tehnoloogilisest taristust, koostalitlusvõimest ning läbipaistvatest otsustusprotsessidest. Praktikas näib, et *inimkesksus* pole (ega saa olla) binaarne väärtus, vaid see asub hägusel kontiinumil, kus soovitud eesmärkideni jõudmiseks ühiskonna ning selle osaliste jaoks tuleb teha otsuseid, mil määral ja moel inimkeskse lähenemise põhimõtteid rakendada. Seejuures on individuaalsed tegevused ning osalejate vastutus nii *mikro* (nt konkreetsete teenuste disain, organisatsiooni äristrateegia), (ühiskondlikud normid, institutsionaalne järelevalve jms) kui ka *makro* (rahvusvahelised standardid, geopoliitilised mõjutused) tasandil erinevalt jaotunud¹¹.

Siinkohal on paslik meenutada, et andmestunud ühiskonna toimimine, sealhulgas seda võimaldav taristu, tehnoloogiad ja standardid ning mittetehnilised mehhanismid, nagu seadusandlus, äri- ning haldusmudelid, on tihedalt läbipõimunud ühiskonnas kehtivate võimuhete, ideoloogiate ning väärtustega¹². Võimuhete problemaatika ei seisne ainult küsimuses, kes kontrollib andmeid, vaid peamiselt selles, kes neist kasu saab, kelle õigusi ja huve eelistatakse ning kelle perspektiiv jääb kaasamata¹³. Lisaks on oluline silmas pidada andmete ning nende kasutamise piiratust. Kuigi andmepõhisuses nähakse tihti petlikku lubadust objektiivsusele, siis pole tehnoloogia ega andmete kasutamine kunagi neutraalne. Alates andmete kogumisest nende kasutamise ning jagamiseni ning isegi kustutamiseni, hõlmates kogu elukaart, on keeruline vältida kallutatust¹⁴. Seetõttu on oluline tagada andmepõhiste protsesside ja tehnoloogiliste lahenduste arendamisel läbipaistvus ning võimalusel kaasata erinevaid huvigruppe selle kujundusprotsessi.

Ühiskonna toimimise laiem kontekst annab viiteid andmekorralduse nn sotsiaalsest kokkuleppest, mis demokraatlikes ühiskondades viitab olulisele kolmikule – kuidas suudetakse andmetega luua majanduslikku ning sotsiaalset väärtust, kuidas tagatakse erinevate ühiskonnagruppide kaasatus andmepõhiste hüvede loomisel ning nende jagamisel, ning kolmandaks, kuidas tekitatakse ning hoitakse usaldust andmete kasutamise osas¹⁵. Tasakaalu leidmine nende elementide vahel on delikaatne ning keerukas ülesanne.

Peamine järeldus

Praegune andmemajandus on valdavalt organisatsioonikeskne, kus inimesed on pigem passiivsed andmeallikad kui aktiivsed osalejad. Inimkeskne lähenemine rõhutab inimese olulist rolli andmete korraldamisel ja väärimdamisel ning vajadust pakkuda inimesele vahendeid, millega kontrollida oma andmete kasutust. See eeldab omakorda muutusi tehnoloogias, ärimudelites ja institutsioonides.

¹¹ The EU human-centric approach to AI: Foundational elements for a global framework. DataEthics.eu. Aguerre, C., Hasselbalch, G., 2025

¹² Euroopa ning Eesti komberuum lähtub nii demokraatlikest väärtustest (nt põhiõiguste kaitse) kui ka individualistlikust ideoloogiast, mis tõstab esile üksikisiku olulisust koos talle kuuluvate vabaduste ning õigustega. Need väärtused satuvad aga sageli konflikti enamlevinud andmepraktikatega, mille eesmärgiks on suurendada tõhusust, optimeerida turgu majanduskasvu soosimiseks ning vältida kuritegevust (nt andmepõhise järelevalve kaudu).

¹³ vt nt Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power.

¹⁴ vt nt D'Ignazio, C., & Klein, L. F. (2023). Data feminism.

¹⁵ vt Maailmapank. (2021). The social contract for data.

1.2 Poliitiline tahe ja andmemajanduslik potentsiaal

Euroopa Liidus kehtib põhimõte, et andmed kuuluvad inimesele, kelle kohta need käivad. Kuigi “kuuluvuse” tõlgendamisel on mitmeid küsitavusi, siis vähemalt poliitilisel ning seadusandlikul tasandil on selge, et andmestunud ühiskonnas on inimesel õigus oma andmetele, sh nende kaitsmisele ja suveräänselt kontrollitud väärimisele. Seetõttu on inimkeskse andmemajanduse eest seismine osa ka laiemast Euroopa andmestrateegiast. Eesti on selles protsessis üks Euroopa pioneere. Strateegiad „Eesti digiühiskond 2030”¹⁶ ja „Eesti 2035”¹⁷ rõhutavad vajadust arendada digiriiki, kus e-teenused on kergesti kättesaadavad ning inimeste õigused andmete kasutamisel on kaitstud. Inimväärikuse, privaatsuse ja võrdse kohtlemise edendamine andmetöötajates on seatud sealjuures keskele kohale. Selle saavutamiseks plaanitakse tegevusi andmekaitse, küberturvalisuse ja andmekirjaoskuse arendamiseks, et tagada digilahenduste jätkuv usaldusväärsus ja vastutustundlik innovatsioon. Sealjuures on soov liikuda edasi ka tehnoloogiliste lahendustega, nagu andmeälgi¹⁸ ja andmenõusolekuteenus¹⁹ laiem juurutamine, mis toetaksid andmete jälgitavust ja haldamist inimese enda poolt.

Samas on uuringud²⁰ osutanud, et inimestel puudub endiselt terviklik ülevaade nende kohta kogutud andmetest ning lihtsad mehhanismid nende andmete jagamiseks või kasutamise kontrollimiseks. See piirab nii uute andmepõhiste teenuste arengut kui ka andmete taaskasutamise võimalusi. Siiski on Eesti unikaalne selles, et näiteks terviseandmete puhul saab inimene juba praegu jälgida, kes ja millal tema andmeid on kasutanud. Samuti on andmeälgi¹⁸ tänaseks liidestunud 16 andmekogu avaliku sektori infosüsteemidest, mida on plaanis täiendada enamate andmekogudega. Andmenõusolekuteenus on hetkel liidestatud vaid üksikute andmekogudega, mis piirab erasektori võimalust ning motivatsiooni luua uusi nõusolekupõhiseid teenuseid, samuti pärsib andmete dubleerimise vähendamise eesmärki. Ka andmenõusolekuteenus kasutamine plaanitakse teha kohustuslikuks enamikele riigiasutustele ja omavalitsustele²¹.

Andmemajanduse potentsiaali hindamiseks puuduvad täna veel selgelt välja kujunenud meetodid, kuid erinevate hinnangute kohaselt on selle majanduslik potentsiaal

¹⁶ Eesti digiühiskonna arengukava aastaks 2030, kättesaadav aadressil <https://valitsus.ee/sites/default/files/documents/2021-12/Eesti%20digi%C3%BChiskond%202030.pdf>, külastatud 23.03.2026

¹⁷ Eesti pikaajaline strateegia “Eesti 2035”, kättesaadav aadressil <https://valitsus.ee/strateegia-eesti-2035-arengukavad-ja-planeering/strateegia>, külastatud 23.03.2026

¹⁸ Vt lähemalt aadressilt <https://www.ria.ee/riigi-infosusteem/inimkeskne-andmehaldus/andmealgija>, külastatud 23.03.2026

¹⁹ Vt lähemalt aadressilt <https://www.ria.ee/riigi-infosusteem/inimkeskne-andmehaldus/andmenousolekuteenus>, külastatud 24.03.2026

²⁰ nt Andmeühiskonna tulevik. Stsenaariumid aastani 2035. Arenguseire Keskus, 2022

²¹ Uus seaduseelnõu: inimestel tekib selgem võimalus oma andmete jagamiseks või selle keelamiseks, vt lähemalt <https://www.justdigi.ee/uudised/uus-seaduseelnou-inimestel-tekib-selgem-voimalus-oma-andmete-jagamiseks-voi-selle>, külastatud 23.03.2026

märkimisväärne. Erinevate uuringute kohaselt moodustab andmemajandus Eestis hinnanguliselt mitu protsenti sisemajanduse koguproduktist (SKP). Näiteks:

- Tartu Ülikooli ja STACCI eksperdid²² hindasid Eesti andmemajanduse mahuks **3-3.5% SKPst** ehk suurusjärgus 1.2-1.4 miljardit eurot (Eesti SKP oli 2024. aastal 39.5 miljardit). Antud uuringus kasutati kulupõhist mudelit (tööjõukulud ja muud kulud).
- 2024. aasta Euroopa andmeturu uuringute²³ järgi hinnati Eesti andmemajanduse mahuks 533 miljonit eurot ehk umbes **1.3% SKPst**, võttes muuhulgas aluseks ka andmemahte, andmeeksperte kui ka ettevõtetest andmepakkujaid ja -kasutajaid.
- Lisaks on andmepõhisel korraldusel potentsiaal ka kokkuhoiuks. Nt aitaks reaalamajandusele üleminek (e-arved, e-kviitungid, aruandluse automatiseerimine, majandusproгноosid, põllumajandus-andmed ja e-logistika) kulusid kokku hoida umbes 210 miljonit eurot, mis teeb töötundides hinnanguliselt kokku 14.1 miljonit tundi²⁴.

Samas sõltub selle potentsiaali realiseerimine suuresti andmeökosüsteemi küpsusest, sealhulgas andmete kvaliteedist, standardiseerimisest ja osapoolte koostööst. Inimkeskse andmekorralduse majanduslikke mõjusid võib sealjuures üldiselt hinnata kolme peamise kategooria kaudu, milleks on **tõhususe kasv** (halduskulude ja aja kokkuhoid), **innovatsioon ja lisandväärtust loovad teenused**, ning kolmandaks **andmete (või andmetoodete) otsesest kauplemisest saadud tulu**. Inimeste suurem kontroll oma andmete üle võib eelduslikult suurendada usaldust teenusepakkujate suhtes ning soodustada andmepõhiste toodete ja teenuste kasutuselevõttu.

Peamine järeldus

Eestis ja Euroopa Liidus on olemas tugev poliitiline ja strateegiline raamistik inimkeskse andmemajanduse arendamiseks, kuid selle praktiline realiseerimine on ebaühtlane. Andmemajandusel on märkimisväärne majanduslik potentsiaal, kuid selle kasutamine sõltub eelkõige andmete kättesaadavusest, kvaliteedist ja usaldusest ökosüsteemis osalejate vahel.

²² Eesti andmemajanduse turuväärtuse hindamise metoodika koostamine, kättesaadav aadressil

https://e964029b-7c32-42a7-817c-37c391a3b976.filesusr.com/ugd/2d9e67_831b07fcab9c41c78748f6444d22cfa4.pdf, külastatud 23.03.2026

²³ European Data Market Study 2024–2026, kättesaadav aadressil

https://ec.europa.eu/newsroom/repository/document/2025-13/EDM_2024_2026_First_Report_on_Facts_and_Figures_9cU0iljcuSZhjmwl9TchwqenidQ_114043.pdf,

külastatud 23.03.2026

²⁴ Reaalamajanduse majandusliku mõju uuringu lõpparuanne, kättesaadav aadressil

https://realtimeeconomy.ee/sites/default/files/2021-12/reaalamajanduse_majandusliku_maju_uuringu_lopparuanne.pdf,

külastatud 23.03.2026

1.3 Õiguslik vaade inimeste andmete korraldusele

Õiguslikust vaatest on inimeste andmetega seotud kõige otsesemalt isikuandmete kaitse üldmäärus (IKÜM)²⁵, mis sätestab EL-i üleselt isikuandmete töötlemisele²⁶ nõudeid nii avalikus kui ka erasektoris. Kuigi IKÜM jätab EL liikmesriikidele võimaluse reguleerida teatavaid isikuandmete töötlemise ja kaitsega seonduvaid aspekte ka siseriikliku õiguse tasandil²⁷ (Eestis on selleks õigusaktiks üldisemal tasandil isikuandmete kaitse seadus (IKS)), näeb otsekohalduv IKÜM ette selge ühtse lähenemise EL-üleselt isikuandmete töötlemise põhimõtete ja õiguslike aluste osas. Määrus sätestab andmesubjektidele mitmed õigused, sealhulgas õiguse tutvuda oma andmetega, nõuda nende parandamist või kustutamist ning piirata andmete töötlemist²⁸.

Oluline õiguslik instrument on ka andmete ülekandmise õigus (IKÜM art 20), mis võimaldab inimesel saada vastutavalt andmetöötlejalt koopia oma andmetest ning edastada need teisele teenusepakkujale (kas ise või nõuda otse ülekandmist kui see on tehniliselt teostatav)²⁹. Selle õiguse eesmärk on suurendada konkurentsi digiturul ning anda inimestele suurem kontroll oma andmete üle. Praktikast on selle õiguse rakendamine siiski piiratud ulatusega, muu hulgas kasutajate madala teadlikkuse, tehniliste ja institutsionaalsete takistuste tõttu^{30,31}.

Lisaks IKÜM-ile mõjutavad andmete kasutamist mitmed teised Euroopa Liidu õigusaktid, sealhulgas andmehaldusmäärus (DGA)³², andmemäärus (DA)³³ ning digiturgude määrus³⁴ (DMA). Need õigusaktid loovad täiendava raamistiku andmete jagamiseks, konkurentsi tagamiseks digiplatvormidel ning innovatsiooni soodustamiseks. Personaalse andmeruumi

²⁵ EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus).

²⁶ IKÜM art 4 p 1 kohaselt on isikuandmete töötlemine isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korraldamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamine, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.

²⁷ Ülevaade, kuidas erinevad EL riigid on IKÜM sätteid siseriiklikus õiguses täiendavalt reguleerinud, on leitav siit: https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection/eu-member-states-notifications-european-commission-under-gdpr_en, külastatud 23.03.2026

²⁸ Vt lähemalt IKÜM III peatükis "Andmesubjekti õigused".

²⁹ Artikli 29 töörühma 5. aprilli 2017. aasta suunised andmete ülekandmise õiguse kohta (WP242 rev.01), mille on heaks kiitnud Euroopa Andmekaitsekoogu (edaspidi „artikli 29 töörühma andmete ülekandmise õiguse kohta, mille on heaks kiitnud Euroopa Andmekaitsekoogu“), lk 3. Kättesaadav: <https://ec.europa.eu/newsroom/article29/items/611233>, külastatud 23.03.2026

³⁰ Reimsbach-Kounatze, C., Molnar, A. (2024). The impact of data portability on user empowerment, innovation, and competition. Going Digital Toolkit Note, No. 25. OECD

³¹ COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0264&from=EN#footnote44>, külastatud 23.03.2026

³² Andmehaldusmäärus, kättesaadav aadressil <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32022R0868>, külastatud 23.03.2026

³³ Andmemäärus, kättesaadav aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=OJ:L_202302854&qid=1774255600006, külastatud 23.03.2026

³⁴ Digiturgude määrus, kättesaadav aadressil <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32022R1925>, külastatud 23.03.2026

arendamisel tuleb arvestada ka digiidentiteedi ja usaldusteenuste regulatsiooniga (eIDAS)³⁵ ning tehisintellekti regulatsiooniga (AI Act)³⁶, mis mõjutavad andmepõhiste teenuste arendamist ja kasutamist. Koos moodustavad need õigusaktid mitmetasandilise regulatiivse keskkonna, milles personaalse andmeruumi lahendused peavad toimima.

Oluline on ka välja tuua, et EL tasandil ollakse käesoleva analüüsi kirjutamise ajal läbi rääkimas uuendusi asjassepuutuvate õigusaktide osas. Euroopa Komisjoni Digital Omnibus³⁷ eesmärk on lihtsustada andmepõhiseid EL-i õigusakte, koondades regulatsiooni peamiselt kaheks tervikuks (IKÜM ja DA) ning muutes vastavuse ettevõtetele konkurentsieeliseks, mitte halduskoormaks. AI Omnibus eesmärk on omakorda lahendada tehisintellekti määruse rakendamisel ilmnenud praktilisi probleeme ja kitsaskohti, et tagada sujuvam ja tõhusam kohaldamine.³⁸

Peamine järeldus

Euroopa Liidu õigusraamistik (IKÜM, DGA, DA jt) annab inimestele formaalsed õigused, kuid ei taga automaatselt nende praktilist rakendamist. Regulatsioonide koosmõju on keerukas ning pigem piirab kui soodustab innovatsiooni, kui puuduvad tehnilised ja institutsionaalsed mehhanismid nende tõhusaks rakendamiseks.

³⁵ Digiidentiteedi ja usaldusteenuste regulatsiooniga (eIDAS), kättesaadav aadressil <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018> , külastatud 23.03.2026

³⁶ Tehisintellekti käsitlev määrus, kättesaadav aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=OJ:L_202401689 , külastatud 23.03.2026

³⁷ Digivaldkonna koondpakett, kättesaadav aadressil <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837> , külastatud 23.03.2026

³⁸ Vt lähemalt: <https://www.aki.ee/rahvusvaheline/euroopa-andmestrateegia/digital-omnibus-ja-ai-omnibus> , külastatud 23.03.2026

2. Teostatavusuuringu läbiviimine

2.1 Uurimiseesmärk ja -küsimused

Uuringu laiem eesmärk on edendada ja soodustada inimeste andmete kasutamist (sh privaatsuse tagamist andmete töötlemisel), inimkeskse andmehalduse juurutamist ning andmete kättesaadavuse ja leitavuse parandamist ning seeläbi laiemalt andmemajanduse edendamist. Sealjuures on **uuringu konkreetseks fookuseks**:

- määratlada personaalse andmeruumi kontseptsioon ning selle peamised funktsionaalsused,
- kirjeldada erinevate osapoolte ärivajadused,
- kirjeldada võimalikud kasutusjuhud ning
- vastata küsimusele, kas ning mil moel saaks personaalse andmeruumi kontseptsioon olla teostatav Eesti kontekstis.

Uuringu eesmärgist lähtuvalt oleme sõnastanud järgnevad **uuringuküsimused**:

1. Milline on inimestega seotud andmete ökosüsteemi hetkeseis Eestis (sh kõige prioriteetsemad sektorid/valdkonnad) ning mil määral realiseeritakse inimkeskse andmehalduse põhimõtteid?
2. Mida tähendab personaalne andmeruum ning kuidas toetavad Eesti tänane õigusruum, digitaalne taristu ja koostöömudelid personaalse andmeruumi(de) arendamist, sh:
 - a. Millised lahendused on täna nii Eestis kui mujal olemas? Mis on puudu ja/või vajaks täiendamist?
 - b. Millised on personaalseid andmeid väärindavate teenuste ja andmevahendust pakkuvate teenuste põhilised ärimudelid?
 - c. Millised on võimalikud (turu)tõrked?
 - d. Kuidas mõjutab Eesti ja Euroopa seadusandlus isikuandmete esmast ning teisest väärindamist?
3. Milline on personaalse andmeruumi osapoolte huvi ja võimekus:
 - a. inimestega seonduvaid andmeid jagada, müüa, osta ja väärindada?
 - b. luua inimestega seotud andmete põhiseid tooteid ja teenuseid?
 - c. arendada ja/või hallata andmevahendust toetavat taristut ja haldusraamistikku?
4. Millised on "personaalse andmeruumi" esmased kasutuslood ja/või teenusmudelid, mille kaudu personaalse andmeruumi(de) rakendamist Eestis katsetada? Mil määral on need teostatavad, arvestades nii ärilisi, tehnilisi kui õiguslikke aspekte?
5. Millised on soovitusel ja praktiline teekaart "personaalse(te) andmeruumi(de)" rakendamiseks Eestis, arvestades nii tehnilisi, õiguslikke kui ka ärilisi/majanduslikke aspekte kui ootusi erinevatele sidusrühmadele?

2.2 Uuringuprojekti ulatus ning piirangud

Kuigi andmestunud ühiskonna ning selle võimaluste ja kitsaskohtade kontekstis on nii inimkeskse andmehalduse kui ka konkreetsemalt personaalse andmeruumiga seonduvaid aspekte uuritud, pole personaalse andmeruumi määratluses veel konsensust leitud (vt lähemalt ptk 3). Seetõttu on käesoleval uuringuprojektil pragmaatiline eesmärk - mõista, mida võiks personaalne andmeruum Eesti kontekstis tähendada ning millisel moel võiks see Eestis rakenduda.

Uuringu ning personaalse andmeruumi ulatuse selgitamiseks on esiteks oluline määratleda, millised andmed on üldse personaalse andmeruumi jaoks relevantssed. Inimeste kohta käivad andmed on kõige spetsiifilisemalt defineeritud isikuandmete mõistega, mis viitab igasugusele teabele, millega saab tuvastada konkreetset isikut, nt nimi, internetiprotokolli (IP) aadress, foto, asukoha andmed, sõrmejäljed vms (EDPB 2025). Samas on isikustatud ning isikustamata andmete vaheline piir muutunud aina hägusemaks, arvestades nt Asjade Interneti (*Internet of Things*, IoT) levikuga tulenevast võimalusest seostada ka inimeste poolt kasutatud seadmete andmeid neid kasutanud isikutega. Lisaks omavad mistahes andmed sotsiaalset ning kultuurilist konteksti (Masso et al 2020), mistõttu võivad esmapilgul mitteisikustatud andmed (nt keele-, ruumiandmed ja Covid-19 pandeemia ajal kogutud reovee andmed) mängida suurt rolli inimeste eluolu mõjutamisel. Käesoleva uuringu käigus on käsitletud peamiselt isikustatud andmeid, mille puhul on võimalik konkreetseid isikuid ka nende haldamisse ning jagamisse kaasata.

Inimkeskse andmekorralduse edendamiseks on paralleelselt käimas ka teisi algatusi, nagu hiljutine inimese digitaalse kaksiku teadusarendusprojekt³⁹. Kui viidatud projektis keskendutakse peamiselt avaliku sektori teenustes ja infosüsteemides kasutatavatele isikuandmetele (sh G2C⁴⁰ teenuste ning kesksete komponentide, nagu andmejälgija, andmenõusolekuteenus, bürokratt, Eesti.ee jt koondamine), siis käesolevas personaalse andmeruumi projektis uuritakse andmepõhist koostööd erasektoris, keskendudes peamiselt B2C⁴¹, B2B⁴² ning B2G⁴³ ärimudelitele. Mõistmaks inimkeskse andmekorralduse ning personaalse andmeruumi arendamise võimalusi ning kitsaskohti erasektoris, on uuringu keskseks lähtepunktiks ettevõtjate ning teiste organisatsioonide ärivajaduste kaardistamine ning analüüsimine.

Projekti läbiviimisel on mitmeid väljakutseid ning piiranguid, mida tuleks uuringu tulemuste hindamisel arvesse võtta.

³⁹ Vt lähemalt <https://riigihanked.riik.ee/rhr-web/#/procurement/8849884/documents?group=B>, külastatud 23.03.2026

⁴⁰ G2C viitab *Government-to-Citizen* ehk avaliku sektori asutustelt otse kodanikule suunatud e-teenuseid, aga ka informatsiooni jagamist.

⁴¹ B2C (*Business-to-Consumer*) viitab eraisikule suunatud (andmepõhiste) teenuste ja toodete pakkumisele, sh ka andmetoodetele.

⁴² B2B (*Business-to-business*) viitab ettevõtetevahelisele äritegevusele toodete ja teenuste (sh andmetoodete) müümisel, kusjuures need võivad tihti sisaldada inimestega seotud andmeid.

⁴³ B2G andmete jagamine on koostöö, mille käigus ettevõtte või muu eraõiguslik organisatsioon teeb oma andmed (või ülevaated) avalikule sektorile (kohalik, piirkondlik, riiklik või EL) avaliku huvi eesmärgil kättesaadavaks. Vt lähemalt nt <https://digital-strategy.ec.europa.eu/en/facts/business-government-data-sharing-questions-and-answers>, külastatud 23.03.2026

- **Personaalse andmeruumi kontseptsioon on mitmekihiline** ning hõlmab nii isikuandmeid töötlevatest osapooltest koosneva ökosüsteemi haldamist kui ka konkreetsete kasutusjuhtude raames rakendatavate toodete, teenuste ja nendega seotud osalejate vaadet. See kihistus tähendab, et **personaalse andmeruumi täpne sisu, vorm ning eesmärk on kontekstispetsiifiline ning selgineb alles praktikas**. Seetõttu on ka antud uuringu raames eristatud laiemalt personaalse andmeruumi kontseptsiooni ning komponente (vt lähemalt ptk 3) ning võimalikke rakendusvaldkondi (vt lähemalt ptk 7 ja 8).
- Käesolev uuring kasutab andmekogumiseks peamiselt kvalitatiivseid meetodeid, mis **ei võimalda uuringutulemusi laiemalt üldistada**. Personaalse andmeruumi kontseptsioon on veel selgelt välja kujunemata, mistõttu otsustas uuringumeeskond meetodi kasuks, mis võimaldab uurida teemat avastuslikult, kaasuda sidusrühmadega otse ning koguda valdkondlikelt ekspertidelt spetsiifilisi teadmisi personaalsete andmeruumide rakendatavuse kohta. Sissevaade organisatsioonide äri vajadustesse, võimalikesse kasutuslugudesse ning personaalse andmeruumi potentsiaali andmemajanduse toetamisel on autorite hinnangul olulise väärtusega, et **toetada avalikku diskussiooni inimkeskse andmekorralduse ümber ning toetada uudsete lähenemiste katsetamist ka teistes valdkondades**.
- Paralleelselt on nii Eestis kui välismaal käimas mitmeid algatusi nagu digitaalse identiteedi kukru arendamine ja kasutuselevõtt EL-üleselt, valdkondlike ning valdkonnaüleste andmeruumide arendamine, erinevad standardiseerimise algatused jne. Samuti on kiire tehnoloogiline areng avamas võimalusi uuteks sotsiaalseteks ning ärilisteks innovatsioonideks, mida tuleb ka personaalse andmeruumi arendamisel ning juurutamisel arvestada. Taoline volatiivsus digisfääri korralduses tähendab, et **teadmatust on palju ning käesoleva uuringu tulemused võivad ajas muutuda**. Samuti pole võimalik kõiki algatusi ammendavalt personaalse andmeruumi kontekstis uurida. Sellegipoolest püüab käesolev dokument seostada teadaolevaid olulisemaid algatusi personaalse andmeruumi määratluse, komponentide ning kasutuslugudega.
- Antud teostatavusuuringu ulatuses pole käsitleda:
 - erinevate andmeökosüsteemide ning täpsemalt andmeruumide võimaldavate raamistike ega erinevate digitalistute, sh X-tee detailset analüüsi, v.a juhul kui see muutub personaalse andmeruumi teenuste teostatavuse määratlemisel oluliseks;
 - ammendavalt hinnata erinevate regulatsioonide ning neis seatud tingimuste koosmõju inimeste andmete kasutamisel. Uuringus on fookuses peamised EL andmete kasutust reguleerivad õigusaktid, tuues võrdlusmomente siseriikliku õigusega;
 - personaalse andmeruumi potentsiaalset laiemat majanduslikku mõju. Selle asemel keskendume personaalse andmeruumi kasutusjuhtude võimalike ärimudelite hindamisele;
 - inimeste kui lõppkasutajate laiemat kaasamist uuringu läbiviimisesse. Kuna personaalse andmeruumi kontseptsioon on alles kujunemisel ning inimeste üldine andmekirjaoskus on pigem madal, siis toetub analüüs peamiselt varem

läbiviidud uuringutulemusele ning antud uuringus kaasatakse peamiselt personaalse andmeruumi võimalikke osapooli organisatsioonide vaatest.

2.3 Metodoloogia ning sidusrühmade kaasamine

Käesoleva uuringu fookuses on nii lahendused personaalse(te) andmeruumi(de) võimaldamiseks kui ka konkreetsed kasutuslood, mis kirjeldaksid personaalse andmeruumi väärtuspakkumist nii inimestele kui organisatsioonidele. Kuna personaalsed andmeruumid on alles väljakujunemise faasis, siis on oluline hoiduda liiga kitsast definitsioonist. Seetõttu kasutame antud uuringus metoodikat, mis aitaks kirjeldada personaalsete andmeruumide võimalikke lahendusi, keskendudes peamiselt nende ühiskondliku ning ärilise kandepinna uurimisele Eestis. Uuringu esimeses faasis viisime läbi **taustmaterjalide analüüsi**, mille käigus uurisime inimeste andmete kaitset ning väärindamist käsitlevaid teadusartikleid, poliitikakujunduslikke dokumente, raporteid, juriidilisi dokumente jne. Selle baasil kujundasime esmaseid hüpoteese personaalsete andmeruumide ulatusest, nende rakendatavusest Eestis ning täpsustasime edasiste uurimisetappide fookust.

Personaalse andmeruumi kontseptsiooni täpsustamiseks ning rakendavuse uurimiseks kaasasime seejärel eksperte nii Eestist kui välismaalt, et uurida, kuidas nähakse inimeste kaasamise potentsiaali oma andmete haldamisel ning jagamisel, et soodustada ettevõtlust, uudsete personaliseeritud teenuste arendamist ning inimkeskema andmekorralduse juurutamist erasektoris. Selleks viisime läbi **18 poolstruktureeritud intervjuud 31 eksperdiga** nii ettevõtetest, riigiasutustest, vabaühendustest kui ka haridusasutustest (ülevaade organisatsioonidest Lisa 1). Kõik potentsiaalsed intervjuueeritavad ei soovinud või ei saanud intervjuud anda (kokku saatsime intervjuupalve 23 organisatsioonile). Intervjuudes keskendusime peamiselt inimkeskse andmekorralduse rakendatavusele erasektoris ning personaalse andmeruumi arenguid toetavatele ja takistatavatele teguritele. Intervjuude kokkuleppimiseks võtsime ühendust mitmete valdkonnaülest ekspertiisi omavate ekspertidega, kuid ka konkreetsemalt kahe uuringu käigus prioritseeritud valdkonna (haridus/tööturg ning pangandus/finants) ettevõtete ning tugiorganisatsioonide esindajatega. Samuti kasutasime lumepallimeetodit, saades soovitusi intervjuueeritavatelt endilt. Intervjuud viidi läbi enamasti online keskkonnas ning need intervjuueeritavate nõusolekul ka salvestati. Tüüpiliselt kestis intervjuu 60 minutit. Intervjuu kava on esitatud Lisana 2.

Lisaks intervjuudele viisime läbi **2 töötuba ning kogusime tagasisidet avaliku sektori esindajatelt**, et saada sisendit potentsiaalsete sidusrühmade huvide, murekohtade, kahtluste ning ootuste kohta personaalse andmeruumi lahenduste rakendamise osas. Sidusrühmade laiem kaasamine võimaldas muu hulgas kaardistada peamised väljakutsed personaalse andmeruumi lahenduse rakendamisel (vt ptk 9.1 Väljakutsed ja riskid).

- Rahvusvahelise MyData 2025 konverentsi (septembris 2025, Aalto Ülikoolis Soomes) raames korraldasime töötoa (ligi 30 osalejaga), et tutvustada personaalse andmeruumi projekti arenguid ning koguda sisendit võimalike riskide kohta. MyData võrgustik koosneb inimkeskse andmekorralduse ekspertidest erinevatest valdkondadest, kes omavad mitmekülgseid kompetentse (sh tehnoloogiline, õiguslik, äriline, disain), ning praktilist kogemust personaalse andmeruumiga seonduvate lahenduste arendamisest ning juurutamisest.

- Avaliku sektori andmehalduritele suunatud Andmelaagris (oktoobris 2025) tutvustasime personaalse andmeruumi projekti ning kogusime osalejatelt tagasisidet nii personaalse andmeruumi visiooni toetavate kui ka takistavate tegurite kohta.
- Koostöös Justiits- ja digiministeeriumi ning Riigi Infosüsteemi Ametiga korraldasime andmenõusolekuteenust ning personaalse andmeruumi projekti tutvustava seminari (detsembris 2025), mille käigus kogusime osalevatelt ettevõtetelt ning organisatsioonidelt sisendit nii nõusolekupõhise andmete jagamise laiendamise kui ka konkreetsete kasutusjuhtude potentsiaali kohta. Kuigi seminaril osales oodatust vähem inimesi (koos esinejatega 12 inimest), siis andis see võimaluse veelgi interaktiivsemaks aruteluks ning sisendi kogumiseks, et täpsustada ka organisatsioonide ärivajadusi ning potentsiaalseid kasutusjuhte.

Andmeanalüüsis kasutati kvalitatiivset, induktiivset ja iteratiivset lähenemist, mis oli kooskõlas uuritava nähtuse kujunemisjärgus olemusega. Intervjuude ja töötubade käigus kogutud andmete põhjal püüti tuvastada korduvaid mustreid, esilekerkivaid teemasid ning nendevahelisi seoseid. Analüüsiprotsess oli iteratiivne, see tähendab et taustaanalüüsi käigus kujunenud lähtehüpoteese täpsustati ja arendati edasi empiirilise materjali põhjal, samal ajal kui sidusrühmade kaasamise kaudu kogutud sisend võimaldas vahetulemusi valideerida ja rikastada. Analüüsis pöörati teadlikult tähelepanu eranditele ja vasturääkivustele, et vältida lihtsustatud järeldusi ning toetada nähtuse mitmetahulist käsitlust. Kogutud andmeid analüüsiti ning tõlgendati vastavalt uurimisküsimustele ning tulemused on integreeritud raporti erinevatesse peatükkidesse. Uuringu koostamisel hoidis uuringumeeskond ka tihedat suhtlust tellijaga, andes uuringutulemusi üle neljas osas, mis võimaldas valideerida uuringu ulatust (sh kaasata uusi intervjuueeritavaid) ja konkreetset fookust ning paremini kaasata tellija ootusi uuringu läbiviimisesse. Selline lähenemine võimaldas kujundada tervikliku ja kontekstuaalselt tundliku arusaama personaalse andmeruumi võimalikest rakendustest, väärtuspakkumisest ning peamistest väljakutsetest.

3. Mis on personaalne andmeruum?

Inimkeskse andmekorralduse raamistikust ning sihtidest tingituna on antud uuringu raames eesmärgiks otsida innovaatilisi andmepõhiseid lahendusi, mis aitaksid inimestel realiseerida oma eesmärgid ning samal ajal hõlbustaksid nende andmeõiguste praktikas rakendamist. Teisalt peaksid need lahendused olema organisatsioonidele äriselt motiveerivad ning toetama andmete väärimist. Selleks pakub võimaluse personaalse andmeruumi kontseptsioon, mille täpsem tähendus ja praktiline rakendus on seni jäänud ebaselgeks.

Varasemad kirjeldused personaalsetest andmeruumidest varieeruvad sõltuvalt sellest, kas analüüsi aluseks on võetud Euroopa Liidu õiguslikes ning poliitikakujunduslikes dokumentides leiduvad selgitused, selle kontseptuaalsed tunnused, disaini- ning rakenduslikud omadused või hoopis organisatsioonide ja üksikisikute perspektiiv (Lähtenoja 2023). Nii on nt Lehtiniemi (2017) kirjeldanud personaalset andmeruumi kui „andmesalvestusteenust koos liidestega andmevoogude haldamiseks” ja kui „vahendusteenuseid, mis võimaldavad kasutajatel isikuandmeid salvestada ja kontrollida nende jagamist kolmandate osapooltega”. Euroopa Andmestrategia (2020) viitas personaalsetele andmeruumidele kui eesmärgile anda inimestele „/.../ kontroll nende andmete üle, tagades neile vahendid ja võimalused teha üksikasjalikke otsuseid selle kohta, mida nende andmetega tehakse /.../.”

