

Kokkuvõte plaanitava riigihanke “Turvaline andmete riskasutus era- ja avaliku sektori vahel” tehnilise kirjelduse kavandist

Käesolev dokument ei ole siduv ning hanke tehnilise kirjelduse parameetrid ja sisu võivad enne hanke väljakuulutamist muutuda.

Probleemipüstitus

Eesti andmemajanduse potentsiaali pärsib lahenduste puudumine, mis võimaldaks sektorite vahel andmeid tõhusalt vääridada ning seeläbi kvaliteetsemaid teenuseid luua ja pakkuda. Eriti napib avaliku ja erasektori vahelise andmete riskasutamise näiteid, kuna on keeruline erinevatel eesmärkidel kogutud andmeid, näiteks avaliku ja erasektori andmeid, omavahel siduda ja nendest uut väärtust luua. Puudub terviklahendus, mis arvestades kohalduvaid andmekaitse reegleid ja õiguslikke küsimusi, võimaldaks paindlikult ja turvaliselt erinevate osapoolte andmeid omavahel siduda ja analüüsida, tagades nende privaatsuse ja konfidentsiaalsuse.

Selleks, et eri osapoolte andmeid omavahel turvaliselt kokku panna, tuleb luua uuenduslik terviklahendus, kus töödeldavate andmete privaatsus on tagatud näiteks privaatsuskaitse tehnoloogia(te) toel. Seni on privaatsuskaitse tehnoloogiate kasutuselevõtt avaliku sektori poolt takerdunud, kuna esmane rakendamine on tehniliselt ja õiguslikult keerukas, ressursimahukas ning nõuab paindlikku lähenemist.

Eesmärk

Hangitava töö eesmärk on analüüsitöö tulemusena luua eeldused ja raamistik, et teostada ühe või vajadusel mitme katseprojekti tehnoloogiline lahendus, mis võimaldab kokkulepitud andmekoosseisude turvalist riskasutamist era- ja avaliku sektori osapoolte vahel. Lõppeesmärk on kujundada välja teenuse pakkumuse kontseptuaalne terviklahendus.

Töö tuleb teostada etappidena, kus iga etapp annab sisendi järgmiseks etapiks ning iga etapi lõpus toimub hindamine järgmise etapi teostatavuse ning selle tingimuste osas.

Tellitakse järgmised tööd, mis on jagatud etappidesse järgnevalt:

1. andmete turvalise riskasutamise eelduste analüüs, õigusliku ja tehnoloogilise raamistiku koostamine, sealhulgas konkreetse privaatsuskaitse tehnoloogia väljavalimine;
2. andmete turvalise riskasutamise tehnoloogilise lahenduse kavandamine, elluviimine ja testimine kokkulepitud ühe või vajadusel mitme katseprojekti alusel;
3. teostatud tehnoloogilise lahenduse laiendatavuse ja tasuvuse analüüs, et kujundada välja andmete riskasutamise teenuse pakkumise kontseptuaalne terviklahendus.

Oodatavad tulemid

Hangitava töö tulemusel valmib läbi katsetatud **terviklik raamistik, tehnoloogiline lahendus ja teenuse pakkumise terviklahendus, mis võimaldaks era- ja avaliku sektori andmete turvalise riskasutamise**

teenuse kasutusele võttu. Selleks analüüsitakse muuhulgas teenuse laiendatavust ja tasuvust, et tagada selle sobivus era- ja avaliku sektori vajadustele ja võimalustele.

Oodatavate tulemite kavandamisel peab arvestama muuhulgas:

- Turvaline andmete riskasutamise teenus peab olema kasutatav võimalikult paljude andmevaldajate ja -omanike vahel. Teenuse sisendandmete pakkujaks kui ka väljundandmete kasutajaks võivad olla nii erasektori, mittetulundussektori (edaspidi ühiselt *erasektor*), kui avaliku sektori asutused ning kõik muud andmevaldajad või -omanikud.
- Korduvkasutatavus – lahendus peab olema selline, mis võimaldab seda korduvalt kasutada erinevates andmete riskasutamise projektides/andmetöötlusülesannetes, ilma et iga kord tuleks luua uus raamistik, meetodika ja tehnoloogiline teostus (välja arvatud iga järgneva projekti/ülesande erisustest tingitud täiendavat tööd vajavad aspektid).
- Laiendatavus ehk skaleeritavus – lahendus peab olema kohandatav erinevatele andmekogudele ja andmestikele ning andmetüüpidele ja andmevajadustele.
- Turvaline andmetöötlus – loodud tehnoloogiline lahendus peab vastama turvanõuetele, mis võimaldavad töödelda konfidentsiaalseid ja isikuandmeid. Turvanõuete tase määratletakse analüüsi käigus ning sõltub ka katseprojekti teiste osapoolte ootustest.
- Sisendandmete töötlemise käigus peab kasutama privaatsuskaitse tehnoloogiat, mis kaitseb kõiki sisendandmeid ning nendele andmetele ei pääse andmeid tuvastaval viisil ligi keegi peale sisendandmete pakkuja. Samuti peab olema tagatud, et väljundandmed oleksid sellised, mis välistavad konfidentsiaalsuse või privaatsuse riive.
- Esimeses etapis teostatav analüüs võib siintoodud ootuste nimekirja täiendada.

Järgnevalt on täpsemalt kirjeldatud etappide oodatavad tulemid.

Esimene etapp: Andmete turvalise riskasutamise eelduste analüüs, õigusliku ja tehnoloogilise raamistiku koostamine, sealhulgas konkreetse privaatsuskaitse tehnoloogia väljavalimine

Töö eesmärk

Esimese etapi eesmärk on tuvastada töö õnnestumiseks vajalikud eeldused ja leida sobivad lahendused selle elluviimiseks. Selle etapi alusel hinnatakse, kuidas on võimalik töö eesmärki saavutada ning kas ja kuidas jätkatakse töö teise etapi ehk katseprojektiga. Esimene etapp on ühtlasi töö eesmärgi ja selle lahenduse valideerimine (*Proof of Concept*), tõestamaks, et planeeritav lahendus võiks teoreetiliselt töötada ja saavutada töö eesmärgi, arvestades asjassepuutuvaid õiguslikke, tehnoloogilisi, meetoodilisi, teostatavuse, tasuvuse jt aspekte.

Teostatavad tööd

Õiguslike nõuete analüüs

Õiguslike nõuete analüüsi käigus tuleb välja selgitada hanke tehnilises kirjelduses määratletud turvalise andmete riskasutamise võimaldamise ja katseprojektide eeltingimused ning selle põhjal hinnata teise etapi otstarbekust ja ulatust.

- **Euroopa Liidu õigusraamistik** Turvalise andmete riskasutamise lahendus ja katseprojekt(id) peavad olema kooskõlas Euroopa Liidu õigusaktidega, sealhulgas isikuandmete kaitse üldmääruse ([link](#)), e-privatsuse direktiivi ([link](#)), Euroopa statistika määruse ([link](#)) jt asjassepuutuvate õigusaktidega.
- **Eesti õiguslik raamistik ja selle võimalused** Õiguslike nõuete analüüs peab pakkuma lahenduse, kuidas olemasoleva Eesti õigusraamistiku piires, sh näiteks isikuandmete kaitse seadus ([link](#)), elektroonilise side seadus ([link](#)) ja riikliku statistika seadus ([link](#)), on võimalik turvalist andmete riskasutust ja katseprojekte tervikuna või osaliselt ellu viia.
- Õiguslike nõuete analüüs peab andma vastused muuhulgas järgmistele küsimustele:
 - Kas valitud PET-i kasutamisel on tegemist isikuandmete töötlemisega?
 - Kui PET-i kasutamisel on tegemist isikuandmete töötlemisega, siis:
 - Kes on andmete vastutav ja volitatud töötleja?
 - Milline on isikuandmete töötlemise õiguslik alus?
 - Millised on andmete riskasutamise võimaldamise eeltingimused, sealhulgas töödeldavatele andmetele rakenduvad õiguslikud nõuded?
 - Millise detailsusega (madalaima agregeerituse tasemega, nt mikroandmed, anonüümitud andmed, agregeeritud andmed) on võimalik andmeid omavahel siduda, arvestades nii õiguslikke piiranguid kui ka tehnoloogilisi võimalusi?
 - Millised on õiguslikud nõuded PET-ile?
 - Millised on peamised õiguslikud väljakutsed seoses (isiku)andmete linkimise ja PET-ide kasutamisega? Millised on lahendused?
 - Kas ja milliseid täiendavaid nõudeid või piiranguid tuleb andmete riskasutamisel arvestada sõltuvalt andmete kogumise eesmärgist (nt avalik-õiguslikul, statistilisel või eraõiguslikul eesmärgil kogutud andmed)?
- **Seadusandlikud takistused ja võimalikud muudatused** Kui analüüsis jõutakse järeldusele, et turvalise andmete riskasutamise lahendus või katseprojekt ei ole Eesti kehtiva õiguse raames võimalik, siis peab analüüs:
 - selgitama, milles seisnevad õiguslikud takistused;
 - pakkuma konkreetseid ettepanekud õigusaktide muutmiseks (vajadusel koostada väljatöötamiskavatsus, eelnõu ja seletuskiri).