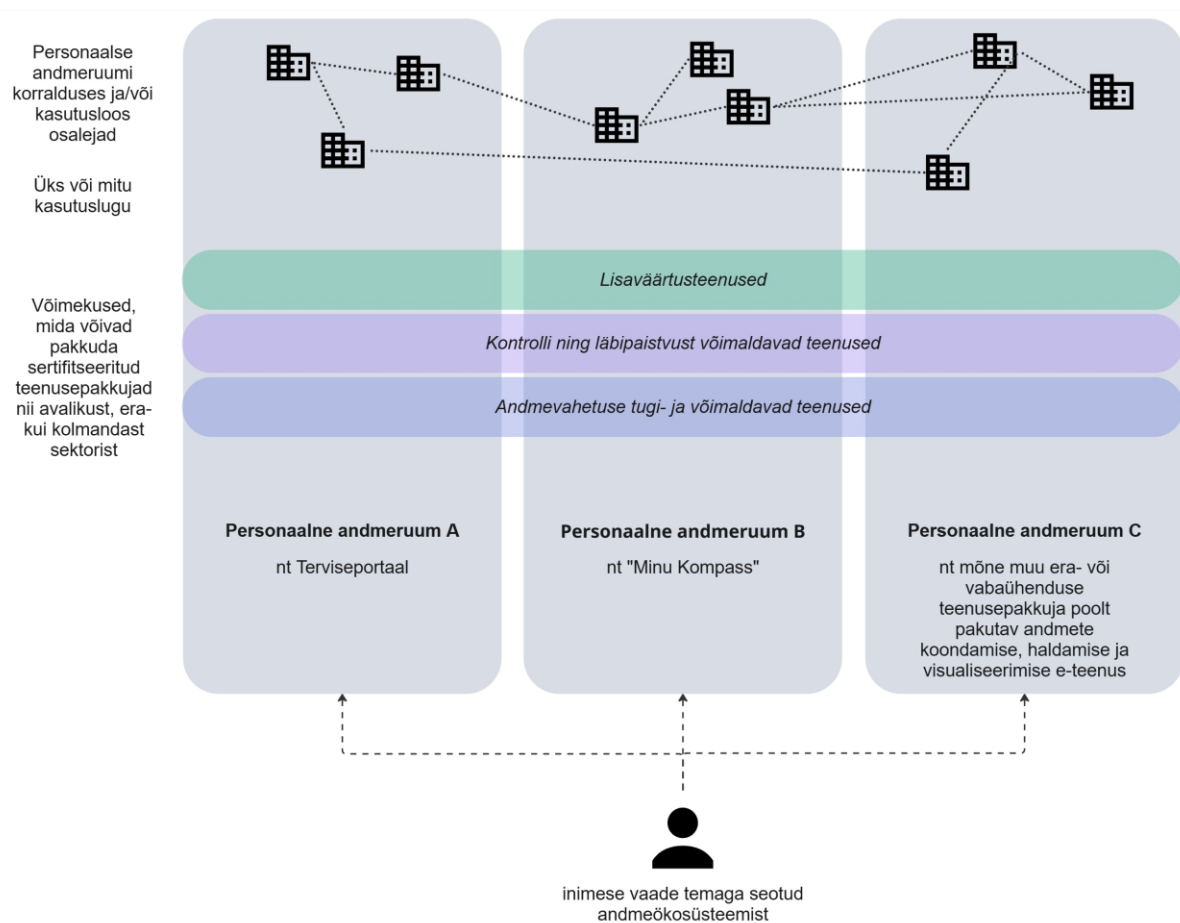
Kirjanduse põhjal näib olevat konsensus vaid personaalsete andmeruumide eesmärgi osas – need peaksid teenima inimeste huve. Praktikas tähendaks see tehnoloogiliste vahendite kasutamist seadusega tagatud õiguste (nt andmete kaitsmine, ligipääs andmetele jms) rakendamiseks, kuid veelgi enam inimeste võimestamist temaga seotud andmetega (nt andmete jagamine ning töötlemine personaliseeritud teenuste saamiseks, andmete iseseisvalt analüüsimine oma eesmärkide saavutamiseks). Nii kirjanduse kui läbiviidud intervjuude põhjal saab öelda, et personaalne andmeruum viitab **isiklikule vaatele temaga seotud andmetest ja seotud andmepõhistest teenustest**. Seetõttu määratleme käesolevas uuringus **personaalset andmeruumi laiema kontseptuaalse raamistikuna**, mis rakendub praktikas ühe või mitme e-teenusena.



Joonis 2. Inimese vaade oma andmetele läbi konkreetsete teenuste, kasutuslugude ja laiema korraldusliku raamistiku kihistuse.

Personaalse andmeruumi raamistik viitab, et inimeste andmete väärindamiseks ning inimkeskseks korralduseks on vajalik nii toimiv andmeökosüsteemi halduslik raamistik, mida turul tegutsevad osapooled suudavad järgida. Veelgi enam, personaalne andmeruum realiseerub vaid konkreetsete kasutusjuhtude kaudu, milles avalduvad ärilised ning halduslikud kokkulepped osapoolte vahel. Praktikas rakenduvad teenused peaksid sealjuures hõlmama konkreetseid funktsionaalseid võimekusi (vt lähemalt peatükist 5.3), mis võimaldavad inimesel oma andmeid hallata, kontrollida, jagada ning ka ise väärindada.

Seega defineerime *personaalse andmeruumi teenust* kui **“üksikisiku huvidest lähtuvat teenust, mis võimaldab temaga seotud andmeökosüsteemis andmeid hallata, kontrollida ning väärindada”**. Sealjuures võib inimene kasutada paralleelselt ühte või mitut personaalse andmeruumi teenust sõltuvalt oma eesmärkidest, eelistustest ning turul pakutavatest lahendustest. Samas võivad erinevates personaalsetest andmeruumides olla kaasatud samad komponendid ja/või mikroteenused (nt eID, nõusolekute haldus vms), mida võivad pakkuda turul sertifitseeritud teenusepakkujad. Joonis 3 annab ülevaate võimalikust stsenaariumist inimese poolt kasutatavatest personaalsetest andmeruumidest.



Joonis 3. Hüpoteetiline stsenaarium, kus inimene saab paralleelselt kasutada ühte või mitut personaalse andmeruumi rakendust, mis võimaldab tal hallata, kontrollida ja jagada oma andmeid talle huvipakkuvate kasutuslugude võimaldamiseks. Iga personaalne andmeruum kätkeb endas konkreetseid osalejaid ja nende vahelist andmekoostööd.

Personaalse andmeruumi teenused koosnevad **alamteenustest**, mis pakuvad teatavaid funktsionaalseid võimekusi (vt lähemalt peatükis 5.3). Neid saab jaotada **kolme eri tüüpi kategooriatesse** – a) otseselt andmevahetust võimaldavad või toetavad teenused, b) teenused, mis võimaldavad omada kontrolli andmete jagamise ning töötlemise üle, sealjuures tagades läbipaistvust andmetehingute osas ning c) lisaväärtust pakuvad teenused, mis kas otseselt või kaudselt väärtustavad inimesega seotud andmeid. Pakutavate alamteenuste täpne portfoolio ning praktiline rakendus sõltub konkreetse *personaalse andmeruumi teenuse* ärimudelist ning väärtuspakkumisest (nii inimesele kui ka liidestunud organisatsioonidele).

Silmas tuleb pidada ka asjaolu, et *personaalse andmeruumi teenused* ei pruugi pakuda inimesele täit vaadet temaga seotud andmetest ning nende töötlemisest. Konkreetse personaalses andmeruumis tekkinud „vaade“ pakub võimalust näha ning hallata vaid neid andmeid ning andmepõhiseid teenuseid, millega vastav *personaalse andmeruumi teenus* on liidestunud.

Peamine järeldus

Personaalne andmeruum viitab isiklikule vaatele inimesega seotud andmetest ja andmepõhistest teenustest, mistõttu tuleks mõista personaalset andmeruumi kui kontseptuaalset raamistikku, mis rakendub praktikas ühe või mitme e-teenusena.

Personaalse andmeruumi konkreetne vorm näib olevat dünaamiline, sõltudes nii osapoolte kokkulepetest andmepõhiseks koostöökaks ning muudest teguritest, mis tingivad selle rakendusliku eesmärgi ning pakutavad funktsionaalsed võimekused. Seetõttu ei pretendeeri käesoleva uuringu autorid kõikehõlmavale ning muid määratlusi välistavale definitsioonile. Pigem on antud uuringu eesmärgiks läheneda personaalse andmeruumi kontseptsioonile pragmaatiliselt, selgitades välja selle põhilised (strateegilised ning väärtuspõhised) karakteristikud, funktsionaalsed võimekused, rakendumise vormi ning potentsiaali Eestis.

Käesoleva uuringu autorite ettepanekul tuleks personaalse andmeruumi arendamisel lähtuda järgmistest põhimõtetest:

- Personaalse andmeruumi teenuse **peamine eesmärk on teenida üksikisiku huve ning eesmäärke**, kusjuures pelgalt andmetest ja selle kasutamisest ülevaate tekitamine ning nõusolekul põhinev andmehaldus pole piisav, et inimesi tõeliselt võimestada (Verhulst et al 2023). Seetõttu rõhutatakse ekspertide poolt ka usaldusisiku funktsiooni (*fiduciary duty*) kandmise olulisust, mis täiendaks andmehalduspraktikast tuttavate, kuid varasemalt peamiselt organisatsiooni eesmäärke täitvate andmehaldurite (*data stewards* ingl k) rolli.
- Inimeste andmete väärtustamiseks tuleb **inimest kaasata andmete haldamisse**, võimaldades tal lisaks IKÜMist tuttava andmesubjekt rollile kanda ka aktiivset andmeomaniku ning andmepakkuja rolli (vt lähemalt ptk 6 Rollimudel).
- Personaalse andmeruumi teenuse **kasutamine on paindlik ning vabatahtlik**, toimides peamiselt mugavusteenusena. See tähendab, et organisatsioonid peavad

arvestama ka võimalusega, et inimene ei soovi anda nõusolekut andmete integreerimiseks või nende täiendavaks töötlemiseks, mistõttu peavad olulisemate teenuste pakkumiseks säilima ka alternatiivsed andmete kogumise võimalused. Samuti on oluliste avalike teenuste puhul mõistlik lähtuda IKÜMi poolt defineeritud seaduslikest alustest, mis looks kindluse, et inimeste andmete kasutamine nt eluliste huvide kaitsmiseks, seadusjärgse kohustuse või avalikes huvides oleva ülesande täitmiseks ei jää inimese nõusoleku või tahteavalduse saamise taha. Küll aga võiksid personaalse andmeruumi funktsionaalsused võimaldada ka nendel puhkudel inimesel saada ülevaadet oma andmete kasutamisest (ning seda vajadusel vaidlustada).

- Turul võivad tegutseda samaaegselt **mitmeid erisuguseid personaalse andmeruumi teenuseid**, mida inimene saab paralleelselt kasutada. Sealjuures on oluline tagada nende koostalitlusvõime, et vältida jätkuvat killustatust ning võimestada inimest oma andmete ning nendega seotud teenuste võimaliku integreerimise läbi.
- Personaalse andmeruumi haldus on **kooskõlas laiema andmeökosüsteemi haldusega**, mis soodustab organisatsioonide ülest selgust erinevate rollidega seotud õiguste, kohustuste ning vastutuste osas.
- Personaalse andmeruumi realiseerimine **eeldab tugevat avaliku ja muude sektorite vahelist koostööd ning õiguslikku raamistikku**. Sealjuures on otsustuskohaks, kas personaalse andmeruumi tingimused tuleks sätestada riiklikul tasandil kehtiva õigusaktiga ning anda personaalse andmeruumi haldamine nt volitusnormiga mõnele konkreetsele avaliku sektori asutusele või pigem soosida sektoriteülest võrgustikupõhist andmeruumi haldust. Uuringu jooksul on autoritel tugevnenud arusaam, et avalikul sektoril on oluline roll andmeökosüsteemide halduse juhtimisel, samas kui innovatsiooni saab pakkuda era- ning kolmas sektor.
- Personaalse andmeruumi teenuste pakkumine eeldab **pikaajaliselt jätkusuutlikku ärimudelit**, lähtudes lisaks inimeste huvidele ka organisatsioonide olemuslikest eesmärkidest.

4.1 Väärtuspakkumine inimesele

Enne kui hakata määratlema personaalse andmeruumi ärilisi, organisatoorseid, tehnoloogilisi ja funktsionaalseid komponente ning nende võimalikku arhitektuuri, on vaja selgelt sõnastada probleem(id), mida *personaalne andmeruum* püüab lahendada ning millist kasu loob see nii inimesele kui organisatsioonidele. Selles ja järgnevas alapeatükis on vaatluse all personaalse andmeruumi kui kontseptuaalse raamistiku potentsiaal väärtusloomeks, mis avaldub veelgi selgemalt konkreetsetes kasutuslugudes (vt lähemalt ptk 8). Järgnev kaardistus on tekkinud autorite ning tellija arutelude analüüsil, mille käigus sõnastati ühiselt personaalse andmeruumi kesksete osapoolte (inimene kui andmesubjekt ja teenuste lõppkasutaja ning organisatsioon kui teenusepakkuja) peamised vajadused ning eesmärgid.

Personaalse andmeruumi **peamiseks eesmärgiks on teenida inimese huve**, arvestades tema erinevatest rollidest tulenevaid eesmärgi elukaare jooksul. Pole olemas standardset inimest, mistõttu tuleks inimkesksest teenusedisaini põhimõtete järgi uurida täpsemalt

erinevate kasutajaprofiilide spetsiifilisi vajadusi ning eelistusi. Nii on tänuväärne nt Justiits- ja digiministeeriumi poolt läbiviidavad inimkesksuse ja digilahenduste omnibussid⁴⁴ ning inimese digitaalse kaksiku uuringus⁴⁵ tehtud intervjuud ning persoonade kaardistus, mis annab väärtuslikku sisendit ka käesolevale uuringule. Need tulemused toonitavad inimeste heterogeensust nii teadlikkuse, ootuste ja eelistuste kui ka usalduse suhtes. Käesolevas uuringus on antud tulemusi analüüsitud inimkeskse andmekorralduse ning personaalse andmeruumi põhimõtete järgi ning kokkuvõtlikult saab välja tuua **neli peamist väärtuspakkumist**. Personaalse andmeruumi rakendused võiksid:

- **luua usaldust** inimese ning teenusepakkujate vahel, fookusega inimese andmete kasutamisel ning jagamisel;
- **suurendada inimese agentsust ning vabadust** teha iseseisvaid otsuseid oma andmete osas ning nende kaudu mõjutada oma elukeskkonda;
- **võimaldada inimesele terviklikku vaadet oma andmetele ning digiteenustele**, hõlbustades nn virtuaalse elu korraldust;
- **luua konkreetset väärtust inimesele**, kusjuures loodav kasu on kontekstispetsiifiline, sõltudes nii inimeste huvidest, eelistustest ning ka konkreetsetest kasutusjuhtudest, mida *personaalse andmeruumi* teenus võimaldab.

Siinkohal võib küll esimest kolme kasutegurit näha personaalse andmeruumi poolt loodava väärtusena iseeneses, kuid kitsamalt vaadatuna näivad need ka olulise eeldusena, et inimesed oleksid üldse valmis kasutama *personaalse andmeruumi* teenuseid ning seeläbi saama erinevate kasutusjuhtude kaudu konkreetset kasu.

Paraku saab nende nelja aspekti osas välja tuua ka mitmeid tänaseid probleemikohti:

- **Usalduse puudumine:** inimeste usaldus ettevõtete suhtes oma andmete kaitsmisel on madal, mis võib viidata tekkinud eraelupuutumatus riivele (saadud kahju) ja/või tingida usaldamatust teenuste kasutamise suhtes (saamata väärtus). Näiteks usaldavad Eesti elanikud 2025 aasta seisuga erasektori ettevõtteid palju vähem (42% elanikkonnast) kui näiteks riigiasutusi (76% elanikkonnast)⁴⁶.
- **Vähene praktiline kontroll:** inimestel puudub lihtne ning mugav võimalus otsustada oma andmete kasutamise üle (või seda mõjutada) ning kasutada endaga seotud andmeid oma elu korraldamisel. Samas on kontrolli rakendamine vabatahtlik ning ei peaks muutuma kohustuseks.
- **Killustatus:** andmed ning kasutatavad teenused on killustunud eri platvormide ning nendega seotud ökosüsteemides.
- **Piiratud kasu või selle ebaõiglane jaotumine:** andmete mittekasutamisel on arvestatav (kuid mitte alati tajutud) kulu (nt ebatõhusad protsessid, dubleerimine jne) ning andmete väärindamisest loodav kasu on piiratud (nn kasutamata võimalused andmepõhiseks väärtusloomeks). Samuti kuulub siia kategooriasse andmete

⁴⁴ Eesti elanike suhtumine digiriiki ja tehnoloogilistesse lahendustesse, <https://andmed.eesti.ee/datasets/eesti-elanike-suhtumine-digiriiki-ja-tehnoloogilistesse-lahendustesse>, külastatud 21.03.2026

⁴⁵ Vt lähemalt <https://riigihanked.riik.ee/rhr-web/#/procurement/8849884/documents?group=B>, külastatud 23.03.2026

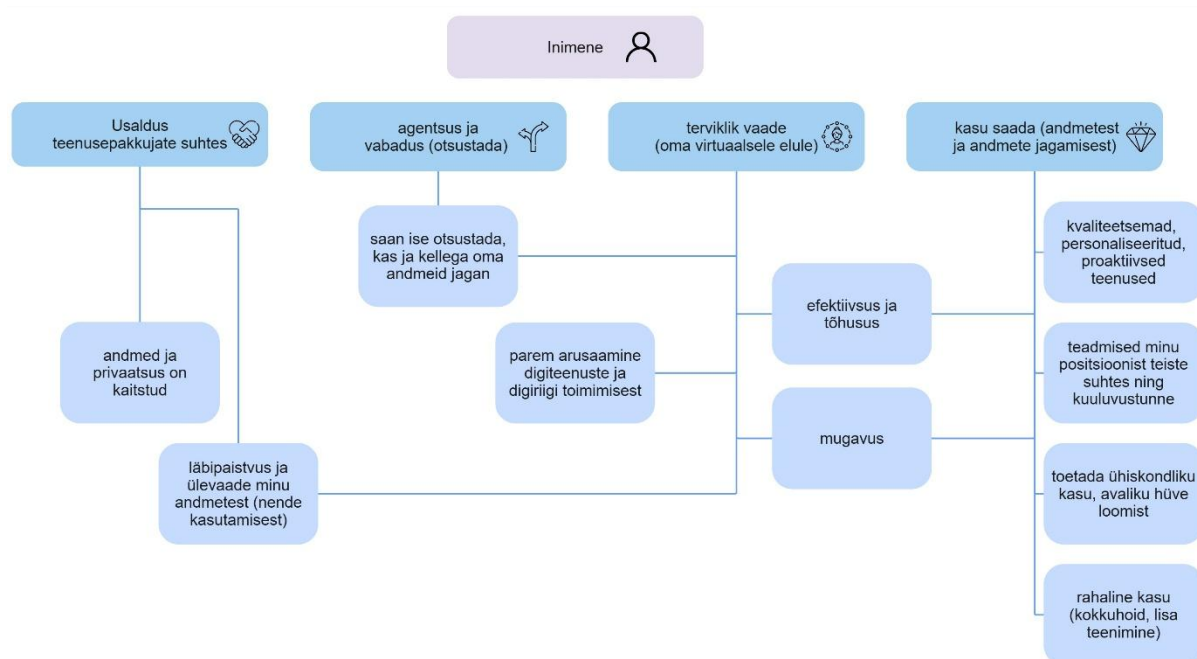
⁴⁶ Tulemused kättesaadavad aadressil <https://andmed.eesti.ee/datasets/eesti-elanike-suhtumine-digiriiki-ja-tehnoloogilistesse-lahendustesse>, külastatud 21.03.2026

väärindamisest saadava kasu ebaõiglane jaotumine, nt inimeste andmete ekspluateerimine kasumi teenimise nimel.

Personaalse andmeruumi eeldatav väärtus inimesele on tugevalt seotud mitmete alamkategoriatega nagu:

- soov, et inimese andmed ja privaatsus oleks kaitstud
- soov ise otsustada, kas ja kellega oma andmeid jagada
- omada ülevaadet oma andmetest (ja nende kasutamisest)
- parem arusaamine digiteenuste ja digiriigi toimimisest
- efektiivsus ja tõhusus
- mugavus
- kvaliteetsemad / personaliseeritud / proaktiivsed teenused
- saada teadmisi enda positsioonist teiste suhtes (millega seondub ka vajadus kuuluvustunde järgi)
- toetada ühiskondlik kasu loomist
- rahaline kasu (kokkuhoid, lisa teenimine)

Nimetatud ootused personaalse andmeruumi poolt loodavale väärtusele on omavahel seostatud ning esitatud ka Joonisel 4.



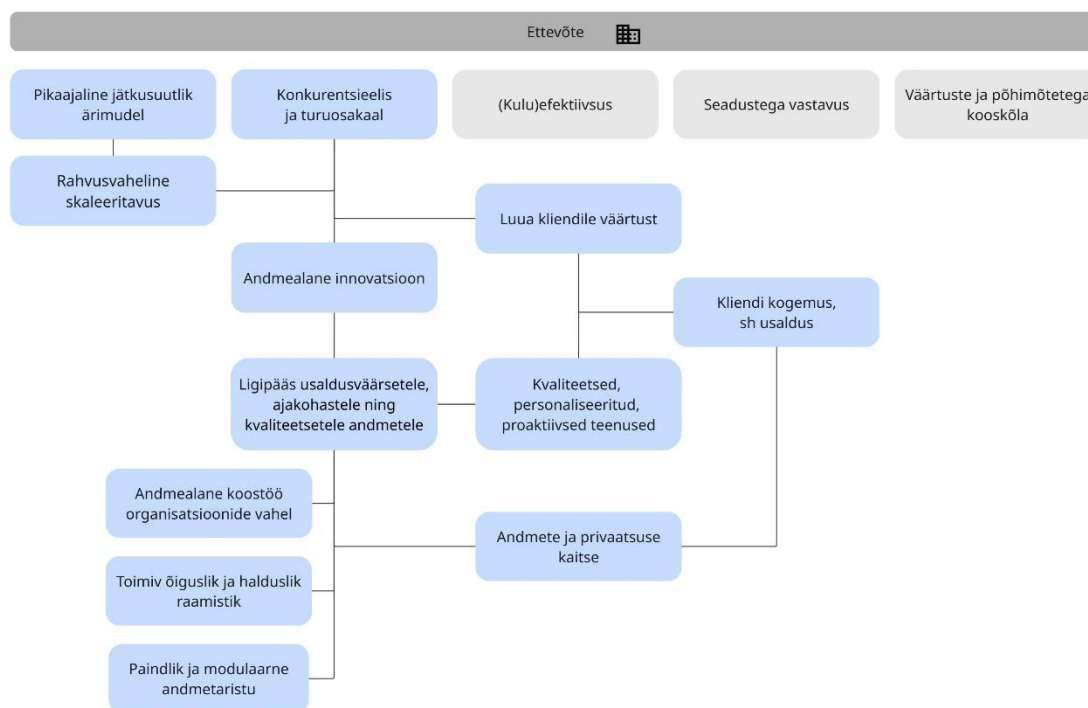
Joonis 4. Inimese eelduslikud vajadused ning ootused personaalse andmeruumi poolt loodavale kasule.

Peamine järeldus

Inimeste jaoks seisneb personaalse andmeruumi rakenduste väärtus eelkõige võimalusena oma andmeid mugavalt kontrollida, saada aru andmete kasutamisest digiteenustes (läbipaistvus) ja saada konkreetset kasu (mugavus, efektiivsus, uued teadmised, personaliseerimine, võimalik rahaline väärtus). Ilma selge ja tajutava kasuta ning usaldusega ei teki inimesel motivatsiooni andmete jagamiseks, isegi kui tehnilised võimalused on selleks olemas.

4.2 Väärtuspakkumine organisatsioonidele

Lisaks inimesele loodavale hüvele on oluline kirjeldada väärtuspakkumist ka organisatsioonide jaoks, kes on vastavate personaalse andmeruumi teenuste peamine arendaja ja/või rakendaja ning selle kaudu andmepõhiste toodete ja teenuste pakkuja. Andmeruumis osalejate motiveerimiseks on vaja defineerida strateegiline eesmärk ja kirjeldada saadav kasu, et õigustada vajaminevaid investeeringuid ning võimalikke muutusi olemasolevates protsessides. Sealjuures on erinevate sektorite organisatsioonidel erinevad ülesanded (kas kasumi teenimine, avaliku ülesande täitmine ja/või ühiskondliku hüve loomine). Käesolevas uuringus on huviorbiidis just eraettevõtted, mistõttu on Joonisel 5 esitatud väärtuspakkumise kaardistus just ettevõtte vaatenurgast. Sealjuures tuleb nentida, et olenevalt tegevusvaldkonnast ning personaalse andmeruumi rollimudelitest lähtuvalt võib täpne väärtuspakkumine üsnagi palju erineda.



Joonis 5. Organisatsioonide olemuslikud eesmärgid ning sellest tulenevad võimalikud vajadused ning ootused personaalsele andmeruumi poolt loodavale väärtusele.

Kokkuvõtlikult näib ettevõtete olulisemateks eesmärkideks olevat tagada pikaajaline jätkusuutlik ärimudel, konkurentsieelis ja piisav turuosakaal. Samuti on oluliseks organisatsiooniliseks huviks tagada tegevustest kuluefektiivsus, seadustega vastavus ning organisatsiooni väärtuste ja põhimõtetega kooskõla. Viimased aspektid on joonisel eristatud halli värviga, kuna personaalne andmeruum neid otseselt ei adresseeri. Küll aga võib personaalse andmeruumi raamistik ning sellele vastavad võimekused toetada ettevõtte äritegevust, kui see aitab luua andmealast innovatsiooni (uued andmealased ärimudelid ning andmepõhised tooted ja teenused), luua klientidele väärtust ning toetada rahvusvahelist skaleeritavust. Selle kasu avaldamiseks saab personaalse andmeruumi raamistik toetada järgnevaid ärivajadusi (kaardistatud ka ptk 4):

- Soosida ligipääsu usaldusväärsetele, ajakohastele ja kvaliteetsetele andmetele;
- Soosida kvaliteetsete personaliseeritud ja proaktiivsete teenuste loomet ning pakkumist;
- Soosida andmealast koostööd organisatsioonide vahel;
- Tagada inimeste andmete ja privaatsuse kaitse;
- Pakkuda paindlikku ja modulaarset andmetaristut;
- Pakkuda toimivat õiguslikku ja halduslikku raamistiku andmete kogumiseks, töötlemiseks ja jagamiseks.

Siinjuures tuleb nentida, et personaalse andmeruumi raamistik on alles väljakujunemise faasis ning seetõttu tuleb hinnata tänaseid lahendusi ettevaatlikkusega.

Peamine järeldus

Ettevõtete jaoks seisneb personaalse andmeruumi väärtus andmete kättesaadavuse suurendamises, uutes ärimudelites ja võimaluses arendada kõrgema lisandväärtusega teenuseid. Samas nõuab see investeeringuid ning selget ärilist põhjendust, mida täna sageli ettevõtted veel ei tunneta (vt lähemalt ptk 4).

4.3 Näiteid Eestist ja mujalt

Personaalse andmeruumi teenuste konkretiseerimiseks on kasulik viidata olemasolevatele teenustele ning teenuspakkujatele, mis rakendavad inimkeskset andmehalduspraktikat. Kuigi personaalse andmeruumiga seonduvaid teenuseid on mitmeid (vt nt Euroopa Komisjon 2025, Micheli et al. 2023, MyData Global 2025), siis järgnevalt toome esile vaid mõned näited nii Eestist kui välismaalt.

Terviseportaal on Eesti inimestele suunatud digivärv nendega (ja nende lähedastega) seotud terviseandmetele ning teenustele, mida haldavad Tervisekassa ning Tervise ja Heaolu Infosüsteemide Keskus (TEHIK). Platvormi kaudu on inimesel võimalik turvaliselt vaadata ja hallata oma terviseandmeid, broneerida vastuvõtte, esitada tõendeid ja deklaratsioone, määrata esindajaid ning samuti tegutseda lähedaste nimel. Terviseportaal on kasulik ka terviseteenuste osutajatele, võimaldades turvalist ning tõhusat andmepõhist koostööd.

Terviseportaali võib käsitleda kui personaalset andmeruumi tervise valdkonnas, mis aitab inimesel ligi pääseda enda terviseandmetele ning otsustada, kes ja millal võib tema andmeid näha või kasutada (nt esindajate määramine, logiraamat juurdepääsude jälgimiseks). Lisaks võimaldab Terviseportaal võrrelda ja mõista oma terviseinfot selges ja lihtsas keeles ning teha teadlikke otsuseid oma tervise ja ravi kohta, tuginedes andmepõhisele ülevaatele. Selline koondatud ülevaade ning protseduurilised võimekused tuginevad inimkesksete põhimõtete rakendamisel andmete ning terviseandmete ökosüsteemi haldamises, et tagada läbipaistvus, soosida inimeste andmesuveräänsust⁴⁷ ning võimestada inimesi tegema andmepõhiseid otsuseid oma tervise eest hoolitsemisel.

Eesti.ee teabevärv on Eesti elanikele ning ettevõtjatele suunatud riiklik digikeskkond, mis eraisiku vaatest koondab riigi poolt kogutud ja kasutatud isikuga seotud andmeid ning võimaldab kasutada näiteks erinevate elusündmustega (nagu lapse sünd, abiellumine jms) seotud e-teenuseid. Inimene saab pärast sisselogimist vaadata oma andmeid eri registrites, dokumentide kehtivust, kusjuures andmed on jätkuvalt talletatud detsentraliseeritult erinevate asutuste serverites.

Eesti.ee portaal koondab endas ka mitmeid personaalsele andmeruumile omaseid funktsioone ja teenuseid. Näiteks võimaldab see jälgida oma andmete kasutust erinevate osapoolte poolt (ligipääs nn logidele) ning hallata enda poolt antud nõusolekuid andmete jagamiseks ning teiseseks töötlemiseks. Sealjuures on Andmejälgija ning andmenõusolekuteenuse kasutamine piiratud sellega liidestunud andmekogude ning andmetarbijatega. Sellegipoolest toimib Eesti.ee keskkond kui strateegiline lüli inimese, riigi ning teatud juhtudel ka kolmandate osapoolte vahel, võimaldades tõhusamat, läbipaistvamat ning kasutajasõbralikumat suhtlust avaliku sektori teenustega.

Athumi on Flandria regiooni avalik-õiguslik ettevõte, mis pakub andmevahendusteenuseid vastavalt ELi andmehaldusmäärusele, sealjuures olles ka Belgia poolt ametlikult tunnustatud andmevahendusteenus⁴⁸. Ettevõtte arendab ja haldab koostalitlusvõimelisi digiplatvorme (nt **GIPOD**, **VIP**, **KLIP** ja **eLys**⁴⁹) energia, liikuvuse, kinnisvara, logistika, tervishoiu jt valdkondades, võimaldades organisatsioonidel ja kodanikel jagada ning kasutada andmeid turvaliselt ja läbipaistvalt. Athumi teenused põhinevad Solid tehnoloogial, mille aluseks on detsentraliseeritud andmeplatvormide (nn Pod-ide, *personal online datastore*) spetsifikatsioon, mis võimaldab üksikisikutel ja organisatsioonidel talletada ning hallata isiklikku või konfidentsiaalset teavet ja kontrollida andmetele ligipääsu- ning töötlemise tingimusi. Nn pod-id on tihedalt seotud isikuandmete kukrute (*personal data store*) lähenemisega, mis võimaldavad inimesel talletada endaga seotud andmeid turvaliselt ning seeläbi omada otsest kontrolli, kes ja mis eesmärgil nendele andmetele ligi pääseb. Athumi positsioneerib end seetõttu ka personaalse andmeruumi arendaja ja pakkujana, rakendades inimkeskse andmehalduse põhimõtteid erinevate osapoolte vahelise andmekoostöö arendamisel ning soosides inimeste andmesuveräänsust, andmeökosüsteemide turvalist ning koostalitlusvõimelist toimimist ning seeläbi ka andmepõhiste teenuste ning toodete arengut.

⁴⁷ Andmesuveräänsus viitab nii inimeste kui organisatsioonide õigusele ja võimele oma andmete üle otsustada ning kontrollida, kas, kuidas ja milleks neid andmeid kasutatakse. Inimkeskse lähenemise järgi rõhutatakse inimeste õigusi oma andmete üle ning sellega kaasnevat andmesuveräänsust, isegi juhul kui andmed on kogutud ning talletatud organisatsioonide poolt.

⁴⁸ <https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services>, külastatud 23.03.2026

⁴⁹ vt lähemalt <https://athumi.eu/en/solutions-platforms>, külastatud 23.03.2026

iGrant.io on Rootsis asutatud eraettevõte, mis pakub nii inimesele suunatud andmevahendusteenust kui ka EUDI50 digikukru teenuseid, mis baseeruvad avatud standarditel, kontrollitavate tõendite (verifiable credentials) kasutamisel ning volituspõhisel andmevahetusel. iGrant.io lahendus pakub nii eraisikutele kui ettevõtetele võimalust läbipaistvaks, turvaliseks ning koostalitlusvõimeliseks andmeökosüsteemiks, soosides seeläbi uute andmepõhiste teenuste teket. Seetõttu seondub iGrant.io lahendus ka personaalse andmeruumi kontseptsiooniga, kuna see võimaldab inimestel hallata oma andmeid, kontrollida nende kasutamist ning jagamist, samal ajal kaitstes inimeste privaatsust ning säilitades andmete terviklikkuse ja regulatiivse vastavuse (IKÜM, eIDAS).⁵¹

⁵⁰ EUDI (European Digital Identity) - Euroopa digitaalne identiteet.

⁵¹ Vt lähemalt <https://www.igrant.io/>, külastatud 23.03.2026

4. Ärivateadused

Eesti digiriigi areng on loonud tugevad tehnoloogilised eeldused turvaliseks andmevahetuseks, millele aitab kaasa usaldusväärne digitaalne identiteet, X-tee kasutamine nii avalikus kui erasektoris, valdkondlikud registrid ning andmetöötuse logimise ja andmenõusolekuteenuse esimesed lahendused. Samal ajal on jätkuvalt mitmeid väljakutseid andmepõhiste teenuste arendamisel ja pakkumisel, samuti pole andmete korraldus ega teenused inimese vaates alati läbipaistvad ega mugavad.

Käesoleva teostatavusanalüüsi üheks eesmärgiks on kaardistada organisatsioonide **äriateadused ja võimalikud kasutusjuhud inimeste andmete jagamiseks ning laiemaks väärimdamiseks**, uurides samal ajal nende nägemust inimkeskse andmekorralduse kasust ning potentsiaali ettevõtluse toetamisel. Sealjuures on antud uuringus fookusesse võetud **finants- ja haridusvaldkonnad**, kuna hinnanguliselt on nendes valdkondades piisav andmeküpsus andmepõhiste teenuste rakendamiseks. Seetõttu tuleks käesolevas peatükis kirjeldatud vajadusi ning väljakutseid hinnata nende valdkondade ulatuses. Ühtlasi on need kogutud uuringu käigus intervjueritud organisatsioonide esindajatelt ning **ei pruugi kehtida teiste organisatsioonide kohta**. Järgnevalt kirjeldame, millised intervjueritavate poolt tunnetatud vajadused võiksid viia personaalse andmeruumi kasutuslugude realiseerimiseni.

3.1 Andmepõhiste toodete ja teenuste pakkumisest tulenevad vajadused

Digitehnoloogiate ning andmete kasutamine ettevõtluseks eeldab organisatsioonide võimekust andmeid koguda, neid analüüsida ning teenusearendusse suunata. Mitmed intervjueritud finants- ja haridusvaldkonna esindajad jagasid seisukohta, et andmed on ettevõtete jaoks olulise väärtusega, kuid isikustatud andmete kasutamise vajadus sõltub konkreetsest protsessist, näiteks müügitöö, lepingute sõlmimine ja menetlemine, teenusearendus.

Andmepõhise äri üheks olulisemaks tingimuseks on **ligipääs kvaliteetsetele andmetele**, et töötada välja vajalikud ärimudelid, tagada otsuste õiguspärasus, täpne riskide juhtimine ning teenuste usaldusväärsus. Tõhus andmepõhine tegutsemine eeldab ligipääsu andmetele, mille päritolu on selgelt tuvastatav ning mida on võimalik masinloetavalt pärida, jagada ning kontrollida. Sageli on andmete pärimisel väljakutseks **andmete ajakohasus, terviklikkus ning samas piisav granulaarsus**. Ühest küljest sooviksid organisatsioonid piisaval hulgal andmeid, et nende relevantsust oma organisatsiooni spetsiifikast lähtuvalt hinnata. Teisalt nähakse kitsaskohana monoliitsete lahenduste kasutamist, kus asutusel pole võimalik andmekogumist valida välja vaid endale huvipakkuvaid andmeid. Seetõttu väljendati ühes intervjuus ka positiivse arenguna 2026. aastast kehtivat muudatust rahvastikuregistrist andmete pärimise hõlbustamisel, võimaldades pärijal küsida vaid osa vajaminevaid andmeid. Teisalt kätkeb endas andmete süstemaatiline kogumine ja pärimine mõnelt muult asutuselt ka **tehnilisi arendusi ning halduslikke kokkuleppeid** (nt lepingute sõlmimine), mis võib näida ebamõistlikult kulukas.

Andmete kogumise kontekstis on organisatsioonide vaatest üheks väljakutseks **andmete killustatus, mis teeb andmete kokku kogumise koormavaks**. Killustatus ei viita ainult

andmete hajususele nende talletamise mõttes, vaid ka andmekirjelduste üheti mõistetavusele ning standardiseeritud viisil esitamisele. Andmete hajusalt hoiustamisel on ka kasutegureid, nt turvalisusega seonduvad aspektid.

Mõni intervjuueeritud organisatsioon väljendas **väljakutsena ka isikupõhiste toodete ja teenuste arendamist ja pakkumist**, kuna see nõuab üsna suurel hulgal andmete kogumist ning keerukate protsesside ülesehitamist. Seni on kehtiv praktika näiteks paljude kindlustustoodete pakkumisel mõne grupitasandi omaduse (vanus, tegevusala jms) kasutamine, mis võimaldab lihtsustada ettevõtte jaoks küll tootearendust, kuid piirates nii inimeste kui innovaatilisemate ettevõtete vaatest võimalust personaliseeritud hinnastamiseks ja uute tootegruppide (nt riskikäitumist ennetavad või leevendavad teenused) pakkumiseks.

Isikuandmete töötlemiseks, sh kogumiseks, peavad organisatsioonid **tagama vastava õigusliku aluse** ning kehtiva õigusraamistiku kontekstis on näiteks nõusolekupõhine andmete kogumine osade ettevõtete silmis **äriliselt liiga ebakindel**. Mõne kaasuse puhul kasutatakse lisaks seadusest tuleneva kohustuse või õigustatud huvi kasutamist ka lepingupõhise andmete töötlemise, sh jagamise, loogikat (nt töötajate andmete jagamise alus on sätestatud juba töölepingus või laenulepingu sõlmimiseks vajaminevate andmete pärimiseks sõlmitakse kliendiga leping). Lepingupõhine andmete jagamine pärsib aga inimese vaatest andmenõusolekute ja/või tahteavalduste terviklikku haldamist, sest protsessiloogika ning võimalused on erinevad.

Intervjuueeritavad väljendasid ka huvi suurendada andmete jagamist ning riskasutust, eriti olukorras, kus kliendid peavad jätkuvalt esitama manuaalselt tõendeid nt oma hariduse, oskuste või sissetulekute kohta, samal ajal kui vastavad andmed on tegelikult juba mõnes registris olemas. Selline olukord loob selge vajaduse lahenduste järele, mis vähendavad **tõendite käsitsi kogumist ja korduvat esitamist** ning toetavad andmete turvalist ja tõhusat taaskasutust inimese kontrolli all. Kuigi mõned lahendused (nagu andmenõusolekuteenus) on täna juba osati kasutusel, pole see veel laiemalt kasutusele võetud. Suurtes kogustes andmete kogumise ning hoiustamise suhtes tunnetatakse ka vastutust ning teatavaid riske, sooviga tagada andmete **kaitse ja turvalisus**.

Peamine järeldus

Andmepõhiste toodete ja teenuste pakkumise kontekstis on olulisemad väljakutsed ja vajadused järgmised:

- *piiratud ligipääs usaldusväärsetele, ajakohastele ning kvaliteetsetele andmetele;*
- *andmete killustatus, mis teeb andmete kogumise keerulisemaks;*
- *andmete jagamist toetavate arenduste ning liidestuste kulukus;*
- *isikupõhiste teenuste ja toodete arendamise keerukus;*
- *nõusolekupõhise andmete kogumise ebakindlus äristrateegia kontekstis – mida teha siis kui nõusolekud tagasi võetakse?;*
- *andmete manuaalne kogumine ja/või korduva esitamine;*
- *andmete ja privaatsuse kaitse.*

3.2 Tehnoloogiast ja andmetaristust tulenevad vajadused

Intervjuude käigus on korduvalt esile toodud, et katsed luua keskne platvorm, mis koondaks eri sektorite andmed ja teenused ühte süsteemi, on osutunud raskesti ülalpeetavaks. Aja jooksul on sellised lahendused kaotanud paindlikkuse, muutunud kulukaks või hääbunud, kuna need eeldasid osapooltelt oma olemasolevate infosüsteemide ümberkujundamist ning rollimuutusi, millega paljud organisatsioonid ei saanud või ei soovinud kaasa minna. Samuti võib selline lähenemine vähendada süsteemide autonoomiat, mis on vajalik selleks, et erinevad valdkonnad saaksid täita oma seadusest või äristrateegiast tulenevaid funktsioone näiteks hariduse, energia, finants- ja tervisevaldkonnas. Ärilisest vaates on seetõttu mõistlikum lähenemine selline, mis ei eelda andmete koondamist ega olemasolevate süsteemide asendamist, vaid loob mehhanismi, mille kaudu senised osapooled saavad andmeid vahetada ühiste põhimõtete, standardiseeritud liidestuste ning seadusega reguleeritud õiguslikel alustel. Selline **paindlik arhitektuurne lähenemine** vähendab nii andmete tsentraliseerimise (või dubleerimisega) seotud riske, võimaldab organisatsioonidel säilitada oma senised rollid ja vastutuse ning toetab osapoolte järkjärgulist liitumist ökosüsteemiga ilma, et kõigilt eeldataks korraga üleminekut uuele platvormile.

Inimeste andmete põhise ökosüsteem realiseerimine sõltub suuresti ka sobiliku **nn pehme andmetaristu olemasolust**, mis soodustaks koostalitlusvõimet organisatsioonide ning jurisdiktsioonide üleselt. See tähendab ühiste organisatsiooniliste, tehniliste ja semantiliste kokkulepete olemasolu, mis võimaldavad turvalist ja masinloetavat andmete taaskasutust, sh standardiseeritud andmemudelite, API-liideste ja selgete metaandmete kirjelduste laialdast kasutuselevõtmist. Koostalitlusvõimeline ning modulaarsele arhitektuurile ülesehitatud ökosüsteem toetaks sealjuures ettevõtete vahelist konkurentsi ning vähendaks sõltuvust üksikute teenusepakujate lahendustest. Intervjueeritavate sõnul on sellise pehme taristu loomisel võtmeroll riigil ning rahvusvahelistel võrgustikel, millega soosida turuosaliste omavahelist andmekoostööd.

Peamine järeldus

Kuigi tehnilised arendused võivad olla sageli keerukad ning nõuavad teatavat lisaressurssi, siis intervjueeritavad ei pidanud tehnilisi väljakutseid oluliseks takistuseks inimeste andmete väärindamisel. Üks olulisemaid kitsaskohti on siiski koostoime ning laialt kasutatavate standardite puudumine.

Peamiste vajadustena väljendati paindliku ning modulaarse tehnilise arhitektuuri rakendamise ning nn pehme andmetaristu olemasolu tagamist, millega soosida turuosaliste vahelist andmete vahetamist.

3.3 Ärikeskkonnast ja ühiskondlikust nõudlusest tulenevad vajadused

Andmepõhine innovatsioon põrkub sageli kehtivate ärimudelite, praktikate ning turuosaliste vaheliste kokkulepetega. Samuti sõltub uute lahenduste realiseeritavus Eesti või rahvusvahelisel turul tekkinud **ärilisest võimalusest**. Näiteks töid intervjueeritavad välja, et Eestis ei oma eratervisekindlustus veel nii suurt ärilist tähtsust, kuna see ei konkureeri riigi poolt pakutava solidaarse tervisekindlustusega. Seetõttu ei näe intervjueeritud kindlustusseltsid veel vajadust isikupõhiste andmete laiemaks väärindamiseks, näiteks personaliseeritud tervisekindlustusprofiilide loomiseks. Teisalt tõdeti, et uute tehnoloogiate kasutuseletuleku ning platvormitöö laia leviku tõttu on tekkinud võimalus pakkuda inimkeskseid tooteid ja teenuseid, mis põhineksid inimese käitumuslikel andmetel, sõltumata organisatsioonist, kus need loodi ja talletati. See avab võimaluse töötada välja proaktiivseid lahendusi, mis keskenduvad ennetusele ning inimese elu, karjääri, tervise ning heaolu juhtimisele. Äriline huvi andmepõhisteks lahendusteks sõltub seetõttu tugevalt **туру seisust ning olemasolevatest lahendustest ning ärivõimaluse tuvastamisest**.

Üks keskseid ärivajadusi andmete laiemaks väärindamiseks on **toimiv ning stabiilne õiguslik ning halduslik raamistik**. Erinevate kasutusjuhtude puhul tugineb andmete töötlemine sageli paralleelselt mitmele õiguslikule alusele, sealhulgas andmesubjekti nõusolekule, lepingulistele suhetele, avalikule huvile või seadusest tulenevatele kohustustele. Ärikeskkonna seisukohast on kriitiline, et nende õiguslike aluste koostoime oleks selgelt määratletud, ette ennustatav ja standardiseeritud, mitte iga konkreetse kasutusjuhtumi puhul eraldi tõlgendatav. Sealjuures on oluline ka selge rollide ning vastutuste jaotus andmete töötlemise ning -vahetuse operatiivse teostamise, andmete (taas)kasutamise, õigusliku hindamise ja järelevalve vahel.

Näiteks reguleerib Euroopa Liidu tasandil pankadevahelist andmete jagamist eelkõige makseteenuste direktiiv (PSD2), mille alusel on kujunenud avatud pangaduse (*Open Banking*) raamistik. See võimaldab kolmandatel osapooltel, sh teistel pankadel või volitatud teenusepakujatel, saada inimese nõusoleku alusel ligipääsu tema kontoinfole standardiseeritud liidest (API-de) kaudu. Samas piirab andmete laiemat taaskasutamist Eesti õiguses krediidiasutuste seaduse paragrahvist 88 tulenev pangasaladuse regulatsioon, mille kohaselt on kliendi kohta teada saadud andmete avaldamine kolmandatele isikutele üldjuhul keelatud ning lubatud vaid seaduses sätestatud erandite või kliendi selgesõnalise nõusoleku alusel. See tähendab, et ka finantsasutuste omavaheline andmevahetus on vaikselt piiratud ning eeldab selget õiguslikku alust. Euroopa Liidu tasandil on seda piirangut asumas täpsustama ja tasakaalustama ka finantsandmete juurdepääsu määrus (*Financial Data Access Regulation*, FIDA⁵²), mille eesmärk on laiendada senist avatud panganduse kontseptsiooni. FIDA peaks looma ühtse õigusraamistiku, mis võimaldab kliendi kontrolli all olevat finantsandmete turvalist ja standardiseeritud jagamist erinevate pankade ja finantsteenuse pakujate vahel, hõlmates lisaks maksekontodele ka teisi finantstooteid. Seeläbi ei kaota pangasaladus oma kaitsefunktsiooni, kuid andmete kasutamine muutub kliendi nõusolekul süsteemseks ja prognoositavaks, mitte erandite põhiseks.

⁵² Vt lähemalt https://finance.ec.europa.eu/digital-finance/framework-financial-data-access_en, külastatud 25.03.2026

Andmepõhise ettevõtluse üheks taotluseks on **konkurentsieelise saavutamine ja majandusliku jätkusuutlikkuse tagamine**. Eesti turu väiksusest tulenevalt on paljude ettevõtete jaoks oluline, et arendatavad teenused oleksid skaleeritavad ja rakendatavad ka väljaspool Eesti turgu. See eeldab **toimivat, prognoositavat ja kulutõhusat raamistikku** andmete kasutamiseks ning jagamiseks ka rahvusvahelisel tasandil, kuid samamoodi skaleeritavate funktsionaalsete komponentide kasutamist (näiteks millistele digitaalse identiteedi lahendustele on teenused üles ehitatud). Kui andmetele ligipääs ja nende kasutamise tingimused on ebaselged või liigselt piiravad, suureneb eriti väiksemate ettevõtete jaoks **innovatsioonirisk** ning väheneb nende võime konkureerida suuremate turuosalistega (kes näiteks juba oma suuruse tõttu saavad organisatsiooni sees andmeid märksa laiemalt väärindada). Seetõttu on ärikeskkonna vaates oluline raamistik, mis toetaks **ausat konkurentsi, standardiseerimist ja koostalitlusvõimet**, vältides samal ajal ülereguleerimist ja Eesti-spetsiifilistesse lahendustesse lukustumist.

Laiemast keskkonnast tuleneva ärivajadusena tõstatasid intervjuueritavad ka **inimeste teadlikkuse, usalduse ja nõudluse** temaatika. Nimelt sõltub inimese poolt kontrollitud andmejagamine tugevalt nende poolt tunnetatud protsessi arusaadavusest, usaldusest teenusepakkujate suhtes ning motivatsioonist andmeid jagada. Mitmed intervjuueritavad väljendasid skeptitsismi inimeste rolli suurenemise osas andmete jagamisel, teised aga nentisid, et uute tehisarude ja muude lahenduste tõttu on inimeste teadlikkus paljuski tõusnud. Inimestel on tekkinud huvi ning kogemus enda andmete osas ning see võiks tulevikus suurendada ka laiemalt inimeste nõudlust kvaliteetsete, personaliseeritud ning andmepõhiste toodete ja teenuste järgi. Samal ajal tuleb arvestada kasutajate väga erineva digipädevuse ja ootustega. Inimkeskne lähenemine ei tähenda kogu vastutuse nihutamist üksikisikule, vaid selget ja realistlikku vastutuse jaotust inimese ja teenuseid osutavate organisatsioonide vahel. Lahendused peavad olema piisavalt lihtsad ja arusaadavad, et toetada laialdast kasutuselevõttu, vältides samas ebarealistlike ootusi kasutajate teadlikkuse või aktiivse sekkumise osas. Teisalt on oluline aga laiemalt mõista inimeste andmetega seonduvaid vastutusi ning selle piire, nt andmete kvaliteedi ja õigsuse tagamine, maandades andmete võltsimisega seotud riske.

Peamine järeldus

Turul puudub veel selge stiimul andmete jagamiseks, kuna loodav väärtus ei pruugi jaotuda õiglaselt ning riskid on kõrged. Samas kasvab nõudlus personaliseeritud ja proaktiivsete teenuste järele, mis loob surve uute lahenduste arendamiseks ja/või rakendamiseks. Intervjuueritavate sõnul on seega äri- ning ühiskondlikust keskkonnast tulenevad väljakutsed ja vajadused:

- *inimkesksete lahenduste realiseerimist mõjutav turuseis;*
- *inimeste andmete jagamiseks ning väärindamiseks sobiliku õigusliku ning haldusliku raamistiku tagamine;*
- *rahvusvahelise skaleeritavuse toetamine;*
- *innovatsiooniriski maandamine;*
- *majandusliku jätkusuutlikkuse tagamine; ning*
- *inimeste teadlikkuse, usalduse ning nõudluse tagamine.*

5. Võimekused ja eeldused inimkeskse andmemajanduse toetamiseks

Juba alates 2000ndatest aastatest on pakutud välja erinevaid (tehnoloogilisi) lahendusi inimese võimestamiseks temaga seotud andmete haldamisel, nagu VRM (*vendor-relationship-management*)⁵³, andmetrustid (*data trusts*)⁵⁴, operaatorid⁵⁵, andmevahendusteenused⁵⁶ jt. Samas on selge, et üksikud andmetaristu ning sellega seotud teenuste pakkujad ei suuda kõikehõlmavalt koondada inimesega seotud andmete ning teenuste ökosüsteemi. Selleks on vaja erinevaid osapooli, kes on kokku leppinud nii halduslikes kui usaldusküsimustes ning suudavad omavahel koostalitleda. Seetõttu tuleb andmeruumide (sh personaalsete andmeruumide) puhul arvestada nii ökosüsteemi võimaldavaid tehnilisi, ärilisi ja organisatoorseid komponente kui ka konkreetseid teenuseid ning nende kasutajaliideseid, mida ökosüsteemis osalevad tegutsejad (nii organisatsioonid kui inimesed) kasutavad ja otseselt kogevad.

Käesolev peatükk annab ülevaate ärilistest, õiguslikest, funktsionaalsetest ning tehnoloogilistest aspektidest, mida peetakse kirjanduse põhjal personaalse andmeruumi toimimiseks oluliseks. Kirjanduse põhjal kogutud teadmist on kõrvutatud uuringu jooksul tehtud intervjuude leidudega ning analüüsitud Eestis olemasoleva digitaristu kontekstis.

5.1 Ärilised aspektid, eeldused ja väljakutsed

Mistahes vabatahtliku andmepõhise koostöö üheks olulisemaks eelduseks on äriiline vajadus, motivatsioon ning sobiva äri- ning koostöömudeli rakendamine. Kuigi mitmel puhul toimub inimeste andmete jagamine ning väärindamine ka seadusega reguleeritud alustel (nt avalike ülesannete nagu tööhõive tagamine), siis käesolevas alapeatükis on fookuses just organisatsioonide ärilised ajendid andmete jagamiseks ning kasutamiseks. Sealjuures viitame andmekoostöömudeleid käsitlevatele ressurssidele, mida oleme osaliselt kasutanud personaalse andmeruumi kaasuste ärilises analüüsis (vt peatükk 8).

Andmeruumide Tugikeskuse projekti⁵⁷ raames on välja töötatud andmeruumi ärimudeli juhend⁵⁸, mis on mingil määral ülekantav ka personaalse andmeruumi raamistikule, eriti arvestades personaalset andmeruumi ümbritsevaid andmeökosüsteeme ja selle ärilisi

⁵³ ProjectVRM on üks varaseid Harvardi ülikooli teadus- ja arendusprojekte, mis oli inspireeritud CRM või kliendihaldustarkvarade lähenemisest, pakkudes välja alternatiivse viisi müüjate või tarnijate halduseks inimeste poolt. Vt lähemalt <https://projectvrn.org/about/> (külastatud 22.10.2025)

⁵⁴ Open Data Institute sõnul puudub andmetrustil selge definitsioon ning see võib viidata nii andmete haldus- kui avaliku järelevalve raamistikule, juriidilisele struktuurile, organisatsioonile või andmete hoiustamise viisile (vt lähemalt <https://theodi.org/insights/explainers/what-is-a-data-trust/> , külastatud 22.10.2025)

⁵⁵ Siin on peamiselt viidatud MyData operaatoritele kui inimkesket andmehaldust soosiva taristu pakkujaid (vt Langford et al 2022, kättesaadav aadressil <https://www.mydata.org/wp-content/uploads/2022/07/Understanding-MyData-Operators-2022-1.pdf>, külastatud 27.02.2026)

⁵⁶ EL liikmesriikide poolt tunnustatud andmevahendusteenused on loetletud aadressil <https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services> , külastatud 27.02.2026

⁵⁷ Vt lähemalt <https://dssc.eu> , külastatud 27.02.2026

⁵⁸ Vt juhendit aadressil <https://blueprint.dssc.eu/?pane=business&business=business-model>, külastatud 27.02.2026

loogikaid. Koostööl põhineva olemuse tõttu aitab ärimudeli juhend määratleda, kes mida teeb, kajastades andmeruumis osalejaid, teenusepakkujaid ja juhtimisorgani liikmeid. Kuigi juhend on lihtne, võivad selle täitmiseks vajalikud eeldused olla keerulised, mistõttu kaasnevad sellega ka mitmed täpsustavad küsimused. Ka Tarkade linnade ja kogukondade andmeruumi⁵⁹ raames on välja töötatud mitmeid osapooli kätkevate andmekoostööde valitsemise juhend⁶⁰, kus on välja toodud erinevad koostöömudelid ning nende osaks olevad ärimudelid. Antud loogikat kasutatakse ka personaalse andmeruumi kaasuste analüüsis. Koostöömudelite valik sõltub tuvastatud stiimulitest ning partnerite vahel eelistatud andmevahetusviisidest, kusjuures kasutusloos võivad olla rakendunud üks või mitu koostöömudelit.

Kuna üheks oluliseks ärivajaduseks on andmete killustatus ning kvaliteet, siis ühe olulise soodustava aspektina on ärilistest vaatest rõhutatud andmeoperaatorite ja/või andmevahendusteenuste⁶¹ olulisust, mis võiks toetada andmete koondamist ja vahendamist, et soodustada nende usaldusväärsust, turvalist ja õiguslikult kooskõlastatud kasutust andmetarbivate poolt. Ka antud uuringu käigus läbiviidud intervjuudes on esilekerkinud vajadus andmete koondamise ja vahendamise järgi, sealjuures pakkudes ka lisaväärtusena andmete kvaliteedi tagamist ning ärianalüütikat nt vastava sektori kohta. Sealjuures on ka antud potentsiaalsete vahendajate vaatest siiski väljakutseks andmete kättesaadavus. OECD on 2021. aasta uuringus⁶² toonud välja, et andmete ülekantavus (*data portability*) võib soodustada uute ärimudelite, sealhulgas andmevahendajate, tekkimist, kuid sealjuures on vastava õiguse rakendamine veel vähearenenud.

Peamine järeldus

Edu sõltub selgetest ärimudelitest ja -stiimulitest, mida praegu napib. Ilma majandusliku motivatsioonita ei teki andmeökosüsteemis piisavat osalust ega investeeringuid.

5.2 Õiguslikud aspektid, eeldused ja väljakutsed

Antud uuringus on õiguslikust vaatest võetud peamiseks fookuseks andmete töötlemise õigusliku aluse uurimine. Kaasuste vaatest muutub oluliseks ka muu õiguslik raamistik, mis reguleerib organisatsioonide ärikeskkonda.

⁵⁹ Tarkade linnade ja kogukondade andmeruumi projekti kohta saab lähemalt uurida aadressil <https://ds4sscc.eu>, külastatud 27.02.2026

⁶⁰ Multi-Stakeholder Governance Scheme, vt lähemalt aadressil https://static1.squarespace.com/static/63718ba2d90d0263d7fc1857/t/651ea670a884c256d84f4864/1696507511/589/DS4SSCC_D2.2+Multi-stakeholder+governance+scheme.docx.pdf, külastatud 27.02.2026

⁶¹ Euroopa Komisjoni ühine uuringute keskus JRC (European Commission Joint Research Centre) on 2023. aastal teinud ülevaate andmevahendajate (data intermediaries) erinevatest tüüpidest, tuues näiteid ka nende ärimudelitest, vt lähemalt <https://publications.jrc.ec.europa.eu/repository/handle/JRC133988>, külastatud 27.02.2026

⁶² Reimsbach-Kounatze, C., Molnar, A. (2024). The impact of data portability on user empowerment, innovation, and competition. Going Digital Toolkit Note, No. 25. OECD

Tulenevalt kehtivast õiguslikust EL-ülesest regulatsioonist on nii avalikus kui ka erasektoris isikuandmeid töödeldes vaja andmetöötlejal tagada õiguslik alus, millele andmeid töödeldes tuginetakse. Selleks võiksid potentsiaalselt sobida IKÜMi artikli 6 valimist potentsiaalselt nt nõusolek või lepinguline õiguslik alus (otsustuskoht hilisemateks etappideks, milline alus valida personaalse andmeruumi kontekstis).

Üldiselt eeldab avalikus sektoris isikuandmete töötlemine õiguslikku alust õigusakti tasandil (nt rahvastikuregistris toimuv isikuandmete töötlemine toimub rahvastikuregistri seaduses⁶³ reguleeritud alustel ning tervise infosüsteemis toimuv isikuandmete töötlemine on reguleeritud tervise infosüsteemi põhimäärusega⁶⁴). Seega, kui lähtuda kontseptsioonist või vaatenurgast, et andmesubjektile hakkab personaalse andmeruumi teenusena pakkuma avalik sektor, peaks selle ideega kaasas käima kehtiva õigusruumi täiendamine ning isikuandmete töötlemise õigusliku aluse ja eesmärgi koos muu seonduvaga ära kirjeldamine kehtivas siseriiklikus seadusandluses (seega oleks idee teostamiseks vajalik uue või muudetud seaduse vastuvõtmine). Kui isikuandmete töötlejaks oleks erasektor, oleks võimalik IKÜM art 6 vaates potentsiaalselt tugineda näiteks ka lepingulise või nõusoleku alusele ning teatavatel andmetöötlusjuhtudel ka näiteks õigustatud huvi õiguslikule alusele.

Nõusolek kui isikuandmete töötlemise õiguslik alus IKÜM art 6 lg 1 p a tähenduses ning tahteavaldusena antav heakskiit teenuse tarbimiseks siduva lepingu kontekstis on omavahel seotud, kuid eristatavat õiguslikult eristatavad tasandid. IKÜM art 6 lg 1 sätestab isikuandmete töötlemise kuus alternatiivset õiguslikku alust. Nende hulgas on punkt a kohaselt töötlemine seaduslik juhul, kui andmesubjekt on andnud nõusoleku oma isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil. Sealjuures on nõusoleku mõiste määratletud IKÜM art 4 p-s 11. Tegemist peab olema **vabatahtliku, konkreetse, teadliku ja ühemõttelise tahteavaldusega**, millega andmesubjekt kinnitab kas avalduse või selge kinnitava tegevusega (vaikimist ja tegevusetust kehtivaks nõusolekuks ei loeta), et ta nõustub teda puudutavate isikuandmete töötlemisega.

IKÜM-i **nõusolek on instrument**, mis legitimeerib andmetöötluse konkreetse eesmärgi suhtes, kui nõusolek on antud korrektselt ja **vastab IKÜM-is sätestatud tingimustele**. Esiteks peab nõusolek peab olema tagasivõetav igal ajal (IKÜM art 7 lg 3). Teiseks ei tohi nõusolek olla isikuandmete töötlemiseks eeltingimus teenusele, kui töötlemine ei ole teenuse osutamiseks vajalik (nn *conditionality* keeld). Kolmandaks peab nõusolek isikuandmete töötlemiseks olema eristatav muudest tahteavaldustest (nt lepingutingimustest). Seega ei ole nõusolek pelgalt formaalne „nõustumine“, vaid **rangete sisuliste kriteeriumidega õiguslik konstruktsioon**. Kui mõni kriteerium (nt vabatahtlikkus) puudub, ei saa nõusolek olla kehtiv isikuandmete töötlemise õiguslik alus.

Nõusolek on üks võimalikest õiguslikest alustest isikuandmete töötlemiseks (lisaks teistele IKÜM art 6 lg-s 1 toodud õiguslikele alustele) personaalse andmeruumi kontekstis. See ei ole eelistatud, parim ega „turvalisim“ alus, vaid sobiv vaid siis, kui:

1. andmesubjektil on tegelik valikuvabadus;
2. töötlemine ei ole vältimatult vajalik lepingu täitmiseks või seadusest tuleneva kohustuse täitmiseks (kui personaalne andmeruumi teenuse pakkumine otsustatakse

⁶³ Rahvastikuregistri seadus, <https://www.riigiteataja.ee/akt/118102024004>, külastatud 29.10.2025

⁶⁴ Tervise infosüsteemi põhimäärus, <https://www.riigiteataja.ee/akt/105042023019?leiaKehtiv>, külastatud 29.10.2025

tulevikus siduda lepingulise suhtega ja teatav andmetöötlus on vajalik lepingu täitmiseks, tuleks valida õiguslikuks aluseks lepingu täitmise õiguslik alus (IKÜM art 6(1)b)).

Teenuse tarbimiseks antav heakskiit on klassikaline tsiviilõiguslik **tahteavaldus**, millega inimene nõustub sõlmima lepingu või aktsepteerib teenuse osutamise tingimusi. See tahteavaldus loob lepingulise õigussuhte, millest tulenevad vastastikused õigused ja kohustused (nt tasu maksmine, kui teenus on tasuline, ja teenuse osutamine). Kui teenuse osutamine eeldab teatud isikuandmete töötlemist, on töötlemise õiguslikuks aluseks tavaliselt IKÜM art 6 lg 1 p b – töötlemine on vajalik lepingu täitmiseks. Sellisel juhul ei ole isikuandmete töötlemise vaatest vaja ega kohane tugineda nõusolekule art 6 lg 1 p a alusel. Lepingutäitmiseks vajalik töötlemine ei sõltu andmesubjekti nõusoleku püsimisest, vaid lepingu olemasolust ja täitmisvajadusest.

Nõusoleku isikuandmete töötlemiseks (1) ja teenusega liitumise heakskiidu tahteavalduse (2) segamini ajamine võib viia järgmiste probleemideni:

- **Vabatahtlikkuse defitsiit** – kui teenuse saamine seatakse sõltuvusse nõusolekust andmetöötluseks, mis ei ole teenuse osutamiseks vajalik, võib nõusolek olla kehtetu.
- **Õigusliku aluse ekslik valik** – lepingulise vajaduse olukorras nõusolekule tugineda muudab töötlemise ebastabiilseks, sest nõusoleku saab igal ajal tagasi võtta. Sellega kaasneb aga vastutavale töötlejale kohustus isikuandmete töötlemine sellele alusele tuginedes lõpetada.
- **Tagasivõtmise tagajärjed** – nõusoleku tagasivõtmine ei lõpeta automaatselt lepingut, kuid kui andmetöötlus oli ekslikult rajatud nõusolekule, võib see muuta lepingu täitmise võimatuks.
- **Osapoolte õiguste (sh IKÜM-ist tulenevate andmesubjekti õiguste), kohustuste ja vastutuse määratlemine** ja nendes teemades personaalse andmeruumi vaatest selle kasutajatele läbipaistval viisil teabe avaldamine ja kommunikeerimine tulenevalt IKÜM artiklist 5.

Vastutav ja volitatud töötleja ning kolmandate seonduvate osapoolte täpsem rollijaotus, õigused, kohustused ning vastutus olenevad sellest, kuidas personaalne andmeruum detailsemalt üles ehitatakse. Praktikas võib vastutav töötleja olla nt personaalse andmeruumi veebilehe omanik ja teenusepakkuja kui tellija leiab, et see on sobivaim formaat personaalse andmeruumi pakkumiseks.

Vastutava töötleja puhul tuleb lähtuda IKÜM art 4 p-s 7 toodud definitsioonist, mille kohaselt vastutav töötleja on füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid; kui sellise töötlemise eesmärgid ja vahendid on kindlaks määratud liidu või liikmesriigi õigusega, võib vastutava töötleja või tema määramise konkreetsed kriteeriumid sätestada liidu või liikmesriigi õiguses. Lisaks tuleb arvestada IKÜM art 4 p-s 8 toodud volitatud töötleja definitsiooniga, mille kohaselt volitatud töötleja on füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.

Ühtlasi on oluline välja tuua, et personaalne andmeruum peab olema üles ehitatud **suveräänsuse põhimõttel**, mis tähendab, et andmesubjektil (ja andmevaldajal, personaalse andmeruumi ökosüsteemi pakkujal, vastutaval töötlejal ja volitatud töötlejal) peab säilima kontroll andmete üle ka siis, kui need on jagatud (andmesubjekti heakskiidul). See nõuab

lõimitud andmekaitse (*privacy by design*) lähenemist, kus õiguslikud ja tehnilised piirangud on süsteemi sisse ehitatud.

IKÜM artikkel 25 kohaselt peab⁶⁵ vastutav töötleja rakendama nii töötlemisvahendite kindlaksmääramisel kui ka isikuandmete töötlemise ajal asjakohaseid tehnilisi ja korralduslikke meetmeid, nagu pseudonümiseerimine või võimalikult väheste andmete kogumine, et tagada isikuandmete töötlemisel lõimitud ja vaikimisi andmekaitset ning kaitsta andmesubjektide õigusi. Sealjuures on vastutav töötleja kohustatud rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, millega tagatakse, et vaikimisi töödeldakse ainult isikuandmeid, mis on vajalikud töötlemise konkreetse eesmärgi saavutamiseks (IKÜM art 25 lg 2). See kehtib kogutud isikuandmete hulga, nende töötlemise ulatuse, nende säilitamise aja ja nende kättesaadavuse suhtes. Nende meetmetega tagatakse eelkõige see, et isikuandmeid ei tehta vaikimisi ilma asjaomase isiku sekkumiseta määramata füüsiliste isikute ringile kättesaadavaks.

Lisaks on õiguslikust aspektist lähtuvalt oluline, et enne personaalse andmeruumi looma hakkamist oleksid kõigile personaalse andmeruumi osapooltele üheselt arusaadav, millised on õiguslikult siduvad nõuded (lepingu või õigusakti tasandil), mis määravad, kuidas andmetele juurde pääseda, neid töödelda ja kasutada. Lisaks tuleks kõigi andmeruumi osapoolte vahel tuleb sõlmida siduvad lepingud, mis määravad vastutuse ja reeglid (sh lepingu lõpetamise tingimused).

Väljakutsed ja otsustuskohad

Õigusliku taustaraamistiku analüüsi vaates on **isikuandmete teisele kasutusele** (*further processing, reuse*) temaatika olulise tähtsusega, kuna andmeruumide üks eesmärk on andmete taaskasutus, kuid õiguslikult aspektist vajab otsustamist, kas algne andmete kogumise eesmärk vastab teisele kasutusele või luua teiseks kasutuseks õigusakti tasandil selge õiguslik alus. Samuti saab siinkohal võrdlusmaterjalina välja tuua Euroopa andmekaitseinspektori (EDPS) seisukoha⁶⁶, et tulevases õigusaktis tuleks kindlaks määrata isikuandmete edasise töötlemise eritingimused ja luua mehhanismid, mis võimaldaks tagada, et teiseks kasutamiseks kättesaadavaks tehtud andmeid ei koguta ebaseaduslikult ega kasutata eesmärkidel, mida algselt ei ole ette nähtud, mis on ebaseaduslikud või millel puudub piisav õiguslik alus. Ühtlasi on rõhutatud läbipaistvuse olulisust. Seda kõike peaks silmas pidama ka Eesti seadusandja personaalse andmeruumi õigusliku regulatsiooni planeerimise kontekstis.

Lisaks IKÜM art 6 lg-le 4 on IKÜM põhjenduspunktis 50 lauses 1 konstateeritud, et isikuandmete töötlemine muudel eesmärkidel kui need, milleks isikuandmed algselt koguti, on lubatud üksnes juhul, kui töötlemine on kooskõlas eesmärkidega, mille jaoks isikuandmed algselt koguti. Samas lisatakse IKÜM põhjenduspunktis, et selleks, et teha kindlaks, kas edasise töötlemise eesmärk vastab eesmärgile, mille jaoks isikuandmed algselt koguti, peaks vastutav töötleja võtma pärast kõikide esialgse töötlemise seaduslikkuse seisukohast vajalike nõuete täitmist muu hulgas arvesse mis tahes seoseid sellise eesmärgi ja kavandatava edasise töötlemise eesmärgi vahel, isikuandmete kogumise konteksti, eelkõige andmesubjekti

⁶⁵ Määrus nendib, et vastutav töötleja peab andmekaitse meetmete rakendamisel võtma arvesse teaduse ja tehnoloogia viimast arengut ja rakendamise kulusid ning töötlemise laadi, ulatust, konteksti ja eesmarke, samuti töötlemisest tulenevaid füüsiliste isikute õigusi ja vabadusi ähvardavaid erineva tõenäosuse ja suurusega ohte.

⁶⁶ "Preliminary Opinion 8/2020 on the European Health Data Space" punkt 19

ja vastutava töötleja vahelisel suhtel põhinevaid andmesubjekti mõistlikke ootusi andmete edasise kasutamise suhtes, isikuandmete laadi, kavandatava edasise töötlemise tagajärgi andmesubjekti jaoks ning asjakohaste kaitsemeetmete olemasolu nii esialgsetes kui ka kavandatavates edasistes isikuandmete töötlemise toimingutes. Seega tuleb isikuandmete töötlemist muudel eesmärkidel kui need, milleks isikuandmed algselt koguti, läbi viia hindamine, kas teise kasutuse eesmärk on esialgsega kooskõlas. Avaliku sektori andmetöötluses on oluline arvestada sellega, et seadusandja peab õigusakti tasandil määrama isikuandmete töötlemise eesmärgiga kindlaks isikuandmete lubatava töötlemise raadiuse. Ka isikuandmete esialgsest erineval eesmärgil töötlemise raadius tuleb kindlaks määrata seaduse tasemel.⁶⁷

Eriliiki isikuandmete töötlemist personaalse andmeruumi ökosüsteemis saab vaadelda IKÜM art 9 kontekstis, mis näeb ette rangemad standardid eriliiki isikuandmete töötlemisele. IKÜM art 9 lg 1 kohaselt on keelatud töödelda isikuandmeid, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilisi andmeid, füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid, terviseandmeid või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. IKÜM art 9 lõiget 1 ei kohaldata, kui esineb mõni IKÜM art 9 lg 2 asjaoludest (nt IKÜM art 9 lg 2 p b kohaselt ei kohaldata eriliiki isikuandmete töötlemise keeldu, kui töötlemine on vajalik seoses vastutava töötleja või andmesubjekti tööõigusest ning sotsiaalkindlustuse ja sotsiaalkaitse valdkonna õigusest tulenevate kohustuste ja eriõigustega niivõrd, kuivõrd see on lubatud liidu või liikmesriigi õigusega või liikmesriigi õiguse kohase kollektiivlepinguga, millega kehtestatakse asjakohased kaitsemeetmed andmesubjekti põhiõiguste ja huvide kaitseks).

Tehniliste ja organisatoorsete kaitsemeetmete rakendamine, sh nn “lävendi” kehtestamine, millistele tingimustele peab osapool vastama, et pääseda personaalse andmeruumi ökosüsteemi osapooleks andmete edastaja või andmepärijana. Näiteks suuremahulise andmetöötluste puhul on vajalik hinnata, kas organisatsioon on rakendanud E-ITS või ISO27001 turbestandardeid, määranud infoturbejuhi või andmekaitse spetsialisti või kas ökosüsteemiga liituda soovival osapoolel on eelnevaid tõsisemaid infoturbe ja/või andmekaitsealaseid intsidente esinenud suurel määral ja või ettevaatamatusest või lohkusest.⁶⁸

Peamine järeldus

Isikuandmete töötlemise puhul on esmatähtis õigusliku aluse tagamine, milleks personaalse andmeruumi puhul on huvipakkuvamaks nii nõusoleku isikuandmete töötlemiseks (1) kui ka teenusega liitumise heakskiidu tahteavaldus. Samas on selle õiguslik tõlgendus ning laialdane rakendamine veel keeruline. Regulaatiivne ebakindlus võib pidurdada innovatsiooni rohkem kui seda soodustada.

⁶⁷ M. Mikiver. Isikuandmeid riskasutav e-riik ja seadusereservatsioon. Kas efektiivsus tõrjub põhiseaduslikud nõuded? – Riigiõiguse aastaraamat 4/2023, lk 54–92; lk 92.

⁶⁸ vt lähemalt <https://www.aepd.es/documento/approach-to-data-spaces-from-gdpr-perspective.pdf>, https://www.edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-82020-european-health-data-space_en ja https://www.edpb.europa.eu/our-work-tools/our-documents/edpb-edps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en, külastatud 23.03.2026

5.3 Funktsionaalsed võimekused

Erinevate andmeruumide ning inimeste andmete põhiste ökosüsteemide käsitluste (sh IDSA referentsarhitektuuri, Gaia-X, MyData mudeli ja ELi õigusraamistiku) analüüs näitab, et erinevad raamistikud rõhutavad eri mõõtmeid, sealhulgas rollijaotust, tehnilisi komponente, föderatiivset usaldust ja regulatiivseid kohustusi, kuid ei sünteesi neid ühtseks inimese juhitaavaks andmekasutuse loogikaks. Eesti konteksti analüüs ja ekspertintervjuud kinnitavad, et personaalse andmeruumi lahendus võiks tugineda hajusale andmehaldus mudelile, olemasoleva identiteeditaristu maksimaalsele kasutamisele ning selgelt eristatud nõusoleku, andmevahenduse ja auditeeritavuse funktsioonidele. Keskse andmelao loomist ei peeta seejuures soovitaavaks.

Sellest tulenevalt on käesolevas töös sünteesitud personaalse andmeruumi funktsionaalsed võimekused, mis on rühmitatud loogilisteks funktsionaalseteks kategooriateks. Võimekuste sünteesi alusena on kasutatud kirjanduse leide, sh isikuandmete turuplatsi taksonoomiat (Scheider et al., 2023), inimkesksete B2C-andmeökosüsteemide referentssüsteemi (Scheider et al., 2023) ja MyData operaatorite referentsmudelit (Langford et al., 2022), samuti Euroopa Komisjoni poolt läbiviidud SEMIC töötubade materjale (Euroopa Komisjon, 2022).

Võimekuste sünteesis joonistuvad välja kolm põhikategooriat:

1. kontrolli ja läbipaistvuse teenused,
2. andmevahetust võimaldavad ja toetavad teenused ning
3. lisaväärtusteenused.

Sealjuures on iga kategooria raames esitatud kohustuslikke võimekusi, mis moodustavad inimese juhitud andmekasutuse tuuma, ning valikulisi võimekusi, mille rakendamise vajadus sõltub teenuse ärimudelist ja ökosüsteemi küpsusest. Järgnevalt kirjeldatakse, milliseid suutlikkusi peab personaalne andmeruum võimaldama inimese juhitud andmekasutuse tagamiseks, enne kui käsitletakse nende funktsioonide tehnilist realiseerimist rakendusarhitektuuri tasandil.

5.3.1 Kontrolli ja läbipaistvust võimaldavad teenused

Kontrolli ja läbipaistvust võimaldavad teenused moodustavad personaalse andmeruumi funktsionaalse tuuma, kuna need loovad eelduse inimese juhitud andmekasutuseks. Nende võimekuste kaudu saab inimene ehk andmesubjekt teostada teadlikku ja suveräänset kontrolli oma andmete jagamise ning töötlemise üle ning omada selget ülevaadet andmete kasutamisest ajas.

Kontroll ei piirdu üksnes nõusoleku andmisega, vaid hõlmab ka õiguste dünaamilist haldamist, kasutuse tingimuste muutmist ning võimalust hinnata varasemate andmekasutuste vastavust inimese tahte ja kehtivatele reeglitele. Läbipaistvus omakorda eeldab, et kõik olulised tegevused on jälgitavad, rekonstrueeritavad ja arusaadaval kujul esitatavad. Samal ajal arvestatakse ka andmevaldajate ja andmetarbijate vajadustega, pakkudes neile struktureeritud liideseid andmete pärimiseks ning ligipääsu haldamiseks kooskõlas kehtivate õiguste ja poliitikatega.

Kohustuslikud võimekused

Personaalse andmeruumi toimimiseks on vältimatult vajalikud järgmised võimekused:

- **Õiguste haldamine**, sealhulgas autoriseerimine, juurdepääsu kontroll ja nõusolekuteenused, mis võimaldavad siduda konkreetse andmekasutuse inimese tahte ja kehtivate tingimustega.
- **Tegevuste logimine ja auditeerimise tugi**, mis tagab andmekasutuse jälgitavuse, tõendatavuse ning võimaldab hilisemat vastavuse hindamist.
- **Inimesele suunatud kasutajaliidesed**, mille kaudu on võimalik suveräänselt hallata nõusolekuid, jälgida andmekasutust ja vajadusel sekkuda.
- **Andmepakkujatele ja -tarbijatele suunatud kasutaja- või teenusliidesed**, mille kaudu saab esitada päringuid ning hallata ligipääsu kooskõlas kehtestatud õiguste ja poliitikatega.

Need võimekused moodustavad inimese juhitud andmekasutuse miinimumraamistiku ning nende puudumisel ei ole võimalik tagada ei sisulist kontrolli ega usaldusväärset läbipaistvust.

Valikulised võimekused

- **Andmete hoiustamine inimese poolt**, näiteks personaalse andmekukru või muu personaalse andmehoidla kaudu, mis võimaldab suurendada individuaalset kontrolli andmete üle.

5.3.2 Andmevahetust võimaldavad ja toetavad teenused

Andmevahetust võimaldavad ja toetavad teenused loovad funktsionaalse aluse sellele, kuidas andmevahetus tehniliselt ja organisatsiooniliselt võimalikuks tehakse ning kuidas tagatakse selle usaldusväärsus. Need võimekused võimaldavad osapoolte turvalist tuvastamist, andmepakkujate ja andmetarbijate üksteise leidmist ning reeglite automaatset rakendumist andmevahetuse hetkel. Andmevahetus ei toimu üksnes tehnilise ühenduvuse kaudu, vaid eeldab usaldusraamistike, poliitikate ja koostalitlusmehhanismide koostoimet.

Kohustuslikud võimekused

Personaalse andmeruumi toimimiseks on vältimatult vajalikud järgmised võimekused:

- **Identiteedihaldus ja autentimine**, mis võimaldavad osapoolte usaldusväärset tuvastamist ning seovad andmepäringud kontrollitava identiteedikontekstiga. See võib tugineda riiklikele või organisatsioonilistele eID-lahendustele ning olemasolevatele autentimistaristutele.
- **Andmepakkujate ja andmetarbijate kokkutoomine ja avastamine**, sealhulgas kasutusjuhtude kureerimine ja teenuste kirjeldamine, et võimaldada struktureeritud andmevahetust ning andmete teisesel kasutamisel põhinevate teenuste kujunemist.
- **Poliitikate ja usaldusreeglite tehniline valideerimine ja jõustamine**, mis tagab, et kehtestatud õigused, piirangud ja kasutustingimused rakenduvad automaatselt andmevahetuse hetkel ning ei sõltu käsitsi kontrollist.

Valikulised võimekused

- **Andmevahetuse realiseerimisviisi valik**, sealhulgas olemasolevatele riiklikele või sektoripõhistele lahendustele tuginemine (nt X-tee infrastruktuuri kasutamine) või eraldi andmevahenduskihi loomine personaalse andmeruumi koosseisus.
- **Andmete ja andmemudelite harmoniseerimine ning andmekvaliteedi tagamine**, mis toetab koostalitlusvõimet ja vähendab semantilisi vastuolusid andmevahetuses.
- **Usaldus- ja haldusraamistike kujundamine ja haldamine**, mis kuulub määratleb andmevahetuse põhimõtted, vastutuse ja osalemistingimused.

Oluline on eristada usaldus- ja haldusraamistiku kujundamist kui juhtimistasandi funktsiooni ning selle tehnilist valideerimist ja jõustamist kui rakenduslikku funktsiooni. Esimene määratleb reeglid ja vastutuse, teine tagab nende automaatse ja järjepideva rakendumise süsteemi tasandil.

5.3.3 Lisaväärtusteenused

Lisaväärtusteenused hõlmavad võimekusi, mis on seotud andmete väärindamise ja väärtusloomega. Kui kontrolli ja andmevahetust võimaldavad teenused loovad personaalse andmeruumi toimimise eelduse, siis lisaväärtusteenused kujundavad selle põhjal tekkiva praktilise kasu nii lõppkasutajatele kui ka andmetarbijatele.

Siinkohal on oluline eristada personaalse andmeruumi kontseptuaalset raamistikku ning konkreetset personaalse andmeruumi teenust. Kontseptuaalne raamistik määratleb põhimõtted ja funktsionaalse tuuma, mis võimaldab inimese poolt juhitud andmete kasutust. Konkreetne teenusepakkuja võib sellele raamistikule tuginedes kujundada oma väärtuspakkumise, mis võib, kuid ei pea sisaldama andmete väärindamise või monetiseerimisega seotud teenuseid. Seega ei ole lisaväärtusteenused personaalse andmeruumi toimimise eeltingimus, kuid need võivad oluliselt mõjutada ökosüsteemi atraktiivsust, kasutuselevõttu ja majanduslikku kestlikkust.

Valikulised võimekused

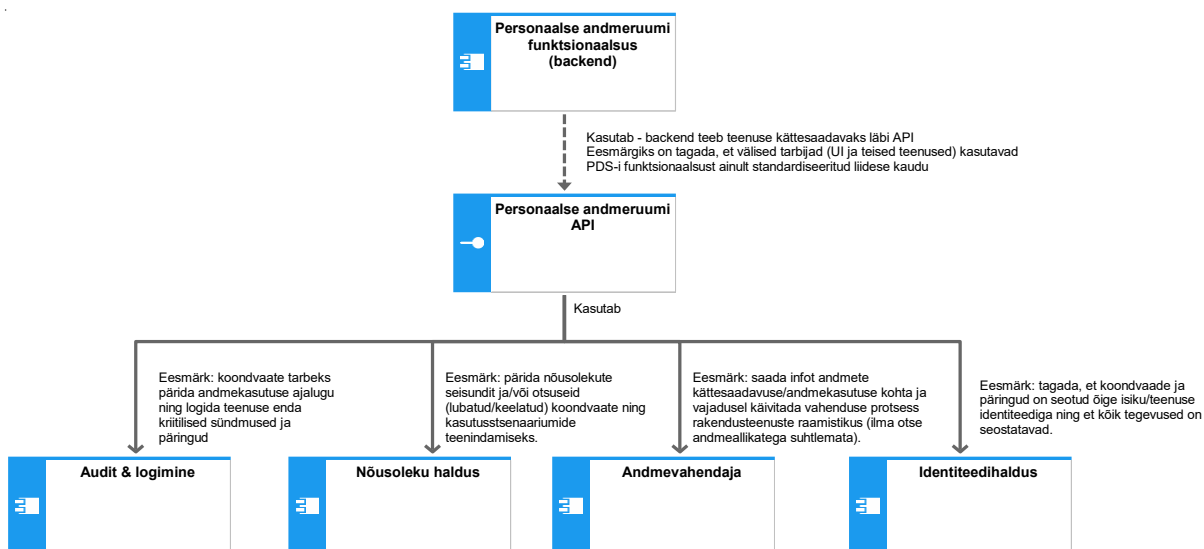
- **Andmete visualiseerimine**, mis võimaldab esitada inimesega seotud andmeid arusaadaval ja konteksti spetsiifilisel kujul, toetades teadlikku otsustamist.
- Inimesega seotud andmete põhjal toimivad **tehisintellekti teenused**, sealhulgas personaalsed analüütilised või soovituspõhised lahendused, mis kasutavad andmeid inimese huvides.
- **Andmetoodete defineerimine ja portfoolio haldus** inimese poolt, võimaldades struktureerida ja kirjeldada oma andmekogumeid ning määratleda nende kasutustingimusi.
- **Väärtusloome haldus**, sealhulgas väärtuse sidumine ja vahetamine nii rahalises kui ka mitterahalises vormis, mis võib hõlmata andmete jagamise eest saadavaid hüvesid või teenuseid.

Peamine järeldus

Personaalse andmeruumi tuum koosneb kolmest võimekuste grupist: **kontroll ja läbipaistvus, andmevahetus ning lisaväärtusloome**. Ilma esimese kategooriata (kontroll ja läbipaistvus) ei teki usaldust, samas kui ilma lisaväärtusteenusteta jääb kasu piiratuks.

5.4 Tehnoloogilised komponendid ja nende rakendusarhitektuur

Eelnevalt kirjeldatud funktsionaalsed rühmad on rakendusarhitektuuri tasandil tõlgendatud selgelt piiritletud rakenduskomponentideks, mille ülesehitus ja vastutusjaotus tulenevad inimese poolt juhitud andmekasutuse põhimõtetest.



Joonis 6. Personaalse andmeruumi rakendusarhitektuuri tuum ja komponendid

5.4.1 Identiteedihalduse komponent

Identiteedihalduse komponent realiseerib identiteedikonteksti haldamise funktsionaalsuse, tagades, et iga personaalses andmeruumis algatatud päring on seotud krüptograafiliselt valideeritava ja masinloetava identiteedikontekstiga. Komponent ei teosta autentimist ise, vaid tugineb olemasolevatele usaldusraamistikele ja identiteediteenustele.

Autentimise tulemusena väljastatakse turvamärgend, mis sisaldab identiteedi, rolli ja kehtivusega seotud atribuute ning võimaldab päringut kontekstuaalselt valideerida. Identiteedikontekst edastatakse päringu osana, järgides olekuta arhitektuurimudelit, kus keskset seansihaldust ei kasutata. Komponent valideerib saabunud turvamärgendite kehtivuse ja allkirja ning normaliseerib identiteedikonteksti sisemiselt kasutatavasse formaati.

See ei tee andmekasutuse lubatavusotsuseid ega vahenda andmeid, vaid tagab usaldusväärse identiteedialuse teistele tuumakomponentidele.

Föderatiivne tugi võimaldab kasutada mitut identiteedipakkujat eeldusel, et need vastavad kokkulepitud usaldus- ja sertifitseerimismõuetele.

5.4.2 Nõusoleku halduse komponent

Nõusoleku halduse komponent realiseerib andmekasutuse lubatavuse hindamise funktsionaalsuse, toimides poliitikapõhise otsustusmootorina. Selle ülesanne on hinnata iga andmepäringu lubatavust päringu hetkel, arvestades identiteedikonteksti, kasutuseesmärki, taotletavate andmete ulatust ning kehtivaid nõusoleku- ja poliitikareegleid.

Komponent on arhitektuuriliselt eraldatud andmeedastuse loogikast ning genereerib masinloetava otsuse, mille jõustamine toimub eraldi komponendis. Nõusolekud talletatakse struktureeritud kujul, võimaldades atribuudi- ja reeglipõhist hindamist, kus iga kirje seob inimese identiteedi, andmekategooria, kasutuseesmärgi, adressaadi ja kehtivusparameetrid.

Otsus tagastatakse lubava, keelava või tingimusliku vastusena ning see on seotud auditiga seostatava otsuseidentifikaatoriga. Nõusoleku muutmine või tühistamine mõjutab järgnevaid päringuid koheselt, vältides püsivate ligipääsuõiguste kasutamist.

5.4.3 Andmevahenduse komponent

Andmevahenduse komponent realiseerib andmevahetuse täitmise ja jõustamise funktsionaalsuse, vahendades andmepäringuid andmetarbijate ja andmevaldajate süsteemide vahel ning tagades, et andmeid edastatakse üksnes lubava otsuse olemasolul. Iga päringut käsitletakse eraldiseisva tehingulise sündmusena, mille täitmine eeldab identiteedikonteksti valideerimist ja lubatavuse kontrolli. Lubava otsuse korral edastatakse päring algallikasse ning vahendatakse vastus kokkulepitud formaadis.

Komponent ei sisalda otsustusloogikat ega halda nõusolekuid, vaid jõustab tehtud otsuse. Personaalse andmeruumi tuumas ei talletata algandmeid püsivalt; andmeedastus on päringupõhine ja piiritletud minimaalse vajaliku andmehulgaga. Kõik päringud seotakse korrelatsiooniidentifikaatori kaudu auditiga, tagades andmevahetuse jälgitavuse.

5.4.4 Auditi ja logimise komponent

Auditi ja logimise komponent realiseerib jälgitavuse ja tõendatavuse funktsionaalsuse, kogudes ja säilitades personaalses andmeruumis toimuvad kriitilised sündmused viisil, mis võimaldab hilisemat rekonstrueerimist, vastavuse tõendamist ja järelevalvet. Kõiki olulisi tegevusi, sealhulgas päringu algatamist, identiteedikonteksti valideerimist, lubatavusotsuse tegemist, andmete edastamist ning nõusolekute muutmist, käsitletakse struktureeritud sündmustena. Iga sündmus seotakse ajamärgise, korrelatsiooniidentifikaatori, osapoolte identiteedikonteksti ning rakendatud poliitika või otsuse viitega, võimaldades taastada konkreetse andmekasutuse täieliku elutsükli.

Korrelatsiooniidentifikaatorite kasutamine tagab, et eri komponentidest pärinevad sündmused moodustavad ühtse loogilise sündmusahela ilma algandmete dubleerimiseta. Auditilogid ei

sisalda andmete sisu, vaid üksnes otsuste ja tegevuste metaandmeid, järgides minimaalsuse ja andmekaitse põhimõtteid.

Logide tervikluse ja ajalisuse usaldusväärsuse tagamiseks rakendatakse mehhanisme, mis võimaldavad tuvastada hilisemaid muutmiskatseid. Seeläbi kujuneb süsteemis tõenduslik sündmusahel, mis toetab vastavuse hindamist ning usalduse kujunemist personaalse andmeruumi toimimise suhtes.

5.4.5 Personaalse andmeruumi vaate rakendusteenus

Personaalse andmeruumi vaadete rakendusteenus realiseerib läbipaistvuse ja ülevaate funktsionaalsuse, pakkudes inimesele ja teenustele ühtset loogilist ligipääsupunkti inimesega seotud andmekasutuse teabele. Tegemist ei ole andmehoidla ega otsustuskomponendiga, vaid koondamis- ja esituskihiga, mis kasutab tuumakomponentide poolt pakutavaid teenuseid. Sealjuures ei tee see komponent iseseisvaid lubatavusotsuseid ega vahenda algandmeid, vaid esitab süsteemi toimimise kohta koondatud ja arusaadava vaate.

Tehniliselt toimib vaate rakendusteenus API-põhise olekuta teenusena, koondades identiteedikonteksti, nõusolekute seisundi ja auditisündmused päringupõhiselt ühtseks vastuseks. Ligipääs teenusele toimub standardsete autentimis- ja autoriseerimismehhanismide kaudu, kasutades turvamärgendeid, mis seovad päringu konkreetse isiku või teenusega ning piiravad kuvatava info rolli- ja kontekstipõhiselt. Sama liidest saab kasutada nii inimesele suunatud kasutajaliidese kui ka masintarbijate poolt, tagades ühtse ligipääsumudeli.

Selline arhitektuur võimaldab esituskihil tehnilist evolutsiooni (nt erinevad kasutajaliidesed või integratsioonid) ilma, et see mõjutaks tuumakomponentide sisemist loogikat või vastutusjaotust.

5.4.6 Komponentide koostöömudel ja päringu tüüpiline elutsükkel

Personaalse andmeruumi rakendusarhitektuur põhineb selgelt eristatud, kuid loogiliselt seotud komponentide koostöömudelil. Iga komponent täidab piiritletud rolli ning suhtleb teiste komponentidega üksnes määratletud teenuste ja liideste kaudu. Arhitektuuri keskne põhimõte on otsustamise, täitmise ja tõendamise eristamine, mis välistab liigse funktsioonide kattuvuse ja vähendab süsteemset riski.

Komponentide koostöö realiseerub tüüpilise andmepäringu elutsükli järgmiste sammudena:

1. **Päringu algatamine** – inimene või teenus algatab andmepäringu kasutajaliidese või API kaudu. Päringule omistatakse unikaalne identifikaator.
2. **Identiteedikonteksti valideerimine** – identiteedihalduse komponent valideerib päringuga kaasas oleva turvamärgendi ning seob päringu usaldusväärse identiteedi ja rollikontekstiga.
3. **Lubatavuse hindamine** – nõusoleku halduse komponent hindab päringu konteksti poliitikate ja kehtivate nõusolekute alusel ning tagastab masinloetava otsuse.
4. **Otsuse jõustamine ja andmete vahendamine** – lubava otsuse korral andmevahenduse komponent edastab päringu algallikasse ning vahendab vastuse andmetarbijale, järgides määratletud ulatus- ja eesmärgipiiranguid.

5. **Sündmuste talletamine** – kõik päringu elutsükli jooksul toimunud tegevused seotakse korrelatsiooniidentifikaatori kaudu ning talletatakse auditi ja logimise komponendis.
6. **Ülevaate võimaldamine** – vaate rakendusteenus võimaldab hiljem päringu kulgemise ja tulemuse koondvaadet, sidudes identiteedikonteksti, lubatavusotsuse ja andmeedastuse sündmused.

Kirjeldatud elutsükkel ei ole jäik protsessiskeem, vaid arhitektuurne koostöömuster, mida saab rakendada erinevates kasutusjuhtudes ja tehnilistes konfiguratsioonides. Selline modulaarne ja sündmuspõhine lähenemine toetab skaleeritavust ja föderatiivset koostalitlust.

6. Rollimudel

Käesolevas peatükis kirjeldatakse personaalse andmeruumi kui kontseptuaalse raamistiku rollimudelit, mis määratleb osapoolte vastutused ja suhted inimeste kohta käivate andmete vahetuse ja väärimise protsessis. Rollimudel (vt Joonis 7) on kujundatud Euroopa andmetaristu raamistike (sh ELi ühiste andmeruumide juhiste⁶⁹, ELi regulatsioonide nagu andmehaldusmäärus ja eIDAS, MyData⁷⁰, Gaia-X⁷¹) analüüsi ning Eesti toimivate praktikate analüüsi põhjal.

Mudel ei kirjelda olemasolevat valmis teenust, vaid normatiivset ja arhitektuurilist sihtmudelit, mis ühendab föderatiivse juhtimisloogika ja inimkeskse andmesuveräänsuse põhimõtted. See struktureerib Eesti praktikas hajusalt realiseeruvad personaalse andmeruumi funktsioonid selgelt määratletud rollide ja vastutuste kaudu ühtseks arhitektuuriliseks referentsraamistikuks.

Lisaks tuleb nentida, et laiapindsemad personaalse andmeruumi teenused toimivad föderatiivses usaldusraamistikus, suhestudes nii andmevahetuses otseselt osalevate rollide kui ka andmeruumi haldus- ja järelevalvefunktsioonidega. Andmeruumi rollid on jaotatavad kolme kategooriasse: otseselt andmevahetuses osalevad rollid, andmevahendust toetavad rollid ja andmeruumi kui terviku haldamise eest vastutavad rollid.

6.1 Otseselt andmevahetuses osalevad rollid

Andmevahetuses otseselt osalevad osapooled, kes loovad, vahetavad või kasutavad andmeid andmeruumi kaudu. Sealjuures võivad nad **kanda ühte või mitut järgmist rolli**:

1. **Andmesubjekt** on IKÜMi kohaselt füüsiline isik, kelle isikuandmeid läbi personaalse andmeruumi raamistikus töödeldakse. Sealjuures on personaalse andmeruumi puhul andmesubjektil aktiivne roll oma andmete jagamisel ning väärimisel, kui talle on tagatud praktilised võimekused kontrollida oma andmete liikumist nt nõusolekute halduse, tahteavalduse määratlemise vm kaudu. Funktsionaalsetest võimekustest vt lähemalt ptk 5.3.
2. **Andmeomanik** on osapool, kellel on suveräänne õigus temale kuuluvate andmete osas otsuseid teha, sh pakkuda neid kolmandatele osapooltele ning määrata nendele ligipääsu ja kasutamise tingimused. Üldjuhul on isikuandmete kontekstis andmete omanikuks füüsiline isik, kelle kohta need käivad (ehk IKÜMi poolt määratletud andmesubjekt). Mõningal juhul võib andmete õiguslik staatus olla keerukas, nt inimeste poolt kasutatavate IoT-seadmete andmete puhul, kus andmete üle võib olla tehniline kontroll seadme tootjal, kuid kasutajal on õigus andmetele ligi pääseda ja neid kasutada.
 - a. Andmeomaniku funktsionaalse alamrollina tuleb käsitleda ka **andmepakkujat**. Sellest hetkest, kui andmeomanik teeb andmed andmetarbijatele

⁶⁹ Vt lähemalt Andmeruumide Tugikeskuse juhiste aadressil <https://blueprint.dssc.eu/>, külastatud 27.02.2026

⁷⁰ MyData operaatorite valge paber, kättesaadav aadressil <https://www.mydata.org/wp-content/uploads/2022/07/Understanding-MyData-Operators-2022-1.pdf>, külastatud 27.02.2026

⁷¹ Gaia-X Architecture Document, kättesaadav aadressil <https://docs.gaia-x.eu/technical-committee/architecture-document/25.11/gaia-x-context/>, külastatud 27.02.2026

kättesaadavaks vastavalt andmesubjekti ja/või andmeomaniku poolt kehtestatud reeglitele ja kokkulepetele, võtab andmeomanik ka andmepakkuja rolli. Andmete kättesaadavaks tegemine võib olla delegeeritud ka eraldiseisvale tehnilisele teenuseosutajale, kuid vastutus andmete töötlemise eesmärkide ja vahendite määramise eest jääb andmeomanikule.

3. **Andmevaldaja** on osapool, kelle infosüsteemides andmed asuvad. Kui tavapäraselt määrab andmevaldaja ka andmete töötlemise eesmärgid ja vahendid, siis isikuandmete ning personaalse andmeruumi raamistikus kehtib eeldus, et andmevaldaja järgib isikuandmete omaniku ehk andmesubjekti poolt sätestatud tingimusi (mis praktikas realiseerub küll pigem eelsätestatud tingimustega nõustumisega). IKÜMi kontekstis vastab andmevaldaja roll üldjuhul vastutava töötleja mõistele, kuid sõltub andmevahetuses osalevate osapoolte vahelisest kokkuleppest. Andmevaldaja vastutab andmete õigsuse, turvalisuse ja töötlemise õiguspärasuse eest ning otsustab, millistel tingimustel andmeid personaalse andmeruumi kaudu kättesaadavaks tehakse.
4. **Andmetarbija** on osapool, kes kasutab andmepakkuja poolt kättesaadavaks tehtud andmeid oma teenuste, analüüsi, teadustöö või otsustusprotsesside jaoks. Andmetarbija esitab andmepäringuid, kasutab saadud andmeid kokkulepitud eesmärgil ning vastutab oma töötlemistegevuse õiguspärasuse eest. IKÜMi kontekstis võib andmetarbija olla sõltuvalt osapoolte vahelisest kokkuleppest kas iseseisev või kaasvastutav töötleja, tegutseda mõne teise osapoole volitatud töötlejana.
5. **Andmepõhise teenuse lõppkasutaja** on füüsiline või juriidiline isik, kes kasutab andmetarbija poolt pakutavat teenust või toodet. Lõppkasutaja ei tarbi andmeid otseselt, vaid tarbib nendest andmetest tuletatud väärtust, näiteks personaliseeritud teenust, raportit, otsust või analüüsi. Personaalse andmeruumi kontekstis langevad andmesubjekti ja lõppkasutaja rollid sageli kokku, kuid need ei ole kontseptuaalselt samastatavad.

6.2 Andmevahendust toetavad rollid

Andmevahendust toetavad rollid pakuvad tehnilist, ärilist või juriidilist tuge andmevahetuse toimimiseks ja arendamiseks. Nendeks on:

1. **Andmetaristu pakkuja** on osapool, kes tagab andmevahetuseks vajaliku tehnilise keskkonna, sealhulgas infrastruktuuri, sidekanalid, turvamehhanismid ja töökindluse. Andmetaristu pakkuja ei määra andmete kasutamise tingimusi ega tee ligipääsuotsuseid, vaid vastutab süsteemi tehnilise toimivuse ja turvalisuse eest. Eesti kontekstis võivad taristu pakkujateks olla nii riigiasutused (nt RIA, Statistikaamet) kui ka eraettevõtted ja VKE-d, sealhulgas IT-ettevõtted, telekommunikatsiooniettevõtted ning spetsialiseeritud usaldusteenuste pakkujad (nt SK ID Solutions). Andmetaristu pakkuja ja andmeteenuse pakkuja rollid võivad praktikas kattuda, kuid neid eristatakse rollimudelil vastutuse ja funktsiooni selguse huvides.
2. **Andmevahendusteenuse osutaja** on osapool, kes osutab andmevahendusteenust andmehaldusmääruse (DGA) tähenduses ja tegutseb neutraalse vahendajana

andmepakkujate ja andmetarbijate vahel. Roll korraldab andmete jagamist ja kasutusõiguste haldust läbipaistvalt ja usaldusväärselt, ilma andmeid ise ärilisel eesmärgil kasutamata. See võib hõlmata andmeturu platvormi, lepingulist vahendamist, nõusolekupõhist ligipääsu ning kasutuslitsentside haldamist (vt EL-i poolt tunnustatud andmevahendusteenuste pakkujaid). Eesti kontekstis on DGA-kohased turupõhised andmevahendusteenused alles kujunemisjärgus ning selgeid kohalikke näiteid pole.

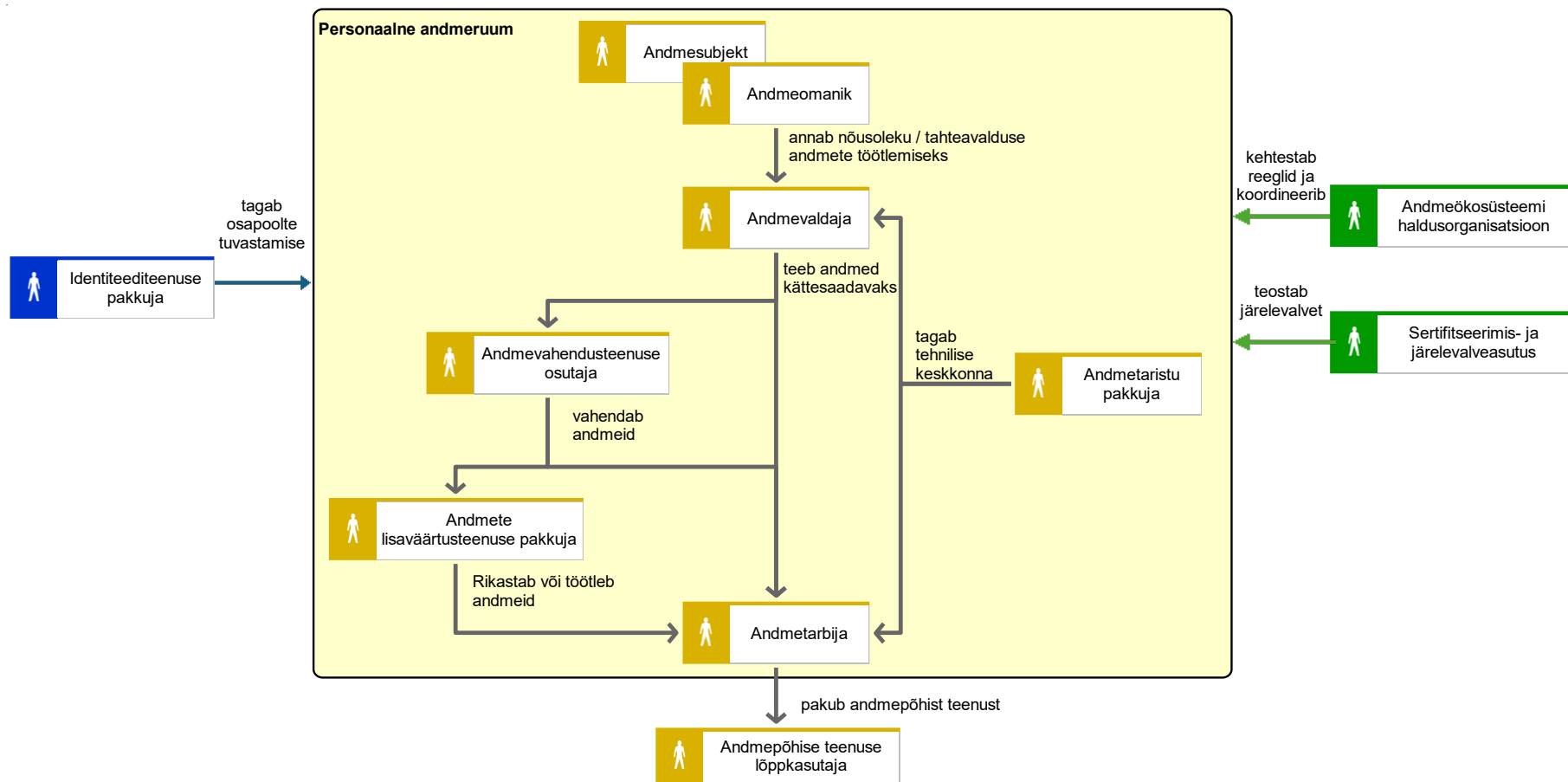
3. **Identiteediteenuse pakkuja** – osapool, kes tagab andmeruumis osalevate inimeste ja organisatsioonide usaldusväärse tuvastamise. Tema roll hõlmab autentimist, identiteedi tõendamist ning vajadusel volituste ja esindusõiguste kontrolli. Identiteediteenuse pakkuja loob eelduse turvaliseks ja tõendatavaks andmevahetuseks, kuid ei sekku andmete sisulisse töötlemisse ega otsusta nende kasutamise eesmäärke. Teenus põhineb standardiseeritud identiteedi- ja volitushalduse raamistikul (nt eIDAS 2.0, ELi digikukru, kontrollitavad tõendid ehk *verifiable credentials*) ning võimaldab nii füüsilistel kui juriidilistel isikutel osaleda andmevahetuses turvaliselt ja tõendatavalt. Identiteediteenuse pakkuja võimaldab digitaalsete identiteeditõendite kasutamist ja valideerimist ning toetab nõusolekute ja ligipääsuõiguste mehhanismide toimimist. Eesti kontekstis täidavad seda rolli näiteks Riigi Infosüsteemi Amet (riiklik autentimisteenus TARA, EL-i digikukru arendus) ning SK ID Solutions (Smart-ID, Mobiil-ID).
4. Andmete **lisaväärtusteenuse pakkuja** on osapool, kes toetab andmevahetuses osalejaid näiteks andmete töötlemise, rikastamise, anonümiseerimise, analüüsi, visualiseerimise või tehisintellekti rakenduste abil. Nende eesmärk on luua lisaväärtust andmete kasutamisel ja jagamisel.

6.3 Andmeökosüsteemi kui terviku haldamise eest vastutavad rollid

Personaalset andmeruumi (või andmeruume) ümbritsevate andmeökosüsteemide toimimine eeldab selgelt määratletud juhtimis-, koordineerimis- ja järelevalverolle, mis tagavad selle usaldusväärsuse, vastavuse ja jätkusuutlikkuse. Sõltuvalt andmeökosüsteemi korraldusest võivad need funktsioonid olla koondatud ühte organisatsiooni või jaotatud mitme osapoole vahel:

1. **Andmeökosüsteemi haldusorganisatsioon** on osapool, kes vastutab andmeökosüsteemi korraldusliku ja strateegilise juhtimise eest. Haldusorganisatsioon määratleb liitumistingimused, kehtestab tehnilised ja organisatsioonilised nõuded, koordineerib osalejate tegevust ning tagab andmeruumi arengu ja toimimise järjepidevuse. Ta võib hallata ühiseid reegleid, standardeid ja koostöömehhanisme ning toimida andmeruumi juriidilise või lepingulise koordineerijana. Haldusorganisatsioon ei osale andmete sisulises töötlemises, vaid kujundab andmevahetuse raamtingimused. Eesti kontekstis nt RIA, MKM või valdkondlik andmeruumi operaator (nt Energia andmeruumi puhul Elering, Enefit).

2. **Sertifitseerimis- ja järelevalveasutus** on sõltumatu osapool, kes hindab ja kinnitab personaalse andmeruumi osapoolte vastavust kokkulepitud tehnilistele, turvalisuse ja privaatsuse nõuetele ning teostab järelevalvet andmeökosüsteemi usaldusraamistiku toimimise üle. Roll hõlmab nii sertifitseerimisfunktsiooni, mille käigus hinnatakse osalejate vastavust kehtestatud standarditele ja põhimõtetele, kui ka järelevalvefunktsiooni, mille raames kontrollitakse nõuete täitmist ja kasutatakse vajadusel õiguspõhiseid meetmeid. Eesti kontekstis täidab seda rolli teiste seas näiteks Riigi Infosüsteemi Amet usaldustaristu tehnilise haldajana ning Andmekaitse Inspeksioon, kes teostab järelevalvet isikuandmete kaitse ja andmete õiguspärase kasutamise üle. Sertifitseerimis- ja järelevalveroll on personaalse andmeruumi juhtimismudelil lahus operatiivsest haldusest.



Joonis 7. Personaalse andmeruumi raamistikus olevate rollide ja seoste mudel, kirjeldamaks rollide omavahelisi juhtimis- ja andmevooge

7. Personaalse andmeruumi esialgsed kasutuslood

Uuringu käigus eelnevalt analüüsitud kasutuslood kirjeldavad, kuidas personaalse andmeruumi kontseptsioon võimaldaks inimestel hallata ja jagada enda kohta käivaid tõendatud andmeid turvaliselt, kontrollitult ja sihipäraselt, vähendades samal ajal halduskoormust ning parandades teenuste kvaliteeti nii finants- kui ka haridusvaldkonnas. Kasutuslugude puhul on keskseks ideeks andmete taaskasutamine kliendi või õppija volituse alusel ning viisil, mis tagab andmete ajakohasuse, nende päritolu kontrollitavuse ja läbipaistva kasutuse.

Finantsvaldkonnas kirjeldasime personaalse andmeruumi kasutusloona esiteks laenuaotluste hindamise protsessi. Laenuotsuse tegemiseks vajavad pangad mitmesuguseid andmeid sissetulekute, olemasolevate kohustuste, pereseisu ja riskikäitumise kohta. Kui praegu kogutakse neid andmeid erinevatest registritest ning osaliselt ka kliendi esitatud dokumentidena, siis personaalse andmeruumi lahenduse korral saaks klient anda pangale ajutise ligipääsu digitaalselt kinnitatud ja ajakohastele finantsandmetele. See vähendaks lisadokumentide esitamise vajadust, suurendaks andmete usaldusväärsust ning võimaldaks kiirendada otsustusprotsessi. Samal ajal paraneks kliendi jaoks läbipaistvus, kuna ta näeb selgemalt, milliseid andmeid kasutatakse ja millisel eesmärgil.

Finantsvaldkonna teise kasutusloona kirjeldasime esialgu vabatahtliku sõidukikindlustuse sõlmimist, mille puhul tugineb riskihindamine paljudele andmeallikatele, sealhulgas sõiduki tehnilistele andmetele, varasemale kahjuajaloole ja kliendi krediitkäitumisele. Eeldusel, et andmete kindlustatus ning erinevad formaadid muudavad protsessi keerukaks ja ebaühtlaseks, näis, et kliendil võiks olla võimalus anda kindlustusandjale ligipääsu personaalsesse andmeruumi koondatud ja valideeritud andmetele, võimaldamaks kindlustusseltsil kujundada täpsem ja riskipõhisem hinnang, vähendada pettuseriski ning soodustada personaliseeritud ning õiglasemat hinnastamist. Intervjuude käigus aga selgus, et tänane liikluskahjude menetlemine on kindlustusseltside vaatest juba piisavalt andmepõhine ning sujuv protsess. Sealjuures tuleb mainida, et kehtiv praktika ei võta arvesse isikupõhiseid käitumuslikke aspekte, mistõttu pole väiksema riskiga liiklejate huvid alati kaitstud, samal ajal kui liikluskindlustusseltside vaatest on äriiline vajadus muudatusteks pigem väike. Intervjuude käigus saime seetõttu ka soovitusel keskenduda pigem elu- ning tervisekindlustuse valdkonnale. See aga ei tähenda, et personaalse andmeruumi ning inimkeskse andmekorralduse vaatest poleks liikluskindlustusvaldkonnas potentsiaali innovatsiooniks.

Lisaks tõime välja kaks kasutuslugu haridus- ja töövaldkonnast, mis keskendusid eelkõige õiglasemale ligipääsule teenustele ja inimese võimalusele oma haridust ning oskusi tõendavaid andmeid selgemalt väärindada. Ühe kaasusena kirjeldasime lasteaia kohatasu soodustuste menetlemist, mis eeldab täna vastavate tingimuste kontrolli eri registritest ning lapsevanema poolt esitatud tõendite hindamist. Personaalse andmeruumi lahendus võimaldaks samas inimesel koondada vajalikud andmed (näiteks pere sissetulekute, töösuhte ning lapse koha staatuse kohta) ühte vaatesse ning sealjuures hallata nõusolekuid vastavatele andmetele ligipääsemiseks nt kohaliku omavalitsuse poolt. Kuna käesolevas

uuringus on peamiseks huviorbiidiks just erasektori poolt pakutavad teenused, jätsime edasises analüüsis selle kaasuse kõrvale.

Teise kasutusloona kirjeldasime töötajate värbamist ja tööleasumist toetava teenuse võimalikkust. Kuigi riiklikud registrid sisaldavad usaldusväärseid andmeid inimeste hariduse ja oskuste kohta, puudub inimesel terviklik ja ajakohane ülevaade oma pädevustest ning tööandjal lihtne viis pääseda ligi kontrollitud tõenditele. Personaalse andmeruumi abil koondataks haridus-, kvalifikatsiooni- ja täiendõppeandmete vaade ühte keskkonda, kus inimene saab otsustada, milliseid andmeid ja kellele ta jagab. Tööandja jaoks tähendaks see kiiremat ja usaldusväärsemat otsustusprotsessi ning väiksemat halduskoormust, samas kui inimene saab säilitada kontrolli oma andmete kasutamise üle. Antud kaasuse võtsime ka fookusesse täiendavas analüüsis (vt lähemalt ptk 8.2)

8. Valitud kasutusjuhtude teostatavusanalüüs

Käesolevas peatükis on fookuses kaks konkreetset kasutusjuhtu, mille kaudu on võimalik uurida personaalse andmeruumi rakendumist praktikas nii ärilise, tehnoloogilise kui õigusliku vaate. Kasutusjuhtude valik oli kogu uuringu ajal avastuslik protsess – uuringu alguses kaalusime erinevad erasektorit puudutavaid kasutusjuhte nii tervise, energia, hariduse kui ka finantsvaldkonnast. Lähtuvalt tellija tagasisidest kitsendasime valiku finants- ja haridussektorile, mille konkreetset kasutusjuhud omakorda täpsustasid intervjuude käigus. Mõlema kasutusloo raames on esitatud ka ptk 6 esitatud rollimudeli rakendumine ning protsesside *as-is* ja *to-be* analüüs. Mõlema kasutusloo vaatest on vastatud ka põhilisele uurimisküsimusele “Millised on “personaalse andmeruumi” esmased kasutuslood ja/või teenusmodelid, mille kaudu personaalse andmeruumi(de) rakendamist Eestis katsetada? Mil määral on need teostatavad, arvestades nii ärilisi, tehnilisi kui õiguslikke aspekte?”.

8.1 Elukindlustus

Elukindlustusteenus on kindlustusleping, millega inimene tagab oma lähedastele rahalise kaitse surmajuhtumi korral, määrates kindlustussumma ja soodustatud isikud. Kui kindlustatu lepingu kehtivuse ajal sureb, maksab kindlustusselts kokkulepitud summa välja lepingus märgitud soodustatud isikutele. Mõnel juhul võib klassikaline elukindlustus sisaldada ka kogumiskomponenti või lisakaitseid, näiteks õnnetusjuhtumi või raske haiguse puhuks. Elukindlustuse saamiseks peab kindlustusvõtja esitama mitmeid isikut tõendavaid andmeid, nagu nimi, isikukood, kontaktandmed jms, lisaks kogutakse andmeid tervises seisundi kohta, näiteks infot varasemate haiguste, operatsioonide, ravimite tarvitamise ja eluviiside (nt suitsetamine, ohtlikud hобid) kohta. Sealjuures tuleb meenutada, et terviseandmed on IKÜM art 9 mõttes eriliiki isikuandmed, mistõttu tuleb rakendada ka suuremaid ettevaatus- ning kaitsemehhanisme. Suurema kindlustussumma korral võib kindlustusandja nõuda ka arstlikku läbivaatust või täiendavaid terviseuuringuid. Samuti võidakse riskide kaardistamiseks ja hindamiseks kindlustusandja poolt küsida infot kindlustusvõtja töökoha ja ameti kohta. Lisaks tõendatud meditsiinilistele andmetele on tänaste nutiseadmetega võimalik koguda ning analüüsida ka mitmeid muid inimese käitumuslikke andmeid, mis võivad inimese terviseriski hindamisel olla oluliseks sisendiks.

Eelnev kirjeldus loob eelduse mitmekesiseks ja laiaulatuslikuks andmetöötluks ning infovahetuseks, kus kindlustusvõtja peamine huvi on maandada surma või raske tervisekahjustuse riski majanduslikke tagajärgi, et tema lähedased ei jääks sissetulekuta või võlakooormuse alla, et katta laenukohustusi (nt eluasemelaen) ning tagada näiteks laste hariduse või muude pikaajaliste eesmärkide rahastamine. Samuti pakub elukindlustus kindlustunnet ja finantsilist stabiilsuse ootamatute sündmuste korral.

Personaalne andmeruum aitaks lahendada mitmeid elukindlustusturu toimimisega seotud probleeme. Esiteks puudub kindlustusseltsidel praegu võimekus arvestada inimese tervise ja elustiiliga seotud dünaamilist teavet, sealhulgas ajas toimuvaid muutusi, mistõttu ei kujune pakkumised piisavalt personaliseerituks ning kindlustusmakse võib olla kliendi tegelikku riskiprofiili arvestades põhjendamatult kõrge. Teiseks ei ole kliendil praktilist, turvalist ja

standardiseeritud võimalust koondada oma tervise- ja elustiiliandmeid erinevatest allikatest ning edastada neid kontrollitult ja eesmärgipäraselt kolmandatele osapooltele. Kolmandaks vähendavad andmete killustatus ja ajakohase info puudumine riskihindamise täpsust, takistavad diferentseeritud tingimuste pakkumist ning ei loo piisavaid stiimuleid tervisekäitumise parandamiseks. Neljandaks puudub inimesel organisatsioonide üleselt ajakohane ja kasutajasõbralik tervikülevaade sellest, milliseid andmeid tema kohta kogutakse, kuidas neid kasutatakse ja kellele need on kättesaadavad, mis omakorda piirab teadlikku ja autonoomset otsustamist oma andmete kasutamise üle.

Personaalse andmeruumi teenuse roll *to-be* vaates on vahendada inimese tahet andmete kasutamisel algsetest andmeallikatest, näiteks terviseinfot koondavatest süsteemidest, haiglate andmebaasidest, riiklikest andmekogudest nagu tervise infosüsteem ning perearstikeskustest. Samuti tagab personaalse andmeruumi teenus, et väliste süsteemide andmekasutus on kooskõlas inimese väljendatud tahtega, sealhulgas terviseandmete edastamisel elukindlustusteenuse pakkuja. Lisaks peab andmekasutus vastama antud nõusolekutele ja kehtivatele õiguslikele ning organisatsioonilistele reeglitele.

Samas tuleb väljakutsetena välja tuua, et terviseandmete jagamine võib osapoolte vahel osutuda keerukaks nii õiguslikel (sh andmekaitsest tulenevatel) kui ka tehnilistel põhjustel ning nende andmete korrektne tõlgendamine võib eeldada vajalike otsuste langetamisel spetsiifilist meditsiinilist kompetentsi. Kindlustusseltsidel endal selline meditsiiniline pädevus üldjuhul puudub, mistõttu vajab terviseinfo hindamine selgeid standardeid, struktureeritud andmevahetust ja vajadusel sõltumatute meditsiinieksperptide kaasamist.

Peamine järeldus

Personaalse andmeruumi kasutamine elukindlustuses võimaldaks oluliselt parandada riskihindamise täpsust ja pakkuda personaliseeritud kindlustustooteid, võimaldades inimesel jagada ajakohaseid tervise- ja elustiiliandmeid kontrollitult erinevate osapooltega. Samas sõltub lahenduse teostatavus piisavast andmete mahust, nende kättesaadavusest ning kvaliteedist, osapoolte vahelisest koostööst, turu mastaabist ning regulatiivsetest piirangutest (nt eriliigiliste andmete töötlemine), mis muudavad ärimudeli hetkel veel ebakindlaks.

8.1.1 Elukindlustuslepingu sõlmimise as-is ja to-be analüüs

Järgnevad joonised kirjeldavad elukindlustuse pakkumise kujundamise protsessi põhietappe. Protsess hõlmab kindlustuspakkumise taotluse algatamist, riskihindamiseks vajalike andmete kogumist ja analüüsi, riskiprofiili koondamist ning kindlustuspakkumise kujundamist ja lepingu sõlmimist.

As-is vaates (vt Joonis 8) toimub andmete kasutamine organisatsioonikeskses mudelis, kus andmevahetus põhineb kindlustusseltsi ja teiste andmepakkujate vahel sõlmitud lepingutel ning tehnilistel integratsioonidel, mis on protsessi keerukusest ning skaleeritava raamistiku puudumiseta pigem piiratud. Andmete kasutamist juhivad peamiselt organisatsiooni sisemised reeglid ja protsessid.

Tabel 1. *As-is* ja *to-be* protsesside kirjeldus elukindlustuses koos ärilise kasu potentsiaali avamisega

Protsessi samm	AS-IS	TO-BE	Parendus
Kindlustus-pakkumise taotluse algatamine	Inimene (potentsiaalne klient) algatab kindlustuspakkumise taotluse ning esitab esmased andmed. Inimene tuvastatakse usaldusväärse identiteediteenuse kaudu.		
	Inimene autentitakse identiteediteenuste (nt ID-kaart, Mobile-ID või Smart-ID) kaudu ning seotakse kindlustusseltsi süsteemis loodud kliendikontoga. Teenuse kasutamine toimub tavaliselt kindlustusseltsi veebikeskkonnas või vahendaja kaudu. Inimese vaatest tähendab see sageli eraldi kasutajakonto loomist ning vajadust samu andmeid erinevates teenustes korduvalt sisestada.	Inimene autentitakse samuti identiteediteenuse vahendusel, kuid identiteedikontekst edastatakse teenusele inimese poolt kontrollitava digitaalse identiteedi kaudu (nt digikukru kaudu). Teenuse kasutamine ei eelda tingimata eraldi kliendikonto loomist, kuna vajalikud andmed saadakse personaalsest andmeruumist inimese antud ligipääsuloa alusel. Inimese vaates tähendab see, et sama identiteeti saab kasutada erinevates rakendustes ja teenustes ilma andmeid korduvalt sisestamata.	Väheneb eraldi kliendikontode loomise vajadus ja andmete korduv sisestamine.
Riskihindamise andmete kogumine	Riskihindamiseks kasutatakse andmeid erinevatest andmeallikatest (nt registrid, meditsiinasutused, krediidiinfo pakkujad).		
	Kindlustusselts kogub andmeid inimeselt otse ning koostöölepingute alusel välistelt andmevaldajatelt. Andmepäringud toimuvad eeldefineeritud liideste kaudu ning õiguslik alus tuleneb kliendilepingust või protsessi alguses antud laiapõhjalisest nõusolekust. Inimese vaates tähendab see sageli vajadust andmeid ise koguda erinevatest registritest, esitada või kinnitada, ilma et tal oleks täielikku ülevaadet, milliseid andmeid kasutatakse ja kas need on ajakohased.	Kindlustusselts esitab personaalse andmeruumi raamistikus teenusepakkuja poolse rakendusteenuse kaudu struktureeritud andmepäringu, milles määratletakse vajalikud andmemelemendid, töötlemise eesmärk ja kasutuse ajapiirang. Inimene saab personaalse andmeruumi kasutajaliidese kaudu koondada vajalikud andmed erinevatest allikatest, kontrollida nende kvaliteeti ning anda nõusoleku või tahteavalduse andmete kasutamiseks määratletud ulatuses. Inimese saab oma andmeid ühest kohast hallata ja otsustada, milliseid andmeid jagada.	Väheneb käsitsi kogutavate andmete hulk ning suureneb andmete kvaliteet ja andmevahetuse automatiseeritus.
Riskiprofiili täpsustamine	Kindlustusselts analüüsib kogutud andmeid riskihindamiseks. Analüüs toimub kindlustusseltsi sisemiste riskimudelite ja ärireeglite alusel.		

Protsessi samm	AS-IS	TO-BE	Parendus
	Vajadusel küsitakse inimeselt või partneritelt täiendavaid andmeid. Inimese vaates on sageli ebaselge, millised andmed otsust mõjutavad ja kuidas neid kasutatakse.	Täiendavad päringud tehakse personaalse andmeruumi rakendusteenuse kaudu ning nende kasutamine on seotud konkreetse nõusoleku või muu õigusliku alusega. Inimene saab oma kasutajaliidese kaudu näha, milliseid andmeid riskihindamisel kasutatakse ning vajadusel neid täiendada või parandada.	Paraneb andmekasutuse läbipaistvus ja kliendi kontroll oma andmete üle. Ettevõttel on mugav ning kiire viis andmete ning nõusolekute pärimiseks, samuti tagab läbipaistev andmete kasutus usaldust tema kui teenusepakkuja suhtes.
Riskiprofiili koondamine	Kindlustusselts ühendab erinevatest allikatest saadud andmed riskiprofiili kujundamiseks. Andmete töötlemine toimub organisatsiooni sisestes infosüsteemides.		
	Andmete töötlemise tingimused määratakse organisatsiooni poliitikate alusel. Inimesel puudub enamasti selge ülevaade sellest, kuidas erinevaid andmeid kombineeritakse.	Andmed koondatakse personaalse andmeruumi raamistikus kaudu saadud andmetest, järgides eesmärgipärasuse ja minimaalsuse põhimõtteid. Inimese saab personaalse andmeruumi rakenduse kaudu andmete päritolu ja kasutust paremini jälgida.	Paraneb andmete päritolu jälgitavus ja kasutuse kontroll.
Kindlustus-pakkumise kujundamine	Kindlustusselts arvutab riskiprofiili alusel kindlustusmakse ja kujundab pakkumise.		
	Otsustus toimub organisatsiooni riskimudelite ja ärireeglite alusel ning kasutatud andmete mõju ei ole kliendile alati nähtav. Inimese vaates võib pakkumise kujunemine olla raskesti arusaadav.	Pakkumine kujundatakse samuti riskimudelite alusel, kuid kasutatud andmed ja nende eesmärk on seotud personaalse andmeruumi kaudu antud nõusolekuga. Inimesel on personaalse andmeruumi kasutajaliidese kaudu võimalik näha, milliseid andmeid pakkumise kujundamisel kasutati, millistest allikatest need pärinevad ning	Suureneb andmekasutuse läbipaistvus ja usaldus.

Protsessi samm	AS-IS	TO-BE	Parendus
		millisel alusel neid kasutati, kuid mitte seda, kuidas täpselt riskimudel nende põhjal otsuse või hinna arvutas.	
Pakkumise esitamine ja otsus	Kindlustusselts esitab inimesele pakkumise (tavaliselt kindlustusseltsi portaali kaudu või e-posti teel).		
	Kitsaskohaks on peamiselt see, et inimesel pole sageli selget ülevaadet, milliseid andmeid pakkumise kujundamisel kasutati.	Inimesel on personaalse andmeruumi rakenduse kaudu ülevaade pakkumise aluseks kasutatud andmetest, mis võimaldab tal otsust teha teadlikumalt.	Suureneb andmekasutuse läbipaistvus ja inimese ning teenusepakkuja vaheline usaldus, mis võib soosida lepingu sõlmimist.
Lepingu sõlmimine	Inimene kinnitab pakkumise ning kindlustusleping vormistatakse kindlustusseltsi süsteemis.		
	Lepingu sõlmimine toimub vastavalt kindlustustingimustele ning inimene annab vajalikud kinnitused ja nõusolekud. Inimese vaates on nõusolekud sageli üldised ja raskesti jälgitavad.	Lepingu sõlmimine toimub sarnaselt, kuid nõusolek on personaalses andmeruumis eraldiseisev, eesmärgipõhiselt hallatav ja korduvkasutatav, võimaldades inimesel hallata oma nõusolekuid erinevate teenuste lõikes ühest kohast.	Selgem andmekasutus ja parem jälgitavus. Inimese vaatest tagab <i>to-be</i> lahendus suuremat kontrolli ja läbipaistvust oma andmete kasutamise üle.

As-is mudelis toimub andmete kasutamine organisatsioonikeskses raamistikus, kus andmevahetus põhineb eelnevalt kokkulepitud tehnilistel liidestel ja lepingulistel suhetel. Andmete kasutamise õiguslik alus tuleneb tavaliselt kliendilepingust või protsessi alguses antud üldisest nõusolekust ning üksikuid andmepäringuid ei hinnata eraldi nende eesmärgi või ajapiirangu alusel. Identiteet on seotud konkreetse teenuse või kliendikontoga ning andmesubjektil puudub ühtne ülevaade oma andmete kasutamisest eri teenustes.

To-be mudelis jäävad äriprotsessi põhietapid samaks, kuid muutub andmekasutuse juhtimise viis. Andmevahetus toimub personaalse andmeruumi föderatiivses usaldusraamistikus, kus identiteet, ligipääsuõigused ja logimine on eraldi hallatavad kihid. Andmepäringud on seotud konkreetse eesmärgi ja ajapiiranguga ning andmesubjektil on võimalik näha, kes ja millisel eesmärgil tema andmeid kasutab.

8.1.2 Rollimudel ja osapoolte kaardistus

Järgnevalt on esitatud autorite poolne hinnang rollimudeli rakendumise kohta Eestis tegutsevate osapoolte lõikes ülal kirjeldatud kasutusloo ning konkreetse protsessi vaates. Seda kaardistust tuleks hinnata hüpoteetilise stsenaariumina, mida võimalike pilootide kaudu praktikas valideerida.

Tabel 2. Hüpoteetiline osapool osapoolte kaardistus elukindlustuse kaasuse puhul, kasutades personaalse andmeruumi rollimudelit. Antud rollijaotust pole mainitud osapooltega valideeritud, mistõttu rollide ja osapoolte jaotus võib praktikas erineda.

Roll / Osapool	Peamised võimalikud osapooled
Andmesubjekt kui andmeomanik	Inimene (nt persoonina „Malle“)
Andmetarbija	Kindlustusselts
Andmevaldaja	TEHIK, MTA, Sotsiaalministeerium, tervise ja heaolurakenduste pakkujad nt Garmin jt
Andmepõhise teenuse lõppkasutaja	Inimene (nt persoonina „Malle“)
Andmevahendus-teenuse osutaja	RIA, aga võimalikud ka teised osapooled (nt tehnoloogiaettevõtted)
Andmetaristu pakkuja	Telia Eesti AS, Elisa Eesti AS, ja/või Tele2 Eesti AS (SIM-kaart ja sidekanal Mobiil-ID toimimiseks), RIA, IT-majad, vajadusel teised tehnoloogiapartnerid
Identiteediteenuse pakkuja	SK ID Solutions (Smart-ID, Mobiil-ID autentimise- ja sertifitseerimisteenus); Zetes Estonia OÜ; RIA (TARA, digikukkur);
Andmete lisaväärtusteenuse pakkuja	Nt Lyfery ⁷² , aga ka tehnoloogiaettevõtted (nt AI-lahenduste pakkujad)
Andmeökosüsteemi haldusorganisatsioon	Nt Eesti Kindlustusseltside Liit (arutelukoht, kes võiks personaalse andmeruumi haldusorganisatsioonina tegutseda)
Sertifitseerimis- ja järelevalveasutus	SK ID Solutions, AKI, RIA, Rahapesu Büroo, Finantsinspeksioon jt

8.1.3. Äriline vaade

Intervjuude põhjal kindlustusvaldkonna esindajatega on valdkond üsna heterogeenne, erinevate ärihuvidega. Näiteks osa kindlustusseltse peab heaks ideeks rohkem andmeid jagada, teistel on aga äristrateegia andmeid mitte jagada, vaid võimendada enda sisemisi andmekogumise, -töötlemise ja -analüüsimise protsesse. Andmed, mida kindlustusseltsid on ise kogunud, ongi nende äriliseks eeliseks – eriti suuremate seltside korral. Samas mõned kindlustuse valdkonna väiksemad ettevõtted/iduettevõtjad on avatumad laiemale andmevahetuse kontseptsioonile, sh personaalse andmeruumi vaatevinklist, mis võib aidata neil omakorda uusi ärimudeleid välja töötada.

⁷² <https://lyfery.com/>, külastatud 23.03.2026

Samuti ei ole kindlustusvaldkond homogeenne kindlustuse võimaliku kasutusjuhu osas. Kaskokindlustuse kasutusjuhu puhul on turg juba piisavalt välja kujunenud ning andmevahetus töötab piisavalt hästi näiteks liiklusõnnetuste puhul. Seetõttu nägid osa kindlustussektori esindajatest potentsiaali hoopis elukindlustuses, eelkõige terviseandmete vaatest, mille osas tuleb täita paberformaadis detailseid dokumente – nende huvi oleks neid saada inimese nõusolekul otse Terviseportaalist.

Ärimudeli vaatest ongi varapõhised kindlustustooted paremini väljakujunenud, kuna need on kohustuslikud (näiteks liikluskindlustus) või siis nõutavad finantsasutuse poolt (kodukindlustus, kaskokindlustus). Elukindlustuse vähene populaarsus ei ole ainult terviseandmete kättesaadavuse taga, vaid peamiselt on see kombinatsioon Eesti turu väiksusest ning teenuse vabatahtlikkusest, eriti mastaabiefekti arvestades (vähem kasutajaid ⇔ kallim teenus). Samuti on oluline maksukeskkond – Eestis ei ole maksuerisusi töandjapoolsele elukindlustusele, sellele rakendub täiel määral erisoodustumaks. Praegu on veel vara hinnata, kas inimeste jaoks, kes terviseandmeid saaksid oma nõusolekul kindlustusseltsiga jagada, muutuks elukindlustus soodsamaks. Probleem on selles, et kindlustusmatemaatika eeldab võimalikku terviklikku infot terve populatsiooni kohta – s.t. tõenäoliselt töötaks see efektiivselt alles siis kui kõik kindlustatud ühtemoodi oma andmeid kindlustusseltsiga jagavad, aga nõusolekupõhine loogika ei pruugi seda toetada.

Lisaks on inimestel mingil määral ka riiklikud alternatiivid surma- ja õnnetusjuhtumite korral (toitjakaotuspension, laiapõhjaline ravikindlustus, hüvitis töövõimetuse kaotamise korral) ning mingil määral ka erasektori alternatiivid (nt pankade panustavad laenumaksekindlustused ja krediitkaardiga kaasnev reisikindlustus). Lisaks on elukindlustus üsna keeruline toode, mille osas tuleb igasuguste välistustega end kurssi viia (näiteks on tavaline, et kindlustusjuhtumit ei hüvitata enesetapu korral, teatud eelnevate haiguste korral, sõjaolukorra tekkel või kui seda mõjutas kindlustatu alkohoolne joove ja/või profisport).

Lähtuvalt 5. ja 9. peatükis viidatud ressurssidele, analüüsimise ka kindlustuse kaasuse andmekoostöömudeleid, millest esimesed kolm on ärilise fookusega. Kindlustusvaldkonna ärimudelil on hea potentsiaal erinevateks ärilisteks ja mitteärilisteks andmevahetuseks. Tõenäoliselt juba praegu ostetakse ja müüakse teistelt ettevõtetelt või organisatsioonidelt ärilistel eesmärkidel andmeid, bilateraalsete kokkulepete alusel ja kindlasti on potentsiaali ka laiemaks andmeturu mudeliks. Samuti on tõenäoline, et kasutatakse erinevaid teenuspakkujaid andmete kvaliteedi ja analüüsi jaoks. Mitteäriline andmevahetus on ärimudeli jaoks oluline kindlasti riiklike andmete kaasamisel (nii avaandmetena kui ka näiteks X-tee kaudu). Samuti on tõenäoline ettevõtete ja organisatsioonide bilateraalne andmevahetus, mille eest tasu ei võeta.

Tabel 3. Autorite poolne hinnang andmealase koostöö mudelite sobivusele antud kasutusloos.

Mudel	Kommentaar
Äriandmed	Teistelt ettevõtetelt või organisatsioonidelt ärilisel eesmärgil (x2B) andmete ost-müük - pigem jah.

Andmeturg	Laiem andmete ost-müük (nt platvormi kaudu) - pigem ei, kuigi mõnes valdkonnas võib olla potentsiaali (nt terviseandmete ost sisendina).
<i>As-a-Service</i> mudel	Andmete kvaliteet ja analüüs välise ärilise teenusena – pigem jah.
Avatud andmed / andmete annetamine	Riigilt ettevõttele (G2B) andmete saamine - kindlasti.
Pragmaatiline / <i>ad-hoc</i> andmete jagamine	Teistelt ettevõtete või organisatsioonidega (x2B) andmete vahetamine – pigem jah.
Usaldusväärne kolmas osapool (vahendaja)	Riigilt või teistelt organisatsioonidelt andmete saamine (x2B) töötab kindlasti – näiteks andmevahetusena X-tee kaudu.
Isikuandmete vahendaja	Mingil määral, potentsiaali on rohkemaks.
Andmeühistu / andmekooperatiiv	Pigem ei (võib-olla uute lahenduste korral).

8.1.4. Tehnoloogiline vaade

To-be vaates võiks elukindlustuse sõlmimise protsess alata inimese teenuste ülese autentimisega föderatiivse identiteediteenuse kaudu. Autentimine toimub sõltumatu identiteedipakkuja vahendusel ning tulemuseks on masinloetav autentimistõend, mida kindlustusseltsi rakendus valideerib ilma, et peaks looma või haldama eraldiseisvat lokaalkontot. Identiteet ei ole seotud üksnes konkreetse teenuse infosüsteemiga, vaid on kasutatav erinevate osalevate süsteemide vahel ühtses usaldusraamistikus.

Peale autentimist genereerib kindlustusseltsi süsteem struktureeritud andmevajaduse kirjelduse, milles määratletakse taotletavad andmekategooriad, töötlemise eesmärk ning kasutuse ajapiirang. See kirjeldus edastatakse nõusoleku- ja juurdepääsuahaldurile, kus inimene kas kinnitab, piirab või keeldub ligipääsu andmisest. Antud nõusolek salvestatakse masinloetava poliitikana ning iga järgnev andmepäring kontrollitakse automaatselt selle poliitika vastu. Ligipääsukontrolli mehhanismid tagavad, et andmeid ei väljastata väljaspool määratletud eesmärki ega ajavahemikku ning et eriliigilised isikuandmed, sealhulgas terviseandmed, on märgendatud ja tehniliselt piiratud vastavalt nende tundlikkusele.

Andmevahetus toimub turvalise vahenduskihi kaudu, kasutades sertifikaadipõhist autentimist ja krüpteeritud ühendusi. Kindlustusseltsi süsteem ei loo otseseid kahepoolseid integratsioone iga andmepakkujaga, vaid teeb päringud standardiseeritud liideste kaudu. Iga päring on digitaalselt signeeritud ja ajamärgistatud ning andmepakkuja valideerib enne vastuse andmist nii päringu päritolu kui ka nõusoleku olemasolu. Andmete edastamine toimub minimaalsuse põhimõttel, edastades üksnes need andmeelemendid, mis on konkreetse riskihindamise jaoks vajalikud.

Saadud andmete alusel teostab kindlustusselts riskihindamise vastavalt oma otsustusloogikale ja ärireeglitele. Töötlemine toimub volitatud andmekoopia või ajutise andmevaate alusel ning toorandmeid ei säilitata kauem, kui see on eesmärgi täitmiseks vajalik. Riskihindamise tulemuseks on hinnapakkumine, kusjuures süsteem ei oma ligipääsu andmetele väljaspool antud nõusoleku ulatust.

Kogu andmevahetus ja töötlemine on jälgitav ning iga päring, vastus ja volitus logitakse ajamärgistatult vastava osapoole süsteemis. Usaldusraamistik määratleb logimise standardid, säilitamise nõuded ja auditeerimismehhanismid, võimaldades vajadusel sündmuste koondvaate loomist. Logide terviklus ja tõendusväärtus tagatakse tehniliste kontrollmehhanismidega, ilma et kõik logid koonduksid ühte keskregistrisse.

Lepingu sõlmimise etapis luuakse uus töötlemise eesmärk, mis realiseeritakse tehniliselt uue poliitika või volituse kaudu. See eristab riskihindamise sammu lepingu täitmise sammust ning tagab, et varasem ligipääs ei laiene automaatselt edasisele andmekasutusele. Edasised päringud valideeritakse juba lepingu täitmise kontekstis ning kõik toimingud jäävad jätkuvalt jälgitavaks ja tõendatavaks.

Tehnoloogilises plaanis, kui on olemas äriine huvi, on lahendus realiseeritav.

8.1.5. Õiguslik vaade

Elukindlustuse kasutusloo õiguslik analüüs keskendub Eesti ja Euroopa Liidu õiguse kontekstis küsimusele, kas ja millistel tingimustel on võimalik rakendada personaalse andmeruumi teenust, mis vahendab isikuandmeid elukindlustusandjale riskihindamise eesmärgil. Analüüsi fookuses ei ole seega kindlustuslepingu traditsiooniline õigusraamistik, vaid eelkõige see, kas kehtiv andmekaitse- ja kindlustusõigus võimaldab luua tehnilis-organisatsioonilise lahenduse, milles inimene kontrollib oma andmete koondamist ja edastamist erinevatest allikatest kindlustusandjale.

Kehtivas ehk *as-is* olukorras reguleerivad elukindlustuse pakkumist Eestis eeskätt kindlustustegevuse seadus¹⁵ ja võlaõigusseadus¹⁶. Kindlustustegevuse seadus sätestab kindlustusandjate tegevusloa, kapitali- ja riskijuhtimisnõuded ning järelevalveraamistiku, mida teostab Finantsinspeksioon (riiklik järelevalveasutus Eestis). Võlaõigusseadus reguleerib kindlustuslepingu sõlmimist ja täitmist ning näeb ette kindlustusvõtja teavitamiskohustuse oluliste riskiasjaolude osas. Elukindlustuse olemusest tulenevalt on terviseseisund ja elustiil riskihindamise keskmes ning kindlustusandjal on õigus küsida andmeid, mis on vajalikud kindlustusrisi hindamiseks ja kindlustusmakse määramiseks (isikuandmete kaitse regulatsioonist IKÜM art 5 põhimõtetest tulenevalt peab selline andmetöötlus mh vastama minimaalsuse ja eesmärgipärasuse põhimõtetele, samuti peab selline andmetöötlus olema andmesubjektile läbipaistev). Kokkuvõtlikult peab selline andmekogumine jääma proportsionaalseks ning olema seotud lepingu eesmärgiga.

Andmekaitse aspektist kohaldub elukindlustuse kontekstis vahetult IKÜM otsekohalduva EL määrusena ning riigisiselt isikuandmete kaitse seadus. Tavapäraste isikuandmete töötlemise õiguslik alus tuleneb üldjuhul lepingu sõlmimise ja täitmise vajadusest IKÜM artikli 6 lõike 1 punkti b tähenduses. Probleemsem on olukord terviseandmetega, mis on käsitatavad

eriliiki isikuandmetena IKÜM artikli 9 tähenduses. Nende töötlemine on IKÜM art 9 lõike 1 kohaselt **põhimõtteliselt keelatud**, välja arvatud juhul, kui kohaldub mõni artikli 9 lõikes 2 sätestatud erand.

Kirjeldatud kasutusloos *as-is* mudelis toimub andmete kogumine valdavalt kindlustusandja ja kliendi vahelises suhtes. Andmed esitatakse taotluse vormis või täiendavate meditsiiniliste dokumentidena ning vajaduse korral kaasatakse kindlustusandja poolt ekspertiis. Andmevood on suhteliselt lineaarsed ning andmete edastamine tervishoiusüsteemidest kindlustusandjale toimub kas kliendi vahendusel või tema nõusolekul. Kuigi ka praegune praktika hõlmab IKÜM art 9 mõttes eriliiki isikuandmete töötlemist ja profileerimist, on andmetöötlus ajaliselt piiritletud lepingu sõlmimise etapiga ning ei pruugi olla pidev ega dünaamiline.

Personaalse andmeruumi teenuse rakendamine muudab seda struktuuri oluliselt. *To-be* mudelis tekiks täiendav osapool, kes vahendab inimese tahet ning võimaldab andmete koondamist erinevatest allikatest – sealhulgas tervise infosüsteemidest, haiglate andmebaasidest ja muudest registritest – ning nende kontrollitud edastamist kindlustusandjale. Selline lahendus eeldab esmalt selget rollijaotust andmekaitse mõttes. Tuleb hinnata, kas personaalse andmeruumi teenuse pakkuja tegutseb vastutava töötlejana, volitatud töötlejana või kaasvastutava töötlejana koos kindlustusandjaga. Kui teenusepakkuja määrab kindlaks andmetöötluse eesmärgid või vahendid, ei saa teda käsitada pelgalt tehnilise vahendajana. Sellisel juhul kaasneb talle iseseisev vastutus IKÜM-ist tulenevate kohustuste täitmise eest, sealhulgas läbipaistvuse, turvalisuse ja andmesubjekti õiguste tagamise osas.

Terviseandmete dünaamiline ja ajas muutuv edastamine kindlustusandjale tõstatab täiendava küsimuse proportsionaalsusest ja eesmärgipärasusest. Kui andmevahetus muutub pidevaks ning hõlmab ka käitumuslikke või näiteks nutiseadmetest pärinevaid andmeid, tuleb hinnata, kas selline ulatus on kooskõlas andmete minimeerimise põhimõttega. Kuigi inimese selgesõnaline nõusolek võib anda formaalse õigusliku aluse, ei kõrvalda see kohustust hinnata, kas töötlemine on tegelikult vajalik ja mõõdukas võrreldes kindlustuslepingu eesmärgiga. Samuti tuleb arvestada, et tervise infosüsteemides kogutud andmed on algselt kogutud tervishoiuteenuse osutamise eesmärgil. Nende kasutamine kindlustusrisi hindamiseks kujutab endast eesmärgi muutust, mille õiguspärasus tuleb hinnata IKÜM artikli 6 lõike 4 alusel ning katta selgesõnalise nõusolekuga artikli 9 tähenduses (antud hindamist käesoleva projekti skoobis läbi ei viidud).

Täiendava mõõtme annab automatiseeritud otsustamine ja profileerimine. Personaalse andmeruumi kaudu koondatud andmete põhjal võib kindlustusandja teha riskihindamise otsuseid, mis mõjutavad inimest märkimisväärselt, näiteks määrates kindlustusmakse suuruse või keeldudes lepingu sõlmimisest. Kui selline otsus põhineb üksnes automatiseeritud töötlusel, võib kohalduda IKÜM artiklis 22 sätestatud piirang, mis nõuab inimsekkumise võimalust ning otsuse vaidlustamise õigust. Seetõttu peab personaalse andmeruumi mudeli praktiline rakendamine sisaldama mehhanisme, mis väldivad täielikult automatiseeritud ja läbipaistmatuid otsuseid.

Arvestades eriliiki andmete ulatuslikku töötlemist ja võimalikku süstemaatilist profileerimist, on suure tõenäosusega vajalik andmekaitsealase mõjuhinnangu läbiviimine vastavalt IKÜM artiklile 35. Mõjuhinnang peab analüüsima riske andmesubjektide õigustele ja vabadustele

ning kavandama tehnilised ja organisatsioonilised meetmed nende riskide maandamiseks. See hõlmab muu hulgas tugevat autentimist, krüpteerimist, juurdepääsu piiranguid ja auditilogisid. Personaalse andmeruumi kontseptsiooni õiguslik teostatavus sõltub seega suuresti sellest, kas süsteem on üles ehitatud *privacy by design* ja *privacy by default* põhimõtteid järgides.

Kokkuvõttes ei ole personaalse andmeruumi teenuse rakendamine elukindlustuse valdkonnas kehtiva õiguse kohaselt sõnaselgelt välistatud. Samas on tegemist kõrgendatud andmekaitseriskiga töötlusmudeliga, mis eeldab täpset rollijaotust, selgelt piiritletud eesmärgi, tugevat tahteavalduste haldamise mehhanismi ning põhjalikku mõjuhinnaangut IKÜM art 35 mõttes. Samas toodi näiteks ühe kindlustusseltsiga läbiviidud intervjuus välja kitsaskoht, et terviseandmeid kui eriliiki isikuandmeid IKÜM art 9 mõttes saab töödelda selgesõnalise nõusoleku (*explicit consent*) olemasolul. Et tuua eriliiki isikuandmeid personaalse andmeruumi konteksti, võib olla vajadus uuendada ka kehtivat EL isikuandmete kaitse õiguslikku raamistikku (IKÜM art 9 lg 2). Praktikas sõltub personaalse andmeruumi teenuse õiguslik teostatavus sellest, kas suudetakse tagada, et andmetöötlus jääb proportsionaalseks, läbipaistvaks ja kontrollitavaks ning et inimese autonoomia oma andmete üle ei muutu pelgalt formaalseks, vaid on sisuliselt realiseeritav.

8.2 Oskuste ja haridusandmete põhine teenus

Oskuste ja haridusandmete põhine teenus on andmepõhine lahendus, mille eesmärk on toetada inimest kogu tema õpiteekonna ja karjääri vältel. Teenuse keskne komponent oleks inimese kompetentsiprofiil, mis sisaldab tema hariduskäiku, kvalifikatsioone, sertifikaate, töökogemust ning erinevaid oskusi. Võimalusel saaks kompetentsiprofiile täiustada ka inimese huvisid, eelistusi ning käitumuslikke tendentse kirjeldavate andmetega. Tegemist oleks masinloetava ja ajas uueneva andmekogumiga, mis võimaldab inimesel võrrelda oma teadmisi ja oskusi tööturu nõudlusega ning aidata tal kujundada personaliseeritud õpiradasid. Lisaks saaks antud teenust kasutada värbamisprotsessis, võimaldades inimesel jagada tööandjatele valideeritud kompetentsiprofiili ning tõendeid ning huvi korral saada ka värbamisteenuste poolt sobilikke töopakumisi.

Teenuse toimimiseks on vajalik mitmekesine ja laiaulatuslik andmetöötlus. Andmeid kogutakse Eesti Haridusinfosüsteemist (EHIS), riiklikust kutseregistrist, tööandjate süsteemidest ning vajadusel haridus- ja tööturuteenuseid osutavatelt teenusepakkujatelt. Lisaks formaalsetele ja tõendatud andmetele võiks süsteem töödelda ka õpitegevuse käigus tekkivaid andmeid (nt e-õppe platvormide logid, kursuste läbimise info), mis võimaldavad hinnata oskuste arengut ajas. Selline eeldab ühtseid standardeid, oskuste taksonoomiat ning kvaliteedikontrolli mehhanisme.

Praeguses olukorras on andmed erinevate asutuste vahel killustunud, sageli dubleerivad või aegunud. Inimesel puudub terviklik ülevaade oma oskustest ja kvalifikatsioonidest ning ta peab neid korduvalt eri osapooltele esitama. Kutsekoda on teinud siin suure hüppe edasi, töötades välja "Oskuste Kompassi" lahenduse, mille kaudu saab inimene koondada enda kohta kvaliteetseid oskus- ja haridusandmeid ning neid ka kolmandatele osapooltele soovitud ajaperioodiks jagada. "Oskuste Kompass" on sealjuures piiritletud peamiselt akrediteeritud

asutuste poolt väljastavate andmetega ning ei hõlma muid tõendeid ja käitumuslikke andmeid, mille hindamine väljakujunenud kompetentsiprofiilidega on suureks väljakutseks.

Tööandjate, karjäärinõustajate ja värbajate vaatest on kitsaskohaks, et värbamisega seonduvaid otsuseid tehakse piiratud ja ebaühtlase kvaliteediga info alusel, mis raskendab kandidaadi sobivuse hindamist. Samuti ei ole piisavalt arvestatud oskuste dünaamilise arenguga ega sellega, kuidas varasemad kogemused ja mitteformaalsed õpiteed võiksid toetada uut karjäärisuunda.

Personaalse andmeruumi lahendus võimaldaks inimesel koondada oma haridus- ja oskuste andmed ühtsesse keskkonda ning määrata selgelt, milliseid andmeid, kellele ja mis eesmärgil jagatakse. Teenus vahendaks inimese tahet andmevaldajate (nt EHIS) ja andmetarbijate (nt potentsiaalne tööandja või koolitusettevõtte) vahel, tagades, et andmekasutus vastab antud nõusolekutele ning õiguslikele nõuetele. See loob võimaluse pakkuda personaliseeritud õpiradasid, tuvastada oskuste puudujääke võrreldes soovitud ametiga, suunata inimeste erinevatesse õppeprogrammidesse või koolitustele ning võimaldada tööandjatele ligipääsu valideeritud ja ajakohasele kompetentsiprofiilile.

Antud kasutusloo puhul on väljakutseks nii standardiseeritud andmevahetuse ja ühise oskuste raamistiku tagamine, et eri süsteemid suudaksid omavahel koostalitleda. Õiguslikust ning eetilisest vaatenurgast tuleb maandada ka algoritmilise profileerimise ja võimaliku diskrimineerimise riskid ning tagada andmete minimeerimine ja läbipaistvus. Eriti tähelepanelikult tuleb käsitleda andmeid, mis võivad kaudselt viidata tundlikele asjaoludele (nt teovõime). Samas on antud kasutusloo puhul selge potentsiaal liikuda killustunud ja reaktiivsest tööturu- ja haridussüsteemist proaktiivse, andmepõhise ja inimese autonoomiat toetava teenusemodelini.

Peamine järeldus

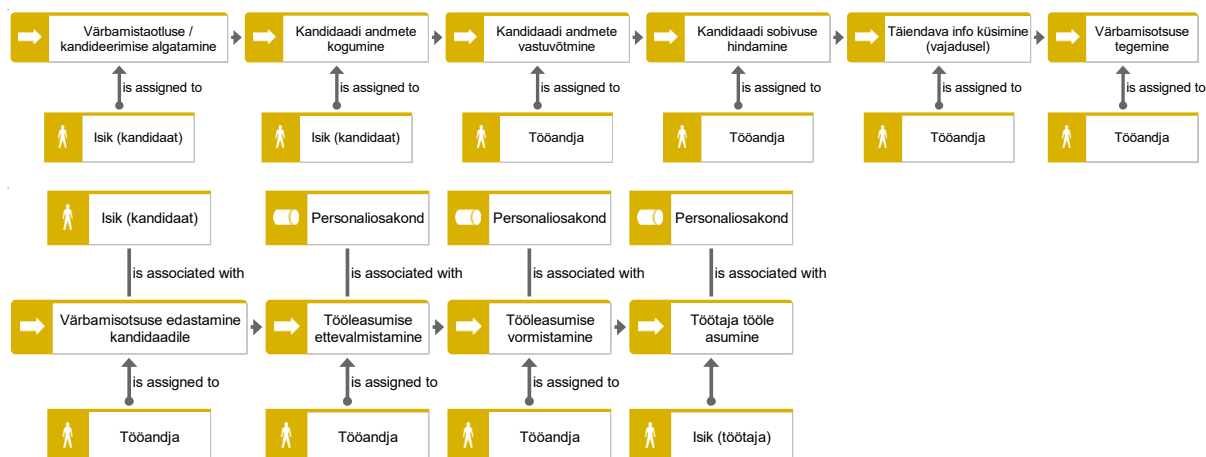
Oskuste Kompas rakenduse (ning isikliku Minu Kompas vaate) näitel on täna Eestis tekkimas personaalse andmeruumi prototüüp oskuste ja haridusandmete kontekstis, võimaldades inimesel koondada killustunud haridus- ja oskuste andmed ühtseks kompetentsiprofiiliks ning kujundada teadlikult oma haridus- ja tööelu. Samas on kitsaskohaks teiste andmete koondamine erasektori poolt pakutavatest teenustest ning oskusprofiili laiem kasutamine värbamisteenuste poolt. Peamisteks takistusteks näivad olevat erinevate andmemudelite kasutamine, väga suur hulk osapooli ning piiratud äriiline motivatsioon, mistõttu lahendus eeldab tugevat riiklikku rolli ja koostööpõhist mudelit.

8.2.1 Värbamise ja tööleasumise protsessi as-is ja to-be analüüs

Järgnevalt on analüüsitud töötajate värbamise ja tööleasumise protsessi põhietappe ning esitatud uuringu käigus kaardistatud as-is ning personaalse andmeruumi raamistikus võimalik to-be vaade. Lihtsuse huvides on kirjeldatud vaid inimese poolt tööle kandideerimise protsessi vaade, kuigi värbamisteenuste puhul on potentsiaali uurida ka võimalust, kuidas inimesed

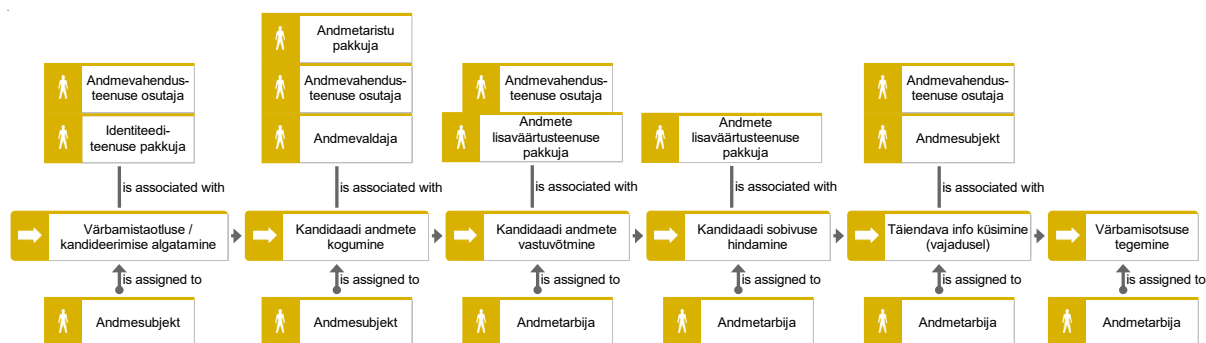
saaksid anda nõusoleku oma haridusliku ja oskuste profiili leidmiseks värbajate poolt, et nendega sobiva töövõimaluse korral ühendust võtta.

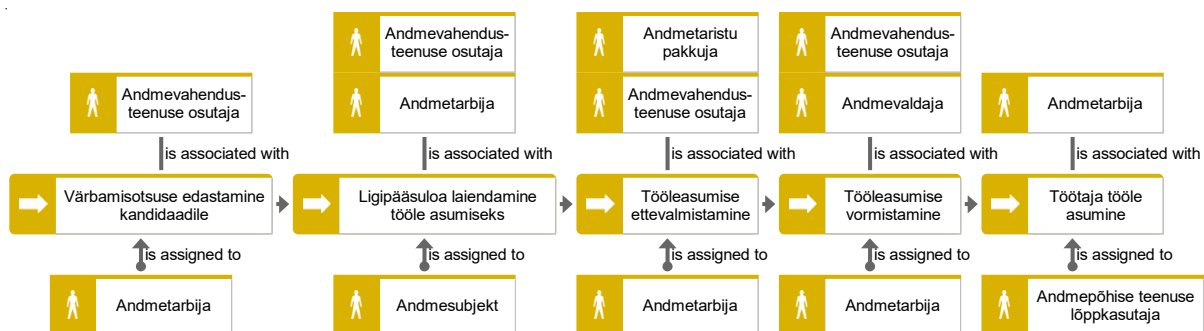
As-is vaates (vt Joonis 10) esitab kandidaat esitab oma andmedotse tööandjale ning andmete kontroll ja nende täiendamine toimub tööandja ja erinevate andmevaldajate vaheliste päringute või integratsioonide kaudu. Andmete kasutamist juhivad eelkõige tööandja sisemised protsessid, värbamispraktikad ja õigusaktidest tulenevad kohustused.



Joonis 10. As-is värbamise ja tööleasumise protsessi mudelid

To-be vaates (vt Joonis 11) võiks tööle kandideerija jagada personaalse andmeruumi rakenduse kaudu oma hariduse- ja oskuste profiili koos tõendatud andmetega masinloetaval kujul otse tööandjaga. Lisaks võib tööandja esitada personaalse andmeruumi rakenduse kaudu struktureeritud andmepäringuid vastavatele andmevaldajatele (kas otse kui selleks on olemas nt seadusega määratud õiguslik alus või küsida kõigepealt inimeselt nõusolekut andmete pärimiseks). Andmete kasutamine on seotud konkreetse värbamis- või töösuhte eesmärgiga ning on inimesele personaalse andmeruumi rakenduse kaudu jälgitav.





Joonis 11. *To-be* värbamise ja tööleasumise protsessi mudelid

Järgmiselt annab Tabel 4 ülevaate ärilisest kasust, mis võiks *to-be* vaatest tulla erinevate värbamise ja tööleasumise protsessi sammude lõikes Tabeli pesades kasutatakse järgmist värvilegend:

Suur parenduspotentsiaal	Mõõdukas parendus
--------------------------	-------------------

Tabel 4. *As-is* ja *to-be* protsesside kirjeldus värbamises ja tööleasumise faasis koos ärilise kasu potentsiaali avamisega

Protsessi samm	AS-IS	TO-BE	Parendus
Värbamis- taotluse / kandideerimise algatamine	Inimene (tööle kandideerija) esitab kandideerimiseks vajalikud andmed ning tööandja tuvastab tema identiteedi.		
	Sageli esitab inimene oma andmed CV ja motivatsioonikirjana e-posti teel, kuid esineb ka lahendusi, kus inimene algatab kandideerimise tööandja keskkonnas ning tuvastatakse organisatsiooni kasutusel olevate autentimis- ja kliendihalduslahenduste kaudu. Inimese vaates on kandideerimise algatamine seotud iga tööandja eraldi süsteemiga, mistõttu tuleb andmeid korduvalt esitada. Ettevõttele tähendab see suure hulga avalduste käsitsi ja ebaühtlast töötlemist. Seetõttu on protsess halvasti skaleeritav ning piirab standardiseeritud, andmepõhist ja masinloetavat käsitlust	Inimene autendib end identiteediteenuse pakkuja kaudu ning seob kandideerimise oma personaalse andmeruumiga. Identiteeti käsitletakse ühtse ja taaskasutatava identiteedikontekstina, mis võimaldab inimesel osaleda erinevates kandideerimisprotsessides ilma korduva tuvastamiseta. Inimese vaates väheneb killustumine ning kandideerimise algatamine ei ole seotud ühe konkreetse tööandja süsteemiga. Ettevõtte vaates toetab see suure hulga avalduste ühtlasemat, andmepõhisemat ja paremini skaleeritavat käsitlemist.	Väheneb vajadus dokumentide eraldi esitamiseks ning paraneb identiteedi ja pädevuste usaldusväärne tuvastamine.
Kandidaadi andmete kogumine	Tööandja kogub inimese kohta andmeid (tõendeid), et neid analüüsida ja teha värbamisotsus.		
	Andmete kontroll ning analüüs toimub sageli käsitsi ja esitatud dokumentide põhjal. Inimesel puudub selge ülevaade, milliseid andmeid kasutatakse ning kuidas.	Inimese haridus- ja kvalifikatsiooniandmed koondatakse andmevaldajate (nt registrite) kaudu ning edastatakse tööandjale ainult vajalikus ulatuses standardiseeritud andmevahetuse kaudu. Inimene saab anda ligipääsu oma andmetele ning jagada neid kontrollitult konkreetse värbamise eesmärgil.	Väheneb manuaalne andmete kogumine ning paraneb andmete ajakohasus ja usaldusväärsus.
	Tööandja kontrollib ja registreerib kandidaadi esitatud andmed.		

Kandidaadi andmete vastuvõtmine	Tööandja hindab dokumentide autentsust ja vastavust ning kasutab neid värbamisotsuse tegemiseks. Andmete kasutamine on sageli piiratud organisatsiooni siseste protsessidega. Kandidaadi vaates jääb sageli ebaselgeks, kuidas tema andmeid hinnatakse ja kasutatakse.	Tööandja esitab struktureeritud andmepäringu ning kandidaadi andmete kasutamine toimub nõusoleku või muu õigusliku aluse alusel. Andmete edastamine toimub turvaliste andmevahendusteenuste kaudu. Kandidaadi vaates on andmete kasutus selgem ja jälgitavam.	Paraneb andmekasutuse kontroll ja vastavus nõusolekutingimustele.
Kandidaadi sobivuse hindamine	Tööandja hindab kandidaadi sobivust tööandja vajaduste ja ametikoha nõuete alusel.		
	Sobivuse hindamine põhineb esitatud dokumentidel ja värbamisintervjuudel. Andmete kvaliteet ja võrreldavus võivad varieeruda.	Sobivuse hindamisel kasutatakse usaldusväärseid ja struktureeritud andmeid, mis on saadud personaalse andmeruumi kaudu ning vajadusel analüütilisi või kompetentsimudeleid.	Paraneb otsuste kvaliteet ja võrreldavus.
Täiendavate andmete kasutamise nõusolek	Täiendavate andmete kasutamiseks peab tööandjal olema õiguslik alus.		
	Nõusolek täiendavate andmete kasutamiseks küsitakse sageli üldisel kujul või eraldi dokumentide kaudu. Kandidaadi vaates võib jääda ebaselgeks, milliste andmete kasutamiseks nõusolek anti.	Andmete kasutamine toimub konkreetse eesmärgi ja ajapiiranguga nõusoleku alusel personaalse andmeruumi kaudu. Kandidaadi vaates on võimalik anda ja hallata nõusolekuid täpsemalt ning jälgida nende kasutamist.	Andmekasutus muutub eesmärgipõhiseks ja paremini kontrollitavaks.
Täiendava info küsimine	Tööandja võib küsida täiendavaid andmeid või dokumente.		
	Tööandja küsib kandidaadilt täiendavaid dokumente või teeb päringuid registritesse. Kandidaadi vaates tähendab see sageli dokumentide korduvat esitamist.	Vajalikud andmed saadakse kandidaadi loal personaalse andmeruumi kaudu registritest või andmevaldajate süsteemidest. Kandidaadi vaates väheneb vajadus dokumente ise koguda ja edastada.	Väheneb halduskoormus ning paraneb andmete kasutamise läbipaistvus.
Värbamisotsuse tegemine	Tööandja teeb kogutud andmete põhjal värbamisotsuse.		

	Otsus tehakse organisatsiooni süsteemides ning andmete kasutamine ja otsuse alused ei ole kandidaadile alati nähtavad. Kandidaadi vaates jääb otsuse kujunemine sageli läbipaistmatuks.	Otsus tehakse samuti tööandja süsteemides, kuid kasutatud andmed pärinevad kontrollitud allikatest ja nende kasutus on jälgitav. Kandidaadi vaates on võimalik paremini mõista otsuse aluseks olnud andmeid.	Suureneb otsuse läbipaistvus ja usaldus.
Värbamisotsuse edastamine	Kandidaadile edastatakse otsus.		
	Kandidaati teavitatakse otsusest e-posti või värbamissüsteemi kaudu. Andmete kasutus jääb kandidaadile suuresti nähtamatuks.	Kandidaat saab personaalse andmeruumi kaudu näha, milliseid andmeid otsuse tegemisel kasutati ning otsuse kinnitamine võib toimuda identiteediteenuse kaudu.	Paraneb otsuse läbipaistvus ja jälgitavus.

Tööleasumise protsessis ei muutu äriprotsessi sammud, kuid andmete kogumine ja kasutamine muutub personaalse andmeruumi kaudu läbipaistvamaks, eesmärgipõhisemaks ja paremini jälgitavaks.

Protsessi samm	AS-IS	TO-BE	Parendus
Tööleasumise ettevalmistamine	Tööandja kogub töötajalt töölepingu sõlmimiseks ja tööle asumiseks vajalikud andmed ning valmistab ette töötamisega seotud administratiivsed toimingud.		
	Tööandja kogub töötajalt vajalikud andmed ning sisestab need erinevatesse infosüsteemidesse. Andmeid registreeritakse mitmes süsteemis eraldi ning andmete haldus toimub tööandja süsteemides. Töötaja vaates tähendab see sageli samade andmete korduvat esitamist ning puudub terviklik ülevaade, kus ja kuidas tema andmeid kasutatakse.	Tööandja alustab tööleasumisega seotud andmetöötlust personaalse andmeruumi kaudu. Ligipääsuõigused ja vajalikud andmed koondatakse töötaja volitatud andmeallikatest ning kasutatakse tööleasumise ettevalmistamiseks. Töötaja vaates väheneb vajadus samu andmeid korduvalt esitada ning tal on parem ülevaade oma andmete kasutamisest.	Väheneb andmete korduv sisestamine ning paraneb andmete haldamine.
Töösuhte vormistamine	Töösuhte vormistatakse vastavalt õigusaktidele ning vajalikud andmed edastatakse riiklikele registritele ja süsteemidele. Töösuhte loomisel määratletakse selgelt edasiste andmete kasutamise eesmärk ja õiguslik alus (nt lepingu täitmine või seadusest tulenev kohustus).		

	Tööandja registreerib töötaja maksu- ja sotsiaalkindlustuse süsteemides. Andmete edastamine toimub tööandja infosüsteemide kaudu deklaratsioonide või päringute abil. Töötaja vaates ei ole sageli selge, milliseid andmeid tööandja erinevatesse süsteemidesse edastab.	Registreerimistoimingud tehakse standardiseeritud andmevahetuse kaudu. Töötaja vaates on andmete kasutamine ja edastamine paremini jälgitav.	Paraneb andmevahetuse jälgitavus ja õiguslik selgus.
Töötaja tööle asumine	Inimene (töötaja) alustab tööülesannete täitmist ning kasutab organisatsiooni infosüsteeme vastavalt oma rollile.		
	Töötaja andmeid kasutatakse organisatsiooni sisestes süsteemides vastavalt tööandja protseduuridele. Töötaja vaates puudub sageli terviklik ülevaade, millistes süsteemides tema andmeid kasutatakse.	Töötaja vaates on võimalik oma andmete kasutust paremini mõista ja kontrollida personaalse andmeruumi rakenduse kaudu.	Suureneb andmekasutuse läbipaistvus ja töötaja kontroll oma andmete üle.

As-is mudelis põhineb värbamisprotsess peamiselt dokumentide esitamisel ning tööandja poolt eraldiseisvate registripäringute tegemisel. Kandidaadi andmed paiknevad erinevates süsteemides ning nende õigsus ja ajakohasus sõltuvad sageli esitatud dokumentidest ja tööandja täiendavast kontrollist. Andmekasutust käsitletakse protsessipõhiselt ning üksikuid andmepäringuid ei seota eraldi nende eesmärgi, kestuse ega kasutusulatusega.

To-be mudelis muutub andmekasutuse juhtimismudel, kus andmevahetus toimub personaalse andmeruumi usaldusraamistikus. Andmepäringud on seotud konkreetse eesmärgi ja ajapiiranguga ning andmesubjektil on võimalik näha, milliseid andmeid värbamisprotsessis kasutatakse ja millisel eesmärgil. Selle tulemusena muutub andmekasutus läbipaistvamaks ja kontrollitavamaks, säilitades samal ajal tööandja vastutuse värbamisotsuste tegemisel. Ettevõtete jaoks vähendab see halduskoormust, parandab andmete võrreldavust ning kiirendab värbamisprotsessi.

8.2.2 Rollimudel ja osapoolte kaardistus

Tabel 5. Hüpoteetiline osapoolte kaardistus tööleasumist soodustava oskuste ja haridusandmete põhise teenuse puhul, kasutades personaalse andmeruumi rollimudelit. Antud rollijaotust pole mainitud osapooltega valideeritud, mistõttu rollide ja osapoolte jaotus võib praktikas erineda.

Roll / Osapool	Peamised võimalikud osapooled
Andmesubjekt kui andmeomanik	Inimene (nt persoonina „Malle“)
Andmetarbija	Tööandja
Andmevaldaja	Haridus- ja Teadusministeerium, Kutsekoda, Maksu- ja Tolliamet
Andmepõhise teenuse lõppkasutaja	Inimene (nt persoonina „Malle“)
Andmevahendusteenuse osutaja	RIA (X-tee), aga võimalikud ka teised osapooled (nt tehnoloogiaettevõtted)
Andmetaristu pakkuja	RIA (X-tee, kui tehniline andmevahetuse taristu), Telia Eesti AS, Elisa Eesti AS, Tele2 Eesti AS (sidekanal ja SIM Mobiil-ID jaoks), IT-majad, vajadusel teised tehnoloogiapartnerid.
Identiteediteenuse pakkuja	SK ID Solutions (Smart-ID, Mobiil-ID autentimis- ja sertifitseerimisteenus); Zetes Estonia OÜ; RIA (TARA, digikukkur);
Andmete lisaväärtusteenuse pakkuja	Kutsekoda, värbamisteenused, aga ka tehnoloogiaettevõtted (nt AI-lahenduste pakkujad)
Andmeökosüsteemi haldusorganisatsioon	RIA (X-tee), Justiits- ja digiministeerium, Haridus- ja Teadusministeerium
Sertifitseerimis- ja järelevalveasutus	SK ID Solutions, AKI, Tööinspeksioon

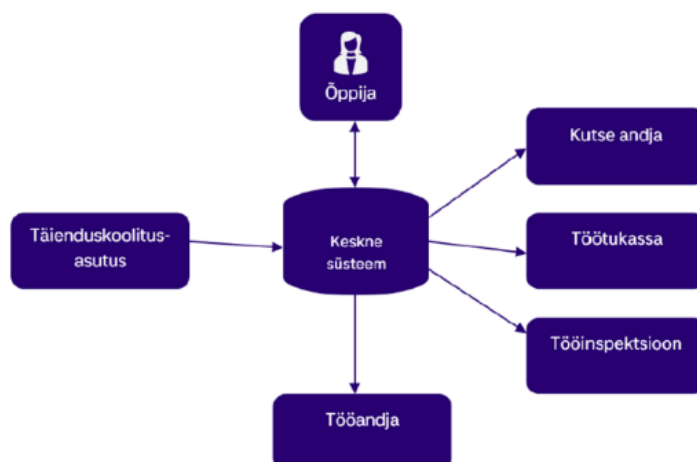
8.2.3. Äriline vaade

Intervjuude põhjal ei pruugi haridusteenustele keskenduv platvorm end Eesti väikse turu tõttu ära tasuda. Suurtel turgudel (nt USA) võivad isegi alustavatel haridusplatvormi ettevõtetel olla tugevamad ärimudelid kui siinsetel kohalikel väljakujunenud ettevõtetel. Need ettevõtted, kes suudavad edukalt laieneda võimalikult varakult Eestist välja, võivad suuta tagada piisava käive, millega äri kasvatada ning üle 10 aasta vastu pidada. Samas, liigne sõltuvus Eesti digiriigi unikaalsest taristust (isikukood, eID, X-tee) on laienemisel keeruline, kuna teenused peavad igal poolt töötama. Osa haridusteenuste eksperte pakkus välja ka radikaalsemaid lahendusi: selle asemel, et riiklikult suuri infosüsteeme arendada, võiks andmevahetuse muuta transaktsioonipõhiseks ja maksta neile, kes pakuvad väärtuslikke andmeid.

Printsiibis on ka nõusoleku paindlikult tagasivõtmine turuosalistele arusaadav, aga ärilisest perspektiivist väikestele haridusettevõtetele pigem keeruline – tegutsetakse vaevalt kasumi piiril, suutes töötajatele vaevu palka maksta. Lisasüsteemide ehitamine on kallid ja seda pigem tehakse ainult siis kui selleks on regulatiivne nõue. Mitmed haridustehnoloogia äriideed on ka pikemalt inkubatsioonistaadiumis – juriidilist keha veel omamata (mis luuakse siis kui äritegevus päriselt omab potentsiaali).

Intervjuudest tuli ka välja, et tööturuteenuste vaates on Eesti Maksu-ja Tolliametil üsna kvaliteetne ülevaade töötajatega seotud andmetest (töötamised, töötasud, koormused), mis võib olla vajalik info ka näiteks töötaja tööleasumisel ja/või juba töötamisel (eriti mitme töökoha puhul), aga see pole realiseerunud tõenäoliselt nii isikuandmete jagamise kui ärimudeli/investeeringu tõttu.

TietoEvry viis 2022. aastal Haridusministeeriumi tellimusel täiskasvanute täiendkoolituse e-tunnistuste analüüsi¹⁹, milles on ka põhimõtteline viide personaalse andmeruumile: „õppija peab ise saama määrata, kas tema tunnistus on avalik, ja kellega ta seda jagab.“ Põhimõtteliselt on eesmärk selline, mis võimaldab keskse süsteemi kaudu võtta sisendiinfot täienduskoolituseasutustelt ning õppijalt endalt ning anda sellele vastavalt õigusele ligipääs õppijale, tööandjale, kutse andjale, töötukaasale, tööinspeksioonile.



Joonis 12. Allikas: TietoEvery Täiskasvanute täiendkoolituse e-tunnistuste analüüs

Viidatud analüüsis hinnati antud keskse süsteemi maksumuseks ligikaudu 275 000 eurot ja teostatavusajaks u 3-5 aastat. Tõsi, selle eeldus on, et väga paljud erinevad täiendkoolituse pakkujad liituvad sellega kohustuslikus korras, kolmes etapis:

1. EHISes registreeritud täiendkoolitusasutused (ca 1200-1400), mis väljendavad selliseid tunnistusi, mis on õppijale kohustuslikud näiteks kutse taotlemiseks või oma ametikohal töötamiseks.
2. Teises etapis liidestuksid kõik teised EHISes registreeritud täiendkoolitusasutused.
3. Kolmandas etapis saaks tunnistuse haldamise keskse süsteemi liidestada välise infosüsteemidega.

Samuti on oluline sätestada andmevahetuseks kohustuslikud andmekomponendid, korrastatud struktuuriga – mis on omakorda suur väljakutse, kuna paljud täiendharidust pakuvad asutused on väikeettevõtjad, erinevate infokogumise, töötlemise ja edastamise oskustega. Ärimudeli mõttes töötaks see tõenäoliselt peamiselt riikliku või riigi poolt tellitud/rahastatud infosüsteemina – erasektoril tõenäoliselt sellise väikese mahu ja nõudlusega avaliku huve teenindava teenuse pakkumise osas aktiivset huvi ei ole.

Kokkuvõttes on see tõenäoliselt infosüsteemi investeeringuna piisavalt jõukohane riigile, aga kuna see eeldab liidestumist tuhandete väikeettevõtjatest täiendkoolitusasutuste poolt mitme aasta jooksul, võib see osutuda keeruliseks. Üalaltoodud põhjustel ei ole oskuste ja haridusandmete ärimudeli veel tugevat potentsiaali äriliseks andmevahetuseks. Mitteäriine andmevahetus on ärimudeli jaoks oluline kindlasti riiklike andmete kaasamisel (nii avaandmetena kui ka näiteks x-tee kaudu). Samuti on tõenäoline ettevõtete ja organisatsioonide omavaheline andmevahetus, mille eest tasu ei võeta.

Tabel 6. Autorite poolne hinnang andmealase koostöö mudelite sobivusele antud kasutusloos.

Mudel	Kommentaar
Äriandmed	Teistelt ettevõtelt või organisatsioonidelt ärilisel eesmärgil (x2B) andmete ost-müük - pigem ei.
Andmeturg	Laiem andmete ost-müük (nt platvormi kaudu) - pigem ei, kuigi mõnes valdkonnas võib perspektiivi olla.
As-a-Service mudel	Andmete kvaliteet ja analüüs välise ärilise teenusena – pigem ei.
Avatud andmed / andmete annetamine	Teistelt ettevõtete või organisatsioonidega (x2B) andmete vahetamine – pigem jah.
Pragmaatiline / ad-hoc andmete jagamine	Riigilt või teistelt organisatsioonidelt andmete saamine (x2B) töötab kindlasti – näiteks andmevahetusena X-tee kaudu.
Usaldusväärne kolmas osapool (vahendaja)	Teistelt ettevõtete või organisatsioonidega (x2B) andmete vahetamine – pigem jah.
Isikuandmete vahendaja	Mingil määral, potentsiaali on.
Andmeühistu / andmekooperatiiv	Pigem ei (võib-olla uute lahenduste korral).

8.2.4. Tehnoloogiline vaade

To-be vaates on antud kaasust kirjeldatud ka võimaliku tehnoloogilise arhitektuuri kaudu. Protsess algab kandidaadi autentimisest tööportaali või tööandja teenuses riikliku e-identiteedi lahenduse kaudu. Autentimistulemus edastatakse personaalse andmeruumi identiteedihaldusele standardsete identiteedi- ja autoriseerimisprotokollide kaudu. Identiteedihaldus ei teosta autentimist ise, vaid kasutab olemasolevate identiteediteenuste poolt väljastatud turvamärgendi infot, seob selle konkreetse rolli ja päringukontekstiga ning varustab teised tuumakomponendid usaldusväärse identiteedikontekstiga. Identiteet ei ole seotud üksnes tööandja sisese kasutajakontoga, vaid toimib teenuste ülese ja taaskasutatava identiteedikihina.

Tööandja süsteem tegutseb andmetarbijana ning esitab personaalse andmeruumi API kaudu masinloetava andmevajaduse kirjelduse. Päring sisaldab taotletavaid andmekategooriaid, kasutuseesmärki, ajapiirangut ning päringu algataja identiteeti ja rolli. Enne andmete edastamist hindab nõusoleku haldus päringu konteksti ning teeb otsuse andmekasutuse lubatavuse kohta. Inimene annab ligipääsuloa kasutajaliidese kaudu eesmärgipõhiselt ja ajaliselt piiratud ulatuses. Nõusoleku haldus ei edasta andmeid ega suhtle registritega, vaid tagastab masinloetava otsuse, mis võimaldab või keelab päringu täitmise.

Lubava otsuse korral käivitub andmevahendaja, mis toimib otsuse jõustamise punktina. Andmevahendaja edastab päringu vastavasse riiklikku registrisse, näiteks EHIS-esse, kasutades riiklikku andmevahetuskihti. Registrid tagastavad kontrollitud ja ajakohased andmed, mis edastatakse tööandja süsteemile kokkulepitud formaadis ja mahus. Andmevahendaja ei talleta andmeid pikaajaliselt ega muuda nende sisu, vaid vahendab need kooskõlas nõusoleku halduse otsusega.

Kõik päringu ja andmeedastusega seotud sündmused edastatakse audit- ja logimiskomponendile. Logikirjed seovad omavahel päringu algataja identiteedi, nõusolekuotsuse, ajamärgid ja andmeedastuse fakti, võimaldades rekonstrueerida kogu andmepäringu elutsükli. Audit ei sisalda algandmeid, vaid viiteid sündmustele ja otsustele, tagades tõendatavuse ilma kesket andmeladu loomata. Personaalse andmeruumi vaade koondab nõusolekute seisu ja andmekasutuse ajaloo ning võimaldab inimesel näha, kes ja millisel eesmärgil tema andmeid kasutas.

Värbamisotsuse järel algab tööleasumise samm, kus andmetöötluse kontekst muutub. Töösuhte vormistamiseks võib tööandja kasutada samu registriandmeid uue eesmärgi alusel, kuid see eeldab eraldi määratletud ligipääsuluba või seadusest tuleneva töötlemisaluse rakendamist. Töötaja registreerimine Maksu- ja Tolliameti süsteemis ning muud kohustuslikud registritoimingud põhinevad õigusaktidest tuleneval kohustusel, mitte nõusolekul. Tehnoloogiliselt viiakse need toimingud läbi tööandja infosüsteemidest, kuid nende toimumine ja ajastus on personaalse andmeruumi auditi kaudu jälgitav.

Töösuhte algusega tekib uus andmetöötluse kontekst, kus andmete kasutamine jätkub seadusest ja lepingust tulenevate eesmärkide alusel, sh värbamisprotsessi käigus antud ligipääs ei laiene automaatselt tulevastele töötlemise eesmärkidele.

Tehnoloogilises plaanis, kui on olemas äriiline huvi, on lahendus realiseeritav.

8.2.5. Õiguslik vaade

Alljärgnev analüüs käsitleb oskuste ja haridusandmete põhise teenuse kasutusjuhtu, võrreldes kehtivat (*as-is*) ja kavandatavat (*to-be*) õiguslikku mudelit.

Praeguses olukorras paiknevad haridus- ja oskuste andmed eri andmekogudes ja infosüsteemides, näiteks Eesti Hariduse Infosüsteem (EHIS), kutseregister ning tööandjate infosüsteemid. Kvalifikatsioonisüsteemi arendamise ja kutseregistri pidamise eest vastutab SA Kutsekoda, kes on loonud ka "Oskuste Kompassi" lahenduse kui ühe kesksema oskuste andmete koondamise vahendi. Selles veebikeskkonnas on igal kasutajal võimalik luua enda isiklik oskuste profiil, mida nimetatakse „Minu Kompass“-iks.

Õiguslikult peab isikuandmete töötlemine iga andmevaldaja (vastutav töötleja) tasandil toimuma vastavalt IKÜM nõuetele. Haridusasutused, registripidajad ja tööandjad tegutsevad iseseisvate vastutavate töötlejatena ning määravad andmete töötlemise eesmärgid ja vahendid oma pädevuse piires. Andmete kasutamine värbamisel või õpiradade kujundamisel võib tugineda lepingu sõlmimisele eelnevatel toimingutel (IKÜM art 6 lg 1 p b), seadusest tuleneval kohustusel (p c) või õigustatud huvil (p f).

Inimese tööle värbamine toimub õiguslikust vaatest eraõigusliku töösuhte loomise kaudu, mille keskmes on töölepingu sõlmimine tööandja ja töötaja vahel (avalikus sektoris peab lisaks arvestama ka sellega, et kohaldub avaliku teenistuse seadus²⁰). Värbamisprotsess algab tavaliselt tööpakkumise avaldamisest ja kandidaatide hindamisest, mille käigus tuleb järgida võrdse kohtlemise ja andmekaitse põhimõtteid. Töösuhte tekib töölepingu sõlmimisega ning seda reguleerib eeskätt töölepingu seadus²¹, mis sätestab töölepingu vorminõuded, poolte õigused ja kohustused, töö- ja puhkeaja regulatsiooni ning vastutuse alused.

Eestis ei toimu töö tegemine üksnes töölepingu alusel, vaid sõltuvalt suhte sisust ja eesmärgist võib kasutada ka muid võlaõiguslikke lepinguvorme. Klassikaline alluvussuhtel (subordinatsiooni) põhinev töösuhe tekib töölepingu sõlmimisega ning seda reguleerib töölepingu seadus. Kui aga inimene osutab teenust iseseisvamalt ning puudub tööandja juhtimis- ja kontrollisuhe, võib õigussuhte aluseks olla käsundusleping või töövõtuleping, mida reguleerib võlaõigusseadus.

IKÜM-i vaates peab tööandjal olema kõikide värbamisprotsessis töödeldavate isikuandmete jaoks olema selge õiguslik alus. Tööle kandideeriva inimese andmete küsimisel ja töötlemisel ei ole peamiseks aluseks üldjuhul nõusolek, vaid muud IKÜM artiklis 6 sätestatud alused. Esiteks võib värbamisel õiguslikuks aluseks olla lepingu sõlmimisele eelnevate toimingute tegemine inimese taotlusel (IKÜM art 6 lg 1 p b). Kandideerimine on käsitatav sammuna võimaliku töölepingu sõlmimise suunas ning tööandjal on õigus küsida andmeid, mis on vajalikud kandidaadi sobivuse hindamiseks ja lepingu sõlmimise otsustamiseks. Teiseks võib töötlemine värbamisel tugineda tööandja õigustatud huvile (IKÜM art 6 lg 1 p f), näiteks vajadusele hinnata kandidaadi kvalifikatsiooni. Sellisel juhul tuleb vastutaval töötlejal (tööandja) või vastutava töötleja poolt volitatud andmetöötlejal (värbamisagentuur) läbi viia õigustatud huvi hindamine ning tagada, et kandidaadi põhiõigused ei kaalu üles tööandja huve. Kolmandaks võib teatud juhtudel olla aluseks juriidilise kohustuse täitmine (IKÜM art 6 lg 1 p c), näiteks kui seadus nõuab enne tööle võtmist isikuandmete töötlemist (nt karistusregistri kontrolli).

Eriliigiliste isikuandmete (nt terviseandmed) töötlemine on värbamisprotsessis üldjuhul keelatud, välja arvatud juhul, kui esineb IKÜM artiklis 9 sätestatud erand, näiteks tööõigusest tulenevate kohustuste täitmine või selgesõnaline nõusolek, kui see on konkreetsetes asjaoludes tööpoolest vabatahtlik.

Seega peab tööandja värbamisprotsessis lähtuma andmete minimaalsuse, eesmärgipärasuse ja läbipaistvuse põhimõtetest (IKÜM art 5 põhimõtted) ning siduma iga küsitava andmekategooria konkreetse ja põhjendatud õigusliku alusega.

Kuigi indiviidil (andmesubjektil) on IKÜM-ist tulenevad õigused (juurdepääs, parandamine, kustutamine, töötlemise piiramine), ei pruugi need realiseeruda as-is vaates koondatud ja dünaamilise kontrollina. Andmete jagamine toimub pigem üksikute teenussuhete raames ning nõusolek või muu õiguslik alus ei ole tehniliselt granulariseeritud iga konkreetse andmepäringu tasandil. Seetõttu on toimiv süsteem õiguspärane, kuid killustunud ning ei pruugi toetada maksimaalsel määral inimese informatsioonilist enesemääramisõigust ega andmete korduskasutusega kaasnevat andmete koordineeritud ja läbipaistvat kasutamist.

Kavandatavas mudelis lisanduks andmevaldajate ja andmetarbijate juurde personaalne andmeruum, mille keskmes oleks masinloetav ja ajas uuenev kompetentsiprofiil. See koondaks andmeid potentsiaalselt EHIS-est, riiklikust kutseregistrist, tööandjate süsteemidest ning vajadusel ka õpitegevuse käigus tekkivatest andmetest (nt e-õppe platvormide logid). Teenus ei asendaks algseid andmekogusid, vaid toimiks potentsiaalselt omalaadse andmete talletamise ja/või vahendamise kihina, mis võimaldab andmete struktureeritud koondamist ja jagamist indiviidi (andmesubjekti) enda määratletud ja kontrollitud tingimustel.

Õiguslikult tähendaks see, et personaalse andmeruumi teenus võtaks rolli, kus teenus tehniliselt jõustaks indiviidi (andmesubjekti) tahte ja andmete kasutamise tingimused. Sõltuvalt arhitektuurist võiks teenusepakkuja olla iseseisev vastutav töötleja kompetentsiprofiili kujundamise ja ligipääsu halduse osas, samas kui algsed andmevaldajad (nt EHIS või kutseandmete registrid) jääksid vastutavaks töötlejaks oma andmekogude pidamisel.

Asjassepuutuvaks õigusaktiks antud kasutusjuhu kontekstis võib pidada ka tööturumeetmete seadust²², mille eesmärgiks § 2 kohaselt on vähendada töötust ja lühendada selle kestust, ennetada töötust ning toetada tööhõives püsimist ja kvaliteetset tööhõivet, suurendada tööjõu pakkumist ning toetada kaasavat ja kohanemisvõimelist tööturgu ja majanduse struktuurimuutusi tööturumeetmete abil.

To-be mudelis muutuks andmekasutuse juhtimine institutsioonikeskselt isikukeskseks. Indiviid (andmesubjekt) saaks määrata, milliseid andmeid, millisele tööandjale või koolitusettevõttele ning mis eesmärgil jagamisele kuuluks. Kindlasti on oluline, et igasugune andmetöötlus tugineks korrektsele õiguslikule (nt kandideerimisel lepingu sõlmimisele eelnev toiming) ning et andmete töötlemine realiseeruks eesmärgipõhiste ja ajaliselt piiratud ligipääsulubadena. Kui andmeid kasutatakse väljaspool konkreetset kandideerimisprotsessi (näiteks tööpakkumiste soovitamiseks või personaliseeritud õpiradade loomiseks) tuleb edaspidises analüüsis hinnata, kas sobivaks aluseks on inimese nõusolek või teenuse osutamise leping.

Olulise lisamõõdme annab algoritmiline analüüs ja profileerimine, mida kasutatakse oskuste võrdlemisel tööturu nõudlusega või sobivate tööpakkumiste soovitamisel. Selline tegevus võib endast kujutada profileerimist IKÜM mõttes²³ ning võib teatud juhtudel mõjutada inimese õigusi või võimalusi tööturul. Seetõttu peab süsteem tagama läbipaistvuse, selgitusvõimaluse ning vajadusel inimsekkumise otsustusprotsessis. Samuti tuleb maandada kaudse

diskrimineerimise riskid, eriti kui kompetentsiprofiili täiendatakse huvide, eelistuste või käitumuslike andmetega, mis võivad kaudselt viidata tundlikele asjaoludele.

Teostatavusuuringu vaates ei seisne peamine õiguslik väljakutse uute materiaalõiguslike aluste loomises, vaid olemasolevate normide, eelkõige IKÜM-i rakendamises keerukas, mitme osapoolega ja sektoriüleses andmeökosüsteemis. Kui rollijaotus, vastutus ja õiguslikud alused on selgelt määratletud ning profileerimise ja diskrimineerimisriskide maandamiseks on rakendatud piisavad tehnilised ja organisatsioonilised meetmed, on personaalse andmeruumi põhine oskuste- ja haridusandmete teenus suures plaanis kooskõlas kehtiva õigusega ning võib tugevdada inimese autonoomiat tööturu- ja haridussüsteemis. Samas ei saa tulevikus välistada vajadust uute õiguslike aluste loomise järele õigusaktide tasandil, sõltuvalt lõplikult valitud teenuse- ja tehnoloogialahendusest.

9. Personaalse andmeruumi arengu võimalused

Personaalse andmeruumi kontseptsioon ja praktiline rakendus on alles välja kujunemas, koos esimeste kasutuslugude uurimise, katsetamise ja valideerimisega. Sellises dünaamilises keskkonnas ei ole **antud uuringus esitatud kontseptsioon ning kasutuslood lõplikud ning personaalse andmeruumi raamistik sõltub mitmetest paralleelselt arenevatest aspektidest**, nagu ettevõtete ärilisest huvist nõusoleku ja/või tahteavalduste põhiste andmete järgi ning innovatsioonist väärtusloome mudelite ning andmealaste koostöömudelite suunal.

9.1 Nõusolekupõhisus ja/või privaatsust kaitsvate tehnoloogiate laiem rakendamine

Praegune personaalse andmeruumi kontseptsioon eeldab **nõusoleku- ja/või tahteavalduse põhist lähenemist**, mis on osaliselt teostatav näiteks riikliku andmenõusolekuteenusu laiendamise kaudu. Paraku on selle skaleerimine keeruline ja kallis, mida kinnitab riiklike registrite vähesus, millega seni andmenõusolekuteenus on liidestatud (vt ka 9.2) ning erasektori kasin huvi sellist teenust omal algatusel käivitada – näiteks pangad ei ole loonud andmenõusolekuteenusle sarnast lahendust teistest pankadest andmete pärimiseks.

Kui inimene soovib eluasemelaenu, saab ta kasutada andmenõusolekuteenust EMTA andmete (näiteks viimase aasta palgatulu ja saadud muu tulu) edastamiseks pangale – inimene saab soovi korral jälgida, millisele organisatsioonile (nt pank) nõusolek on antud, kui kaua andmete kasutamise õigus kehtib ning tal on võimalus nõusolek tagasi võtta eesti.ee/nõusolek keskkonnas. Samas soovivad pangad eluasemelaenu pakkumisel saada infot ka kõigi teiste pangakontode väljavõtete kohta. Kuna eluasemelaenu on inimeste jaoks üks olulisemaid finantstehinguid kogu elu jooksul, on tavaline, et pakkumist küsitakse mitmest pangast, mitte ainult kodupangast. Antud juhul inimene küll annab nõusoleku andmete edastamiseks ühest pangast teise, aga tal puudub efektiivne võimalus seda tagasi võtta ning samuti puudub võimalus näha, kellele see nõusolek on antud ning kui kauaks. Lisaks kasutavad pangad osaliselt ka kolmandate osapoolte teenuseid pangakontode info töötlemiseks – mis teeb inimese perspektiivist arusaamise, mida tema privaatsete andmetega tehakse, raskemini jälgitavaks. Kuna üldiselt on pangakontode info väga sensitiivne (kui palju ja kust inimene raha saab, kellele ta ülekandeid teeb, millistest poodides ja teenuspakkujate juures ta millal käib, kui palju ta reisib jne), siis üldiselt inimesed seda infot teistega jagada ei soovi (isikliku pangakonto väljavõtet ei jagata näiteks kolleegide, sõprade ega sageli ka pereliikmetega), aga eluasemelaenu saamiseks tuleb seda jagada teiste pankadega ja teinekord ka väliste ettevõtetega - ilma selleta protsess ei tööta. Kui inimene näiteks antud pangast eluasemelaenu ei võta, puudub tal efektiivne võimalus enda pangakontosid puudutav andmenõusolek koheselt lõpetada. Kui juba suured ja kasumlikud pangad ei soovi omal algatusel sellesse investeerida, siis näiteks intervjueritud haridussektori platvormiettevõtted ei suuda seda teha ainuüksi ärilistel kaalutlustel.

Alternatiivina nõusolekupõhisele teenusele saaks kaaluda **privaatsust kaitsvate tehnoloogiate rakendamist ja/või andmete teisese kasutamise suuremat seadustamist**,

mis on lahti kirjutatud näiteks Arenguseire Keskuse personaalriigi stsenaariumite uuringus.⁷³ Esimesel juhul on võimalik privaatsusriske paremini maandada, kuigi tehnoloogiliselt on see veel arendusjärgus. Teisel juhul on võimalik andmepõhiselt oluliselt paremini erinevaid riske ennetada, kuigi sellega võib kaasneda ka potentsiaalselt suur põhiõiguste riive. Üsna efektiivne viis suuremaks andmekasutuks (soovitav küll vaid kriitiliste teenuste puhul) on andmete vaikimisi jagamine – see tõstab jagatavate andmete mahu potentsiaali kordades. Näiteks e-tervise osas on võimalik, et inimeste terviseandmed on vaikimisi kõigile arstidele kättesaadavad või tuleb neid jagada üksiku päringu põhisel. Eestis on terviseandmed vaikimisi kõigile arstidele kättesaadavad (s.t. inimene annab vaikimisi nõusoleku), aga inimene saab soovi korral selle nõusoleku ise tagasi võtta nii üksiku(te) epikriisi(de) kui ka terve terviseinfo osas. Samuti kaasneb sellega võimalus näha logifaile, kes on terviseandmeid nimeliselt pärinud ning inimest kaitsevad ka õiguslikud meetmed pahatahtlike päringute korral. Praegu on valdav osa terviseandmetest selle vaikimisi jagamise tõttu kättesaadavad kõigile litsentseeritud arstidele. Kui aga oleks otsustatud, et inimene peab ise minema nõusolekut andma (mis kontseptuaalselt oli võimalik), siis oleks enamus terviseandmeid arstidele suure tõenäosusega tänaseni kättesaamatud.

9.2 Alternatiivsed väärtusloome stsenaariumid

Autorid soovivad rõhutada, et uuringus käsitletud kaasused ei ole lõplikud. Personaalse andmeruumi arendamise perspektiivsus võib lähtuda ka Belgia riigi poolt Flandrias asutatud riigiettevõtte Athumi lähenemisest (viidatud ka ptk 4.3). Athumi ei loo rakendusi, mis ise isikuandmeid kasutaksid või neid monetiseeriks. Nende roll on luua usaldustaristu, mis võimaldab ettevõtetel teha turvalist ja nõuetele vastavat koostööd nii avaliku kui erasektoriga. Athumi on rakendanud isikuandmete ruumi kontseptsiooni andmekukrute (*data pod*) platvormina – iga inimesel on oma andmekukkur, kuhu saab salvestada andmeid erinevatest andmeruumidest. Oluline komponent on nõusoleku haldusel ehk kuidas inimese nõusolek kogutakse ja salvestatakse teenusepakkuja poolel. Athumi on tuvastanud personaalse andmeruumi raamistikus neli väärtusloome klastrit:

1. **Mugavus ja tõhusus:** Inimesed ei soovi kõiki oma andmeid sirvida – nad tahavad väärtust, milleks on mugavus ja tõhusus. Näiteks ka peatükis 8.2 tutvustatud kasutuslugu sujuvaks tööle asumiseks: andmekukkur võimaldab turvaliselt jagada vajalikke dokumente uue tööandjaga ühe nupuvajutusega. Ettevõtetele on väärtus selles, et andmed on autentset ja tõendatud – lisatakse verifitseeritav tõend, mis kinnitab, et andmed pärinevad algsest ja kontrollitud allikast.
2. **Ühiskondlik kasu:** Andmeid jagatakse anonüümselt teadusuuringuteks, näiteks terviseandmete teisese kasutuse puhul Euroopa terviseandmete ruumi kontekstis. Inimene annab ise ligipääsu oma terviseandmetele, et sellest tekiks ühiskondlik hüve.
3. **Veebipõhine personaliseerimine** (veebiküpsiste alternatiiv): Andmekukkur saab kasutada alternatiivina veebiküpsistele (*browser cookies*). Koostöös Hollandi meediaetevõtetega katsetati lahendust, kus kasutaja eelistused salvestatakse

⁷³ Personaalriigi tulevik Eestis. Stsenaariumid aastani 2040. <https://arenguseire.ee/raportid/personaalriigi-tulevik-eestis-stsenaariumid-aastani-2040/>, külastatud 23.03.2026

andmekukrusse ning inimesel on kontrollpaneel, kus saab määrata, milline meediaettevõtte tema andmeid kasutab.

4. **Elukorraldus ja AI-assistendid:** Kontseptsioon AI-assistendist, mis näiteks optimeerib kodu energiatarbimist, kasutades isiklikus andmekukrus olevaid andmeid, samal ajal säilitades kasutaja kontrolli.

Ka Eesti potentsiaalsed personaalse andmeruumi kasutusjuhud võib sarnaselt väärtusloomele ümber mõtestada ja osapoolte huvi korral proovida neid piloteerida. Samuti on uuringu autorid tuvastanud võimalusi järgmisteks personaalseteks teenusteks, mida uuringu mahu tõttu ei jõutud eraldi süvitsi uurida:

- **Personaalne bilanss ja tulem:** Inimene saab enda palgainfo, muu(de) tulu(de), pangakonto(de), kinnisvara(de), ettevõtete, aktsiate, kviitungute, arvete, pensionifondide jne abil ülevaate reaajas oma kumulatiivsetest sissetulekutest, varadest ja kohustustest, mida on võimalik agregeerida, et algandmeid esitamata näiteks pangast laenu saada, paremat kaskokindlustust teha, lasteaiakohast vabastust saada jne. Inimese enda soovil võib anda ligipääsu ka valikuliselt algandmetele (detailsed sissetuleku andmed vs usaldusreiting).
- **Minu elulugu:** Verifitseeritud elulugu, kus on info tegelike palgaandmete kohta, formaalse ning mitteformaalse hariduse detailide kohta, töökohakinnitused EMTA ja tööandja poolt, erinevad kutsetunnistused ning võimalus teha päringud välisriikide keskkondadesse. Inimene saab ise otsustada, mis andmeid ta kellega jagab ja kuidas (näiteks usaldusreiting või detailsed algandmed).
- **Võrdlusefekt: mina populatsioonis:** Kui andmete turvalise jagamise raamistik on paigas, saab inimene näiteks enda (või enda laste) hariduse osas tulemusi võrrelda populatsiooniga (kus teised ka vabatahtlikult andmeid jagavad). Nominaalsed hinnad (nt 2,3,4,5) on ilma taustasüsteemita pikemas perspektiivis vähemväärtuslikud – oluline on aru saada, kuidas oskused ja hinnad suhestuvad populatsiooni. Näiteks, kus õpilane paikneb reaalinete õppetulemute osas normaaljaotuse teljel. Sarnaselt ei ole keskmine palk või mediaanpalk kõige parem võrdlus – oluliselt parem on, kui inimesel on võimalik normaaljaotuse järgi võrrelda, kuidas tema palk suhestub populatsiooni (selleks võib olla terve Eesti, või siis näiteks doktorikraadiga mehed).

Veelgi suurem võrdlusefekt võib tekkida personaalsete terviseandmete osas. Näiteks OpenAI on koostöös arstidega välja töötamas ChatGPT Health rakendust, mis ühendab inimese terviseinfo ja ChatGPT intelligentsuse sadade miljonite inimeste populatsiooni võrduses. Võrreldes tavalise ChatGPT-ga, kasutab antud rakendus spetsiaalselt tervise jaoks loodud kaitsekihte (krüptimist ja isoleerimist, et hoida tervisealased vestlused privaatsed ja eraldatud). Personaalse andmeruumi tekkeks on võimalik erinevas formaadis meditsiiniline info laadida üles nii manuaalselt (nt PDFid) kui ka automaatselt liidestatuna (nt. Apple Health). Kuna ChatGPT-d kasutavad sajad miljonid inimesed üle maailma (sh tehakse u 230 miljonit tervist puutuvat päringut igal nädalal), on nii võimalik andmepõhiselt ja populatsioonipõhiselt saada enda jagatavale personaalsele terviseandmetele tähenduslikku tagasisidet. Kui personaalne andmeruum võimaldaks ühildada nt Eesti Terviseportaali infot inimese enda soovil

OpenAI-ga või siis hoopiski luua Terviseportaali juurde eraldi *ChatGPT Health* sarnane turvaline tervise rakendus, on võimalik inimesele anda tagasisidet tema tervisliku seisuga, võrreldes populatsiooniga. Antud juhul on OpenAI / ChatGPT lihtsalt üks näide võimast võrdlusandmete kasutamisest suurandmetega treenitud algoritmide loogika järgi – läbimurre võib ka mõnest muust sektorist / muu tehnoloogiaga tulla.

9.3 Andmealased koostöömudelid

Organisatsioonide vahelised andmealased koostöömudelid ning nende ärilise potentsiaal personaalse andmeruumi raamistikus on erinevad. Tarkade linnade ja kogukondade andmeruumi raames on välja töötatud mitme osapoolega valitsemisskeem⁷⁴, mis toob esile ka põhilised andmealased koostöömudelid (vt Tabel 7). Kui kokku on seitse koostöömudelit, siis ainult esimesed kolm on autorite hinnangul ärilise fookusega. Esimene mudel (äriandmed) tähendab andmete müüki organisatsioonide vahel kahepoolsete kokkulepete alusel. Teine mudel (andmeturg) eeldab andmete ostmist platvormi kaudu, mis on mitmepoolne kokkulepe (see võib kaasata inimest ennast ka oma andmete müüjana, kuigi selle osas väga efektiivseid lahendusi veel ei ole). Kolmas mudel (*As-a-Service*) eeldab seda, et osa andmetöötlustest toimub välise partneri juures, tasu eest. Viimased neli mudelit ei eelda ärilist fookust, vaid on kas altruistlikud ja/või koostööpõhised. Antud uuringus käsitletud kasutusjuhtude puhul näib suurem ärilise potentsiaal olevat elukindlustuses, hariduse ja oskuste andmete kasutus on pigem altruistlik / koostööpõhine.

Tabel 7. Andmealased koostöömudelite ülevaade ärilisest perspektiivist

Mudel	Andmevahetuse tüüp	Äriline potentsiaal
Äriandmed	Kahepoolne	Jah, ärikeskne
Andmeturg	Mitmepoolne	Jah, ärikeskne
As-a-Service mudel	Kahe- / mitmepoolne	Jah, ärikeskne
Avatud andmed / andmete annetamine	Ühepoolne	Ei, altruistlik
Pragmaatiline / ad-hoc andmete jagamine	Kahe- / mitmepoolne	Ei, koostööpõhine
Usaldusväärne kolmas osapool (andmevahendusteenus)	Mitmepoolne	Ei, koostööpõhine
Isikuandmete vahendusteenus	Mitmepoolne	Ei, altruistlik / individuaalne kontroll
Andmeühistu / andmekooperatiiv	Mitmepoolne	Ei, koostööpõhine

■

9.4. Väljakutsed ja võimalused

Ühest küljest on Eesti personaalse andmeruumi loomisel soodsas positsioonis tänu laialdaselt juurutatud ja tegelikult kasutus olevatele digiteenustele. Eesti digiriigi andmetaristu (X-tee)

⁷⁴ Multi-Stakeholder Governance Scheme, kättesaadav aadressil

https://static1.squarespace.com/static/63718ba2d90d0263d7fc1857/t/651ea670a884c256d84f4864/1696507511589/DS4SSCC_D2.2+Multi-stakeholder+governance+scheme.docx.pdf, külastatud 23.03.2026

koos digitaalse identiteediga (eID) on aidanud luua personaalse andmeruumi esimesed teenused avalikus sektoris - andmejälgija, andmenõusolekuteenus, Terviseportaal jt. Samas võib olemasolev arhitektuur ja varasemad lahendused kujuneda barjääriks personaalse andmeruumi teenuste skaleerimisel ja uute funktsioonide integreerimisel. Lisaks on personaalse andmeruumi puhul oluline silmas pidada selle rakendamist just era- ning kolmandas sektoris, kuna inimeste vaatest on andmesuveräänsuse tagamise problemaatika peamiselt just seal.

#1 Millist personaalset andmeruumi Eesti inimesed vajavad?

Personaalse andmeruumi puhul on eelduseks, et see on loodud inimeste jaoks ja nende huvides. Samas, Eesti elanikkond on heterogeenne ning erinevatel kasutajarühmadel on erinevad vajadused ning eelistused andmete haldamise ning jagamise osas. Üks peamisi väljakutseid on seetõttu aru saada, kui vajalikud ja atraktiivsed võiksid personaalse andmeruumi teenused laiemalt inimeste jaoks olla ning millised tegelikke probleeme see lahendab. Samas on metodoloogiliselt keeruline hinnata tavaelanike ootusi teenusele, mida nad ei ole kunagi kasutanud. Inimese vaatepunkti selgitamiseks on käesolev uuring tuginenud mahupiirangute tõttu peamiselt olemasolevatele uuringutele (sh Statistikaameti andmestikud, inimese digitaalse kaksiku teadus-arendusuuring) ning ekspertide hinnangutele.

Personaalse andmeruumi juurutamiseks on oluline tagada inimeste usaldus. Eesti kontekstis on oluliseks võimaluseks ning soodustavaks teguriks asjaolu, et inimeste usaldus digitaalsete teenuste vastu on keskmisest kõrgem ning ühiskond on väiksuse tõttu tihedalt lõimunud. See loob eeldused personaalse andmeruumi positiivseks vastuvõtmiseks, eeldusel, et personaalse andmeruumi teenus(ed) on kasutajate jaoks mõistlik(ud) ja kasulik(ud).

#2 Kuidas luua personaalne andmeruum, arvestades Eesti digiriigi konteksti?

Eesti digiriigi edu sai alguse kui 1990ndatel ja 2000ndatel ehitati riik uuesti üles, nii õiguslikult kui ka teenuste mõttes. Väga olulised andmeruumi puudutavad otsused (ID-kaardi / eID kohustuslik kasutuselevõtt, X-tee kohustuslik rakendamine) tehti veel enne Euroopa Liiduga ühinemist. Sisuliselt oli sel hetkel väga hea ajaaken radikaalse innovatsiooni jaoks, mida Eesti ka edukalt rakendas (vähemalt tagasivaates). Tänapäevaks on Eesti regulatiivselt, majanduslikult ning tehnoloogiliselt väljakujunenud riik, mis paratamatult aeglustab võimalike uute lahenduste kasutuselevõttu. Seega on põhjust arvata, et innovatsioon toimub täna samm-sammult ning peab integreeruma olemasolevasse taristusse ja arvestama kehtiva regulatiivse raamistikuga. See tähendab, et personaalse andmeruumi osas tuleb arvestada Eesti digiriigi taristuga ning selle peale tekkinud teenustega (nt. andmejälgija, andmenõusolekuteenus), samuti tuleb arvestada Euroopa Liidu regulatsiooni (nt IKÜM, andmemäärus jt) ning muude arengutega (nt digikukkur, andmeruumid jne). Olemasolev taristu ning regulatiivne keskkond võib aga uute algatuse jaoks olla ka pärssiv, nn *lock-in*⁷⁵ efekti pärast (kui taristu ja

⁷⁵ Nn *lock-in* lahendusteks on ka andmejälgija, andmenõusolekuteenus ning Terviseportaal, kuna need on juba õiguslikult ja tehnoloogiliselt teenustena olemas. Samas, personaalse andmeruumi loomise mõttes ei saa välistada, et võib olla ka mõni kiiremini skaleeritavam viis, kuidas inimestele anda võimalus tema andmete kasutust jälgida ning otsustada, kes ja mis tingimused tema andmetele ligi pääseb. Andmejälgija teenust kasutavad 16+ andmekogu ning nõusolekuteenust 4+ andmekogu – on fakt, et need ei ole kiiresti skaleerunud. Samuti ei ole uute andmebaaside lisamine lihtne, vaid eeldab olulist poliitilist, ajalist ning rahalist investeerimist. Positiivse arenguna

regulatsioon on juurdunud, siis uued lahendused peavad sellega arvestama; radikaalne muutus on oluliselt keerulisem). Sellest tingituna ei tohiks personaalset andmeruumi näha kui eraldiseisvat lahendust, vaid pigem muude teenustega lõimitud funktsionaalsust, mis johtub andmehalduslikest ning protseduurilistest kokkulepetest, kuidas inimene saaks paremini jälgida ning kontrollida endaga seotud andmete kasutamist ning jagamist.

#3 Kuidas teha personaalne andmeruum atraktiivseks erasektorile?

Personaalse andmeruumi kontseptsiooni rakendamise teeb keeruliseks andmete jagunemine erinevate organisatsioonide vahel. See tähendab, personaalne andmeruum on ka praegu tingulikul võttes olemas, aga inimene ei saa seda lihtsal viisil näha ega selle osas efektiivselt otsused vastu võtta.

Kui riigisektor saab soovi korral võimalikult palju riiklikult reguleeritud andmebaase liidestada näiteks andmejälgija ning andmenõusolekuteenusega, siis oluliselt keerulisem on see erasektori andmebaasidega – inimese üldhuvidest lähtuvaid investeeringuid on raske põhjendada, eriti konkureerivas keskkonnas. Veelgi väljakutsuvamaks teeb olukorra see, et paljud inimese andmeid koguvad ning töötlevad ettevõtted on rahvusvahelised suurettevõtted (nt. Meta, Google, Bolt, Garmin jne) ja/või on nende lahendused piiriülesed (nt Rimi, Stockmann, Circle K, McDonalds jne).

Selles valguses, ideaalset personaalset andmeruumi, mis suudaks koondada kõik inimese andmed ühte kohta, tõenäoliselt kunagi ei teki. Ei ole reaalne, et kõik ettevõtted ja andmeid omavad / töötlevad organisatsioonid hakkaksid kõiki personaalseid andmeid tegema kõigile ühes formaadis kättesaadavaks nagu on jälgitav nt Eesti andmejälgijas.

Võimalus võib aga tekkida laiemalt selleks, et teenusepakkuja enda juures tekib lihtsam võimalus andmete kasutamist jälgida ning nende osas otsuseid teha. Näiteks terviseandmete kasutamisega on võimalik tutvuda eraldiseisevas terviseportaali keskkonnas, kus saab otsustada, millised andmed (sh erasektori omad) on teistele (nt arstid, pereliikmed) kättesaadavad. Kui oluliste teenusepakkuja juures tekib inimesel võimalus enda andmeid automaatselt edastada ka kolmandatele osapooltele (näiteks kolmanda osapoole poolt pakutav juhtlaud), siis sellest võibki tekkida personaalne andmeruum (mis on võib olla ka iga inimese jaoks erinev). Tõsi, see eeldab mitmetasandilist regulatiivset raamistikku, investeeringud ning ka eesmärgipärast elluviimist. Veelgi olulisemana – see eeldab inimeste huvi ning oskust oma andmete kasutamist paremini jälgida ning neid kontrollida.

#4 Kuidas tagada kommunikatsioon, oskused ja turvalisus?

Peamised riskid on seotud ebapiisava väärtuspakkumise selguse ja kommunikatsiooniga, mis vähendab kasutajate (nii inimeste kui ka organisatsioonide töötajad) motivatsiooni ning võib tekitada vastuseisu muutustele. Oluliseks väljakutseks on ka inimeste madal andmekirjaoskus ja ühiskondlikult kujunenud hoiakud, mis mõjutavad usaldust uute andmekasutusviiside suhtes. Sellega seondub ka inimeste andmete taaskasutamist toetava õigusloome aeglane areng (nt võttis andmenõusolekuteenuse reguleerimine aastaid), mistõttu ei pruugi

on Eesti riik otsustanud muuta andmejälgija kõigile riiklikele andmebaasidele kohustuslikuks (<https://www.err.ee/1609768860/andmejalgija-infot-naeb-vaid-16-andmekogu-kohta>).

äriarenduseks vajaminev sotsiaalsete ning õiguslike kokkulepete saavutamine käia samas rütmis äriliste vajadustega.

Inimeste andmete taaskasutamisega seonduvad riskid tulenevad ka küberturvalisuse nõrkustest, võimalikest andmeleketest, võimalikest poliitilistest valikutest (nt otsused suurendada andmepõhist jälgitatavust elanike üle) või andmete väärkasutusest pahatahtlikel eesmärkidel. Samuti võivad kasutajakogemuse kohmakus, vähene kodanike kaasamine teenuse kujundamisse ja tehnoloogiline keerukus takistada personaalset andmeruumi võimaldavate lahenduste laialdasemat kasutuselevõttu. Lõpuks ei pruugi personaalse andmeruumi lahendused saavutada oma täit potentsiaali, kui see ei suuda integreerida inimese andmeid ja teenuseid tõeliselt terviklikuks „ühe vaate“ lahenduseks.

Kuigi personaalse andmeruumi väärtus selgub kõige konkreetsemalt just kaasuspõhiselt, võimaldades paremini analüüsida spetsiifilisi äriprotsesse ning täpsustada inimkeskse lähenemise väärtuspakkumist eri osapooltele, siis on sellisel lähenemisel ka omad riskid. Nimelt on vaja personaalse andmeruumi kontseptsiooni arendamiseks hoida ökosüsteemiülest vaadet, nii valdkonna (finants, haridus jt), riigi kui ka rahvusvahelisel tasandil, et vältida vaid konkreetse valdkonna- või riigispetsiifilise rakenduse arendamist (nn silostumist ning jätkuvat killustumist). Personaalse andmeruumi laiem potentsiaal avaldub (nii inimesele kui ettevõtetele) alles siis kui süsteemi on kaasatud mitmeid eri valdkondi, andmepõhiseid teenuseid ning nende osapooli. See on oluline, et balansseerida nõudluse ja pakkumise vahelist suhet, suurendada nn võrguefekti, toetada andmete kättesaadavust, taaskasutamist ning tervikliku vaate tekitamist. Seetõttu on konkreetse personaalse andmeruumi teenuste ning selle kaasuste arenduse (nn *mikro* tasand) kõrval vaja toetada ka laiema ökosüsteemi arengut nii nn *meso* (haldusraamistikud, institutsionaalne järelvalve jt) kui ka *makro*¹¹ (rahvusvahelised algatused, standardid, regulatsioonid jms) tasandil.

10. Soovitused ja teekaart

10.1 Soovitused personaalse andmeruumi lahenduste arendamiseks

Personaalse andmeruumi kontseptsiooni praktikas rakendamine eeldab koordineeritud arengut tehnoloogilisel, õiguslikul ja institutsionaalsel tasandil. Eesti senine digiriigi taristu loob selleks tugeva lähtekoha, kuid potentsiaali realiseerimine eeldab sihipäraseid poliitilisi valikuid ning riigi, erasektori ja teiste sidusrühmade koosloomet. Personaalset andmeruumi ning selles raamistikus pakuvaid lahendusi pole võimalik arendada tavapärase IT-teenusena, mis kataks mingi konkreetse organisatsiooni või kasutaja vajadust ning ootusi. Selle arendamine eeldab ökosüsteemiülest innovatsiooni, millega toetada inimeste andmete taaskasutamist erinevate osapoolte ning teenuste poolt, pakkudes samal ajal inimestele terviklikku ülevaadet ning mugavat hallatavust. Käesolevas peatükis esitatakse soovitused peamiselt riigile kui antud uuringu tellijale personaalse andmeruumi raamistiku ning seda toetava ökosüsteemi arendamiseks. Sealjuures on personaalse andmeruumi väärtusloome kontekstis oluline roll just erasektoril, mistõttu leiab siit ka võtmetähtsusega soovitusi ettevõtetele.

1. Tõsta nii Eesti elanike teadlikkust digiriigi ning andmemajanduse toimimisest kui ka soosida digipädevuste arendamist

Inimkeskse andmemajanduse arendamisel tuleb pöörata tähelepanu inimeste teadlikkuse ja digipädevuste arendamisele, mis on oluliseks eelduseks, et inimesed oleksid valmis võtma aktiivset rolli oma andmete haldamisel ning nende kasutamise kontrollimisel. Inimkeskse andmemajanduse toimimine eeldab, et nii inimesed kui organisatsioonid mõistavad andmete kasutamise võimalusi ja riske ning suudavad teha teadlikke ning vastutustundlikke otsuseid. Riik peaks seetõttu süsteemselt panustama andmekirjaoskuse arendamisse ning toetama vastavate kompetentside kujundamist nii haridussüsteemis kui ka tööelus.

Personaalse andmeruumi kontseptsiooni keskmes on üksikisik – andmesubjekt, kes saab suurema kontrolli oma andmete üle. Selleks, et inimesed oleksid valmis sellistes süsteemides aktiivselt osalema, peab nende kogemus olema selgelt positiivsem võrreldes varasema olukorraga. Riik saab olla siin suunanäitajaks ka erasektorile, soodustades lahendusi, mis on kasutajale arusaadavad, läbipaistvad ja lihtsasti kasutatavad (seetõttu on ka tervitav nt Andmejälgija ja Eesti.ee edasiarendus inimese digitaalse kaksiku projekti vaatest). Kui kasutajatel on selge ülevaade sellest, milliseid andmeid nende kohta kogutakse, kes neid kasutab ning millisel eesmärgil, siis tekib eelduslikult ka suurem nõudlus sarnaste lahenduste järgi muude teenuste suunal. Sealjuures on oluline arendada andmehaldusteenuseid ettevaatavalt – mida rohkem on inimesed kaasatud andmete kasutamisse nõusolekute ning tahteavalduste jagamise kaudu, seda lihtsam peab olema nende haldamine (andmine, muutmine ja/või tagasivõtmine) teenuste üleselt.

2. Tagada toimiv ja prognoositav õigus- ning haldusraamistik

Personaalse andmeruumi areng eeldab toimivat ja prognoositavat õigus- ning haldusraamistikku. Kuigi olemasolevad regulatsioonid – eeskätt isikuandmete kaitse ja andmete kasutamist käsitlevad Euroopa Liidu õigusaktid – loovad üldise ning tugeva raamistiku, võivad personaalse andmeruumi teenuste rakendamisel tekkida tõlgenduslikud küsimused näiteks andmete jagamise, vastutuse ja volituste osas.

Riigi roll on tagada, et nii teenusepakkujatel kui ka kasutajatel oleks selge arusaam õigustest, kohustustest ja vastutusest andmete haldamisel. See hõlmab vajadusel täiendavate juhendite, standardite või suuniste loomist, mis aitaksid selgitada, kuidas olemasolevaid regulatsioone personaalse andmeruumi kontekstis rakendada. Samuti on oluline, et regulatiivne keskkond ei looks põhjendamatuid takistusi innovatsioonile, vaid toetaks uute teenuste tekkimist ja katsetamist.

Õigusliku selguse loomisel võiks riik teha tihedat koostööd nii ettevõtete, teadusasutuste kui ka rahvusvaheliste partneritega. Kuna andmeökosüsteemid on sageli piiriülesed, on oluline, et Eesti lähenemine oleks kooskõlas Euroopa Liidu tasandi arengutega ning toetaks tulevikus potentsiaalselt ka koostalitlusvõimet teiste riikide lahendustega. Seejuures on oluline hoida tasakaalu õiguskindluse ja innovatsiooni toetamise vahel ning panustada ka Euroopa Liidu tasandi aruteludesse personaalse andmeruumi regulatiivse raamistiku kujundamisel. Selleks loob hetkel “võimaluste ajaakna” ka käimasolev arutelu Digital ja AI Omnibusi⁷⁶ teemadel, kuhu on Eesti esindajatel võimalik ELi tasandi arutelude raames integreerida ka personaalse andmeruumi edasiste arengute temaatika (nt teha ettepanek lisada uuendatavasse õigusakti selgitav põhjenduspunkt (recital) personaalse andmeruumi kontekstis lubatavuse, õigusliku aluse, toimemehhanismide ja vastutuse kohta või täiendada IKÜM IX peatükki eraldi artikliga personaalse andmeruumi kontekstis, mis reguleeriks personaalse andmeruumi aspektist isikuandmete töötlemise rolle, vastutust ja õigusi.

3. Suurendada andmete kättesaadavust ning vahetust tuginedes toimivale digitaristule ning usaldusväärsetele andmevahendusteenustele

Eesti eeliseks on olemasolev digiriigi taristu ning kesksed komponendid, nagu digiidentiteet ja andmenõusolekuteenus, mis toetavad personaalse andmeruumi raamistikku ning lahendusi, eriti avaliku sektori teenuste ning nende poolt kasutavate andmete suunal. Seetõttu peaks riik keskenduma eelkõige olemasolevate komponentide, nagu nõusolekuhaldus ja kasutajakesksed läbipaistvusteenused, täiendavale arendamisele ning koostalitlusvõime tagamisele (mh lepinguline selgus andmeajamiseks ning andmeajamise standardsete formaatide loomine). Sealjuures tuleb arvestada, et riigi digitaristuga liidestumine võib ettevõtete jaoks olla liiga kulukas, mistõttu on tekkinud ka näiteid n-ö vahemeestest (nt

⁷⁶ <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal>, , külastatud 24.03.2026

CreditInfo), kes toetavad andmete koondamise ja väärindamisega spetsiifilistes sektorites. See viitab vajadusele kas spetsiifilistes sektorites või laiapindsel tegutsevate andmevahendusteenuste ning ärianalüütika põhist lisaväärtust loovate teenuste järgi, et toetada sektoriülest koostööd ning luua paremat andmepõhist teadmist turuspetsiifikast.

Personaalse andmeruumi raamistikus toimivad teenused eeldavad ulatuslikku (isiku)andmete kogumist, töötlemist ja jagamist. Seetõttu on kriitilise tähtsusega tagada nende süsteemide kõrge turvalisuse ja andmekaitse tase. Sealjuures on lisaks tehnilisele kasutusmugavusele oluline ehitada ja hoida usaldust. Usaldus tekib siis, kui inimesed näevad selget kasu oma andmete jagamisest – näiteks paremaid teenuseid, personaliseeritud lahendusi või lihtsamat asjaajamist. Eriti erasektori poolt pakutavate teenuste puhul on riigi ülesandeks tagada korralik ning süsteemne riiklik järelvalve ning tugi, mis toetaks ühest küljest avatud ja vastutustundlikku innovatsiooni, kuid teisalt võtaks andmeid väärkasutanud ettevõtted ka proportsionaalselt vastutusele. Näiteks võib inimeste andmete lekke puhul usaldus digiteenuste ja nende loojate vastu mureneda, eriti olukorras kui andmesubjekt ei näe andmete väärkasutuse puhul selgeid tagajärgi.

4. Toetada andmealast koostööd erasektoris

Personaalse andmeruumi majanduslik potentsiaal sõltub suurel määral erasektori kaasatusest luua personaliseeritud ning proaktiivseid teenuseid ning teha andmealast koostööd. See eeldab hetkel kehtivast andmetel põhinevast ärimudelist (*“the winner takes it all”*) loogikast üleminekut andmete kasutamisele koostööpõhiselt, suurendades võimalust teha sektoriülest innovatsiooni. Pikemas perspektiivis kujuneb ettevõtete konkurentsieeliseks mitte niivõrd andmete omamine, vaid võime neid usaldusväärselt ja koostöömõiselt kasutada ning jagada. See nõuab aga oma süsteemide ja protsesside ümberkujundamist viisil, mis võimaldab turvalist ja standardiseeritud andmevahetust teiste osapooltega.

Sellise arengu toetamiseks võiks riik luua regulatiivseid ja tehnoloogilisi katsekeskkondi (nt *sandboxid*), mis võimaldavad ettevõtetel testida personaalse andmeruumi komponente kontrollitud tingimustes. Samuti on põhjendatud kaaluda meetmeid, mis aitavad vähendada liidestumise ja vastavusnõuete täitmisega seotud kulusid, eelkõige väiksema ja keskmise suurusega ettevõtete puhul.

See tähendab, et riigi roll peaks personaalse andmeruumi arendamisel keskenduma eelkõige toimiva ja prognoositava keskkonna kujundamisele, mis loob eeldused erasektori initsiatiivil põhinevate lahenduste tekkeks ja skaleerimiseks, mitte üksikute teenuste tsentraalsele arendamisele. Näiteks võiks riik luua tingimused, mis soodustaksid ettevõtete huvi andmepõhiste teenuste arendamise vastu, sh toetades pilootprojekte ja innovatsiooni ning edendades avaliku ja erasektori koostööd. Selleks on täna juba avatud mitmed toetusmeetmed, nagu “Ettevõtjate digitaliseerimise, reaalamajanduse lahenduste ja andmemajanduse kasutusjuhtude arendamise toetamine”⁷⁷, et vähendada ettevõtete innovatsiooniriski ning pakkuda võimalust uute lähenemisviiside katsetamiseks. Lisaks

⁷⁷ Ettevõtluse ja Innovatsiooni Sihtasutuse meede, kättesaadav aadressil <https://www.riigiteataja.ee/akt/127012026020>, külastatud 24.03.2026

rahastusmeetmetele võiks riik kaaluda ka erinevate arendusprogrammide ning kiirendite⁷⁸ toetusmeetmeid, mis aitaksid ettevõtetel arendada andmepõhiseid teenuseid ja soodustada personaalse andmeruumi raamistikus toimivat andmeökosüsteemi loomist.

Oluline on ka toetada ühtsete standardite ja koostalitlusvõime põhimõtete kujunemist, et tagada erinevate lahenduste sujuv koostoime ning vältida turu killustumist.

5. Siduda personaalse andmeruumi raamistik ettevõtte äristrateegiaga ning tagada tugev strateegiline juhtimine

Organisatsioonid peaksid käsitlema personaalset andmeruumi kui strateegilist suunda oma tegevuses, mis muudab organisatsiooni rolli andmemajanduses ning laiemalt positsiooni turul. See tähendab süstemaatilist liikumist andmete kogumiselt ja kontrollimiselt ärimudelini, kus ettevõtte suudab luua tooteid ja teenuseid inimkeskse andmekorralduse põhimõtetest lähtuvalt. See eeldab tugevat strateegilist juhtimist ja järjepidevat piloteerimist. Tegemist ei saa olla üksiku teenuse või IT-osakonnale suunatud arendusprojektiga, vaid süsteemse innovatsiooniga organisatsiooni sees ning koostööpartnerite vahel, mis nõuab selget vastutusjaotust, sidusrühmade kaasamist ning poliitikakujunduse ja praktiliste katsetuste tihedat seostamist.

Personaalse andmeruumi raamistiku edukas rakendamine eeldab ka riigi võimet kujundada terviklik ja usaldusväärne raamistik, mis ühendab kasutajakesksuse, õigusliku selguse, tehnoloogilise võimekuse ja majanduslikud stiimulid. Sealjuures on oluline määrata selge eestvedaja ja luua ministeeriumite ülene koordineatsioon.

* * *

Kokkuvõttes eeldab personaalse andmeruumi edukas arendamine terviklikku ja koordineeritud lähenemist, mis ühendab teadlikkuse tõstmise, selge õigusraamistiku, usaldusväärse tehnoloogilise taristu ning erasektori aktiivse kaasamise. Riigi roll on kujundada soodne keskkond, mis toetab nii innovatsiooni kui ka kasutajate usaldust, tagades samal ajal andmete turvalise ja läbipaistva kasutamise. Ainult erinevate osapoolte koostöös ja strateegilise juhtimise toel on võimalik realiseerida personaalse andmeruumi potentsiaal ning kujundada inimkeskne andmemajandus, mis loob väärtust nii üksikisikule kui ka ühiskonnale tervikuna. Järgmises alapeatükis on antud soovitusel esitatud ka 5+ aastasel teekaardil, mis kirjeldab personaalse andmeruumi(de) jaoks oluliste õiguslike, tehnoloogiliste, äriliste ja organisatsiooniliste võimekuste arendamist etapiisiliselt.

⁷⁸ Vt nt Soomes läbiviidud kiirendi näidet, mis lõi aluse haridus- ja oskuste andmeruumi edasiseks arenguks: <https://mydata.org/2020/09/14/interesting-outcome-of-the-mydata-accelerator-project/>

10.2 Teekaart personaalse andmeruumi rakendamiseks

Tabel 8. Teekaart soovitud personaalse andmeruumi rakendamiseks

Aeg	Murekoht	Soovitav suund	Peamised initsiatiivid	Oodatav tulemus
Käivitamise faas keskendub eelkõige ärilise ja organisatsioonilise võimekuse loomisele, sealhulgas eestvedamise, sidusrühmade kaasamise ja teadlikkuse tõstmisega seotud soovitude elluviimisele. Alustada võiks käesolevas uuringus tuvastatud kasutuslugudest ning nendega seotud osapooltest, kuid laiendada kasutuslugude otsinguid ka teistesse valdkondadesse. Sealjuures võtta arvesse ka ptk 9 esitatud alternatiivseid mudeleid väärtusloomeks.				
2026	Eestvedaja puudumine ja killustunud algatused	Määrata eestvedaja ja luua ministeeriumite ülene koordinatsioon	• Luua töögrupp või programm; • Siduda personaalse andmeruumi ökosüsteemi arendamine digiarengukavaga; kaasata ministeeriumid; • Kaasata RIA, EIS ja teised digiriigi arendajad ning määrata keskne eestvedaja või kompetentsikeskus; Kasutada käesolevas uuringus analüüsitud kasutajalugusid ja rollimudelit lähtepunktina	Ühine strateegiline suund ja koordineeritud tegevused
2026 - 2027	Huvi väheste „pioneeride“ seas erasektoris	Käivitada piloodid ja innovatsiooni-meetmed (nt EIS, Riigikantselei Innofond)	• Valideerida ja laiendada käesolevas uuringus kaardistatud kasutuslugusid koostöös erialaliitude ja sektori osalistega; • Valmistada ette pilootlahendused ning käivitada need andmemahukates ja kõrge väärtuspotsiaaliga sektorites (nt tervishoid, kindlustus, tööjõuturg, energeetika); • Hinnata pilootprojektide käigus nii lahenduste tehnilist teostatavust kui ka esmast teenuste väärtuspakkumist ja majanduslikku potentsiaali; kasutada pilootide elluviimiseks innovatsiooni- ja arendusmeetmeid; • Tõsta inimeste teadlikkust personaalsest andmeruumist ja arendada digipädevusi	Sektorite huvi Esimesed kasutuslood Suurenenud teadlikkus ja kompetents

Aeg	Murekoht	Soovitav suund	Peamised initsiatiivid	Oodatav tulemus
Raamistiku loomise faas keskendub peamiselt õigusliku ja tehnoloogilise võimekuse arendamisega seotud soovitude realiseerimisele. Lisaks on rõhuasetus kasutuslugude põhiste reeglite määratlemisel, mis sätestavad kes, millistel tingimustel ja millises ulatuses võivad andmetele või teenustele ligi pääseda.				
2027	Ebakindlus ärimudelite osas / inimkeskse andmemajanduse kaasuste innovatsioonirisk erasektori vaatest	Arendada usaldus- raamistik ja standardid; Katsetada andmealase koostöö formaate ettevõtluse toetamisel läbi praktiliste pilootide	• Valideerida ja formaliseerida käesolevas uuringus pakutud rollimudel; • Luua kiirendid andmealase koostöö soodustamiseks sektoriülest, võttes aluseks inimkeskse andmemajanduse põhimõtted; • Valideerida teenuste ärinte väärtsu ning kujunevate ärimudelite jätkusuutlikkus; • Hinnata personaalse andmeruumi lahenduste majanduslikku mõju ja teenuse turupotentsiaali. • Luua andmeruumi osalejate sertifitseerimise põhimõtted; defineerida ligipääsupoliitikat	Proгноositavam keskkond ettevõtetele; Töötavad prototüübid ja valideeritud mudel
2027-2029	Tehnoloogiline killustatus	Luua ja/või võtta kasutusele referents- arhitektuur ja koostalitlus- standardid	• Määratleda identiteedi, nõusoleku, volituste ja auditi komponendid; • Tagada seos digikukru, X-tee ning teiste digiriigi komponentide arenguga; • Arendada käesolevas uuringus kirjeldatud arhitektuuri- kontseptsioonist personaalse andmeruumi referentsarhitektuur; • Valideerida lahenduste tehniline toimivus.	Ühtne arhitektuuriline raamistik
Kasutuselevõtu ja laienemise faas keskendub peamiselt pilootlahenduste praktilisele rakendamisele ning personaalse andmeruumi komponentide rakendamisele erinevates kasutuslugudes/teenustes.				
2030 - ...	Ökosüsteemi laienemise vajadus	Toetada erasektori teenuste arengut	• Laiendada katsetatud lahendusi sektoripõhistes projektides (nt tervis, energia, kindlustus); • Soodustada avatud standardite ja liideste kasutamist.	Personaalse andmeruumi teenuste ja kasutuslugude laienemine ning andmeökosüsteemi küpsusastme tõstmine.

11. Kasutatud kirjandus

1. Aguerre, C., Hasselbalch, G. (2025) The EU human-centric approach to AI: Foundational elements for a global framework. DataEthics.eu. <https://dataethics.eu/research/the-eu-human-centric-approach-to-ai-foundational-elements-for-a-global-framework/>
2. Andmekaitse Inspektsioon. (2025). Isikuandmete ülekandmine. <https://www.aki.ee/isikuandmed/inimese-oigused/isikuandmete-ulekandmine>
3. Andmekaitse Inspektsioon. (2025). Töötlemise õiguslikud alused. <https://www.aki.ee/isikuandmed/andmetootlejale/tootlemise-oiguslikud-alused>
4. Andmekaitse Inspektsioon. (2025). Digital Omnibus ja AI Omnibus. <https://www.aki.ee/rahvusvaheline/euroopa-andmestrateegia/digital-omnibus-ja-ai-omnibus>
5. Arenguseire Keskus (2022). Andmeühiskonna tulevik. Stsenaariumid aastani 2035. Raport. Tallinn: Arenguseire Keskus. https://arenguseire.ee/wp-content/uploads/2022/12/2022_andmehiskonna-tulevik_raport.pdf
6. Arenguseire Keskus (2024). Personaalriigi tulevik Eestis. Stsenaariumid aastani 2040. <https://arenguseire.ee/raportid/personaalriigi-tulevik-eestis-stsenaariumid-aastani-2040/>
7. Athumi. (2025). Solutions and Platforms. <https://athumi.eu/en/solutions-platforms>
8. Cybernetica. (2025). Eesti e-identiteedi ökosüsteem. Ülevaade. <https://www.ria.ee/sites/default/files/documents/2025-10/eID-okosusteem-lisadega-2025.pdf>
9. Cybernetica. (2025). Interoperability mõiste. Andmekaitse ja infoturbe portaal. <https://akit.cyber.ee/term/822>
10. Cyber Risk GmbH (2025) The Financial Data Access (FiDA) Regulation. <https://www.financial-data-access.com/>
11. D'Ignazio, C., & Klein, L. F. (2023). Data feminism. MIT Press. <https://data-feminism.mitpress.mit.edu/>
12. Data Spaces Support Centre. (2025). Alphabetical list of all defined terms in Blueprint v2.0. <https://dssc.eu/space/BVE2/1071252161/Alphabetical+List+of+All+Defined+Terms+in+Blueprint+v2.0>
13. Data Tank. (2025). Data stewardship program. <https://www.datatank.org/data-stewardship-program>
14. Euroopa Komisjon (2022). Ettevõtete vaheline andmete jagamine: Küsimused ja vastused. <https://digital-strategy.ec.europa.eu/et/faqs/business-government-data-sharing-questions-and-answers>
15. Euroopa Komisjon (2015). Questions and answers: Data protection reform. https://ec.europa.eu/commission/presscorner/detail/et/memo_15_6385
16. Euroopa Komisjon. (2016). An emerging offer of “personal information management services”: Current state of service offers and challenges [European Commission Report]. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=40118
17. Euroopa Komisjon. (2017). Guidelines on the right to "data portability" (wp242rev.01) <https://ec.europa.eu/newsroom/article29/items/611233>
18. Euroopa Komisjon (2022). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

- (General Data Protection Regulation). Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
19. Euroopa Komisjon (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Official Journal of the European Union. <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32022R0868>
 20. Euroopa Komisjon (2023). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). <https://eur-lex.europa.eu/eli/reg/2023/2854>
 21. Euroopa Komisjon (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>
 22. Euroopa Komisjon (2024). Consolidated text: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018>
 23. Euroopa Komisjon (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
 24. Euroopa Komisjon. (2025). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837>
 25. Euroopa Komisjon. (2025). Data marketplace. ELISE - European Location Interoperability Solutions for e-Government glossary. <https://interoperable-europe.ec.europa.eu/collection/elise-european-location-interoperability-solutions-e-government/glossary/term/data-marketplace>
 26. Euroopa Komisjon. (2025). EU member states' notifications to the European Commission under the GDPR. https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection/eu-member-states-notifications-european-commission-under-gdpr_en
 27. Euroopa Komisjon. (2025). European Data Market Study 2024–2026: First report on facts & figures (Deliverable D2.1). https://ec.europa.eu/newsroom/repository/document/2025-13/EDM_2024_2026_First_Report_on_Facts_and_Figures_9cU0iljcuSZhjmwl9TchwqenidQ_114043.pdf
 28. Euroopa Komisjon (2020) Euroopa andmestrateegia, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066>
 29. Euroopa Komisjon (2020) Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0264&from=EN#footnote44>

30. Euroopa Komisjon (2025) ELI andmevahendusteenuste register. <https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services>
31. European Data Protection Board. (2025). Frequently asked questions. What is personal data? https://www.edpb.europa.eu/sme-data-protection-guide/faq-frequently-asked-questions/answer/what-personal-data_en
32. Gangneux, J. (2023). Multi-Stakeholder Governance Scheme. Data Space for Smart and Sustainable Cities and Communities. https://static1.squarespace.com/static/63718ba2d90d0263d7fc1857/t/651ea670a884c256d84f4864/1696507511589/DS4SSCC_D2.2+Multi-stakeholder+governance+scheme.docx.pdf
33. Haridus- ja Teadusministeerium (2025). Haridusportaal. <https://haridusportaal.edu.ee/>
34. iGrant.io (2025) iGrant.io veebilehekülg. <https://www.igrant.io/>
35. Justiits- ja Digiministeerium. (2024) Andmete ja tehisintellekti valge raamat 2024–2030. https://www.kratid.ee/files/ugd/7df26f_9a6d060409214b9da2774e5b5eabf717.pdf
36. Justiits- ja Digiministeerium (2025). Eesti elanike suhtumine digiriiki ja tehnoloogilistesse lahendustesse. Andmete teabevärv. <https://andmed.eesti.ee/datasets/eesti-elanike-suhtumine-digiriiki-ja-tehnoloogilistesse-lahendustesse>
37. Justiits- ja Digiministeerium. (2025). Eesti andmeruumide pikaajaline plaan. https://www.kratid.ee/files/ugd/2d9e67_5a304a96ef014f3099939b9271c33a57.pdf
38. Justiits- ja Digiministeerium. (2025) Uus seaduseelnõu: inimestel tekib selgem võimalus oma andmete jagamiseks või selle keelamiseks <https://www.justdigi.ee/uudised/uus-seaduseelnou-inimestel-tekib-selgem-voimalus-oma-andmete-jagamiseks-voi-selle>
39. Kutsekoda (2025) Kutseregister. <https://www.kutsekoda.ee/>
40. Kutsekoda (2025) Oskuste Kompas. <https://kutsekoda.ee/oskuste-kompass/>
41. Kutsekoda (2025) Oskuste register. <https://kutsekoda.ee/oskused-2>
42. Langford, J., Poikola, A., Janssen, W., Lähteenoja, V., Rikken, M. (Eds.). (2022). Understanding MyData operators. MyData Global.
43. Lauf, F., Scheider, S., Bartsch, Jan., Herrmann, P., Radic, M., Rebbert, M., Nemat, A. T., Schlueter Langdon, C., Konrad, R., Sunyaev, Al., & Meister, S. (2022). Linking Data Sovereignty and Data Economy: Arising Areas of Tension. Wirtschaftsinformatik 2022 Proceedings. 19. https://aisel.aisnet.org/wi2022/it_for_development/it_for_development/19
44. Lehtiniemi, T. (2017). Personal data spaces: An intervention in surveillance capitalism? Surveillance & Society, 15(5), 626–639. <https://doi.org/10.24908/ss.v15i5.6424>
45. Lähteenoja, V. (2023). What are “personal data spaces”? In Companion Proceedings of the ACM Web Conference 2023 (WWW '23 Companion) (pp. 1–5). ACM. <https://doi.org/10.1145/3543873.3587656>
46. Lähteenoja, V., Flanagan, A. J., & Warren, S. (2021) On the importance of human centrality. World Economic Forum https://www3.weforum.org/docs/WEF_On_the_Importance_of_Human_Centricity_2021.pdf
47. Lähteenoja, V., Leonard, M., Langford, J. (2024). Personal data spaces: Workshop series. Publications Office of the European Union. <https://doi.org/10.2760/748099>
48. Maailmapank. (2021). The social contract for data. <https://wdr2021.worldbank.org/stories/the-social-contract-for-data>
49. Majandus- ja Kommunikatsiooniministeerium. (2021). Digiühiskonna arengukava 2030. <https://www.mkm.ee/digiriik-ja-uhenduvus/digihiskonna-arengukava-2030> ning

- <https://valitsus.ee/sites/default/files/documents/2021-12/Eesti%20digi%C3%BChiskond%202030.pdf>
50. Manohar, S., Kapoor, A., Ramesh, A. (2019). Understanding data stewardship: taxonomy and use cases. Aapti Institute. <https://thedataeconomylab.com/wp-content/uploads/2020/06/Understanding-Data-Stewardship-Aapti-Institute.pdf>
 51. Masso, A., Tiidenberg, K., Siibak, A., Pahtma, L (2020) Kuidas mõista andmestunud maailma? Metodoloogiline teejuht. TLÜ Kirjastus
 52. Micheli, M., Farrell, E., Carballa Smichowski, B., Posada Sanchez, M., Signorelli, S. and Vespe, M. (2023). Mapping the landscape of data intermediaries, Publications Office of the European Union <https://doi:10.2760/261724>
 53. Mikiver, M. (2023). Isikuandmeid riskasutav e-riik ja seadusereservatsioon. Kas efektiivsus tõrjub põhiseaduslikud nõuded? Riigiõiguse aastaraamat 4/2023, lk 54–92; lk 92.
 54. Modhvardia, V., Reid, A. (2024). Participatory inclusive data stewardship. Ada Lovelace Institute. <https://www.adalovelaceinstitute.org/report/participatory-inclusive-data-stewardship/>
 55. Mötte, M., Espenberg, S., Vörk, A., Lehes, L., Saaroja, A., & Sepp, T. (2024). Eesti andmemajanduse turuväärtuse hindamise metoodika koostamine ja selle tulemuslikkuse hindamine. Tartu Ülikool, Sotsiaalteaduslike Rakendusuuringute Keskus & STACC OÜ. https://www.kratid.ee/_files/ugd/2d9e67_831b07fcab9c41c78748f6444d22cfa4.pdf
 56. MyData Global (2017). MyData declaration. <https://mydata.org/declaration>
 57. MyData Global (2025). MyData Awards. <https://mydata.org/participate/awards/>
 58. Norman, D. A. (2019). The four fundamental principles of human-centered design and application. <https://jnd.org/the-four-fundamental-principles-ofhuman-centered-design-and-application/>
 59. Open Data Institute. (2018). What is a data trust? <https://theodi.org/insights/explainers/what-is-a-data-trust/>
 60. Project VRM. (2025). About Project VRM. <https://projectvrn.org/about/>
 61. Reimsbach-Kounatze, C., Molnar, A. (2024). The impact of data portability on user empowerment, innovation, and competition. Going Digital Toolkit Note, No. 25. OECD https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/the-impact-of-data-portability-on-user-empowerment-innovation-and-competition_ee329380/319f420f-en.pdf
 62. Riigihangete register. (2025). „Tulevikukindel andmemajanduse ökosüsteem ja taristulised lahendused: inimese digitaalse kaksiku kontseptsioon ja prototüüp“ loomine. <https://riigihanked.riik.ee/rhr-web/#/procurement/8849884/documents?group=B>
 63. Riigi Infosüsteemi Amet (2025) Riigiportaali eesti.ee. <https://www.ria.ee/riigi-infosusteem/personaali/riigiportal-eestiee>
 64. Riigi Infosüsteemi Amet (2025). Andmenõusolekuteenus. <https://www.ria.ee/riigi-infosusteem/inimkeskne-andmehaldus/andmenousolekuteenus>
 65. Riigi Teataja (2025) Rahvastikuregistri seadus. <https://www.riigiteataja.ee/akt/118102024004>
 66. Riigi Teataja (2025) Tervise infosüsteemi põhimäärus, <https://www.riigiteataja.ee/akt/105042023019?leiaKehtiv>
 67. Scheider, S., Lauf, F., Geller, S., et al. (2023). Exploring design elements of personal data markets. Electronic Markets, 33(28). <https://doi.org/10.1007/s12525-023-00646-3>
 68. Scheider, S., Lauf, F., Möller, F., et al. (2023). A reference system architecture with data sovereignty for human-centric data ecosystems. Business & Information Systems Engineering, 65, 577–595. <https://doi.org/10.1007/s12599-023-00816-9>

69. Sõnaveeb. (2025). <https://sonaveeb.ee> (viitega Raud, R. (2013). Mis on kultuur? Sissejuhatus kultuuriteooriatesse. TLÜ Kirjastus.)
70. Tervisekassa (2025). Terviseportaal. <https://tervisekassa.ee/tervisekassa/e-tervise-tooted/terviseportaal>
71. TietoEvy. (2021). Reaalajamajanduse majandusliku mõju uuringu lõpparuanne. https://realtimeeconomy.ee/sites/default/files/2021-12/reaalajamajanduse_majandusliku_moju_uuringu_lopparuanne.pdf
72. Vabariigi Valitsus (2021). Strateegia "Eesti 2035". <https://valitsus.ee/strateegia-eesti-2035-arengukavad-ja-planeering/strateegia> ja https://valitsus.ee/sites/default/files/documents/2021-06/Eesti%202035_PUHTAND%20%C3%9CLDOSA_210512_1.pdf
73. Verhulst, S., Sandor, L., Stamm, J. (2023). The urgent need to reimagine data consent. Stanford Social Innovation Review. https://ssir.org/articles/entry/the_urgent_need_to_reimagine_data_consent
74. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.

Lisad

Lisa 1: Intervjueeritud organisatsioonid

Intervjuud	Organisatsioon	Intervjueeritavate hulk
1	Athumi	2
2	Cachet	2
3	CompensaLife	2
4	CreditInfo	2
5	EdTech Estonia	1
6	ELIIS	1
7	Haridus- ja Teadusministeerium	1
8	Haridus- ja Teadusministeerium (2)	1
9	iGrant.io	1
10	Justiits- ja Digiministeerium	1
11	Kutsekoda	4
12	LHV	2
13	LKF / EKSL	2
14	Majandus- ja Kommunikatsiooniministeerium	1
15	PZU	2
16	Riigi Infosüsteemi Amet	2
17	Tallinna Tehnikaülikool	1
18	Töötukassa	3

Lisa 2: Intervjuu kava

I osa: Taust ja inimkeskse andmemajanduse hetkeseis

1. Palun kirjeldage, kuidas puutute oma töös kokku inimeste andmete korralduse või kasutamisega.
2. Millised on teie organisatsiooni peamised teenused / tooted, mis põhinevad inimeste andmete kas esmasel või teisesel analüüsimisel?
3. Milliseid väljakutseid olete tuvastanud?
4. Milline on teie hinnangul inimeste andmete korralduse hetkeseis teie valdkonnas (ja/või Eestis laiemalt)?
5. Millised takistused esinevad? Milliseid võimalusi näete?
6. Kas oskate tuua näiteid erasektori teenustest, mis võimestavad inimest oma andmeid kontrollima, kasutama ja jagama, nt paremate teenuste saamiseks?
7. Millistes valdkondades näete kõige suuremat võimalust inimkeskse andmekorralduse laiendamiseks (sh inimesi kaasata oma andmete jagamisse ning kasutamisse)? Miks?

II osa: Personaalse andmeruumi arengud

8. Mida tähendab teie jaoks isikliku vaate omamine oma andmetele ning andmepõhiste teenustele?
9. Milline on teie arvates inimeste roll oma andmete kontrollimisel, jagamisel ning kasutamisel (teie tegevusvaldkonnas)?
10. Kas ja milliseid võimalusi näete inimeste rolli suurendamiseks oma andmete haldamisel ning jagamisel?
11. Milline on teie arvates ettevõtete ja organisatsioonide huvi ja võimekus:
 - a. inimestega seonduvaid andmeid jagada, müüa, osta ja väärindada?
 - b. luua inimestega seotud andmete põhiseid tooteid ja teenuseid?
12. Millised tegurid toetavad ja/või pärsivad teie arvates personaliseeritud teenuste ning inimkeskse andmekorralduse arenguid: õiguslikud, tehnoloogilised, ärilised, poliitilised ja ühiskondlikud eeldused/takistused)?

Kokkuvõte

- Küsimusi meile?
- Järgmised uuringu tegevused ning sündmused
- Keda võiksime veel intervjuuerida?

Lisa 3: Intervjuu kava 2

Uuringu hilisemas etapis kohendati intervjuu kava, et veelgi selgemalt uurida kasutuslugude teostatavust seotud osapooltega.

I osa: Vaade teie organisatsioonile ning andmepõhiste teenustele

1. Palun kirjeldage, kuidas puutute oma töös kokku inimeste andmete korralduse või kasutamisega.
2. Milliseid on teie organisatsiooni peamised andmepõhised teenused, milleks te kogute ning kasutate inimeste kohta käivaid andmeid?
3. Milliseid takistusi või väljakutseid olete tuvastanud andmepõhiseks teenusearendusel ja/või andmete laiemaks väärindamisel?
4. Millisel viisil te inimeste andmeid kogute?
(Näiteks otse inimestelt või organisatsioonidelt küsides; kolmandate osapoolte (nt teised riigiasutused, ettevõtted) kaudu; andmevahendajate kaudu? Kas te olete ka andmeid ostnud?)
5. Kas ja millisel määral te vahendate andmeid (sh isikuandmeid) või andmetooteid teistele osapooltele?

Kui jah, siis kas seate andmete jagamisel ka tingimusi (nt kasutustingimused, tasu küsimine vms)?

II osa: Võimalik personaalse andmeruumi kasutuslugu

Kaasuse lühitutvustus: Täna on haridus- ja oskusteave killustunud, mistõttu puudub töötajal terviklik ja ajakohane ülevaade oma pädevustest (sh võrdluses teistega) ning töandjal usaldusväärne, kiiresti kontrollitav info kandidaatide kompetentside kohta. Personaalne andmeruum koondab inimese haridus-, kvalifikatsiooni- ja täiendõppe andmed ühtseks vaateks. Töötaja saab hallata ja jagada digitaalselt tõendatud diplomeid, sertifikaate ja oskusi ajutise ning kontrollitud ligipääsu kaudu. Lisaks võimaldab lahendus siduda olemasolevad pädevused kutsestandardite ja tööturu vajadustega, pakkudes soovituslikke õpiteekondi ja tuge karjäärivalikutes. Töandjale tähendab see kiiremat ja kulutõhusamat värbamist: koondatud, valideeritud ja ajakohased andmed vähendavad taustakontrolli koormust ning kiirendavad otsustusprotsessi.

Kaasuse lühitutvustus 2: Elu- ja tervisekindlustuse riskihindamine tugineb täna killustatud ja ebaühtlase kvaliteediga andmetele, muutes protsessi ajamahukaks ja ebatäpseks. Personaalne andmeruum koondab inimese andmed turvalisse, kliendi volitusel jagatavasse keskkonda, võimaldades kindlustusandjal hinnata riske automaatselt, kiiremini ja täpsemalt. Personaalses andmeruumis integreeritakse registriandmed, kindlustusajalugu, tervise- ja käitumuslikud andmed. Tulemuseks on ajakohane ja terviklik riskiprofiil ning õiglasem, personaalsem hinnastamine. Lahendus vähendab eri osapooltele halduskulusid ja pettuseriski ning toetab andmete taaskasutust kogu teenuse elutsükliks, pakkudes võimalusi uuteks ärimudeliteks.

6. Kui a) oluliseks ja b) realiseeritavaks te seda kaasust peate?

7. Millised võimalusi ja/või kitsaskohti näete?
8. Milliseid arenguid on vaja teha, et antud kaasust realiseerida (kui üldse)?
9. Milliseid alternatiivseid võimalusi näete isikuandmete taaskasutamiseks teie tegevusvaldkonnas?

III osa: Personaalse andmeruumi arengud

10. Milline on teie arvates inimeste roll oma andmete kontrollimisel, jagamisel ning kasutamisel (teie tegevusvaldkonnas)?
11. Milliseid funktsionaalsusi oleks inimestele vaja pakkuda (teie tegevusvaldkonnas), et toetada inimeste kontrolli oma andmete üle ning samal ajal toetada andmete taaskasutust ning teenuste arendust? (soovitame ka unistada, mõeldes kaugema tuleviku peale)

(Kui jääb aega)

12. Millised tegurid toetavad ja/või pärivad teie arvates personaliseeritud teenuste ning inimkeskse andmekorralduse arenguid: õiguslikud, tehnoloogilised, ärilised, poliitilised ja ühiskondlikud eeldused/takistused)?

Kokkuvõte

- Küsimusi meile?
- Järgmised uuringu tegevused ning sündmused
- Keda võiksime veel intervjuuerida?