Kui analüüsis selgub, et lahendus on osaliselt võimalik, peab analüüs:

- määratlema, millises ulatuses on turvaline andmete riskasutamise või katseprojekti teostamine võimalik;
- pakkuma konkreetseid ettepanekud õigusaktide muutmiseks (vajadusel koostada väljatöötamiskavatsus, eelnõu ja seletuskiri), mis võimaldaksid lahendust täielikult rakendada.

Märkus: Hankija kaasab õiguslike nõuete analüüsi läbiviimisse justiits- ja digiministeeriumi ning andmekaitse inspeksiooni eksperdid, kes valideerivad ja nõustavad töö käigus tekkivaid õiguslikke küsimusi ja lahendusi. Lisaks osalevad töös transpordiameti eksperdid, kes aitavad hinnata katseprojekti kasutatavate andmete linkimise mõju tulemuste kvaliteedile.

Metoodika analüüs

- Teenuse toimimiseks vajalike protsesside ja metoodiliste tingimuste kirjeldus;
- Protsessijoonis(ed) ja võtmekasutajate teekonnad.

Tehnoloogiline analüüs

- Tehnoloogiliste ja tarkvaraliste võimaluste analüüs (millised võimalikud PET lahendused tagavad vajalikul tasemel turvalisuse)?
- Infoturbe nõuete analüüs, sh piisava turbetaseme tagamiseks vajalike nõuete kaardistamine.
- Sobivate lahenduste maksumus, sh millised on taristu (ning sellel toimiva teenuse) loomisega seotud ühekordsed kulud ning püsikulud? Millised on tehniliste komponentide nagu riist- ja tarkvara hooldus- ja halduskulud?

Teenuse pakkumuse analüüs eelistatud katseprojekti näitel

- Katseprojekti realiseerimise esialgne kuluanalüüs ja hinnastusmudel;
- Katseprojekti realiseerimiseks vajalike rollide ja nende täitmiseks nõutud kompetentside kirjeldus;
- Katseprojekti andmevajaduse kirjeldus, mis määratleb sisendandmetele esitatavad nõuded; seejuures andmete detailsus ja kvaliteet peavad toetama katseprojekti eesmärke;
- Õiguslikud, meetoodilised või tehnoloogilised **erinõuded**, et katseprojekti realiseerida.
- Millised on teenuse loomisel võimalikud alternatiivid ja nende kulukus?

Märkus: Pakkuja kaasab teadlasi ja spetsialiste, kellel on pädevus mobiilpositsioneerimise andmete töötlemise meetoodika vallas ning kes oskavad hinnata erineva detailsusastmega mobiilpositsioneerimise andmete linkimise täpsust, uurida meetoodilisi keerukusi nende seostamisel ja valitud meetodite mõju analüüsi tulemustele.

Lisaks peab esimese etapi analüüsidokument vastama järgmistele küsimustele:

- Millised on takistused ja nende lahendused andmete riskasutamiseks?
- Milline on ühiskonna hoiak lahenduse suhtes? Kas ja kuidas on vaja sellega tegeleda (teadlikkuse suurendamine, hoiakute muutmine positiivses suunas jms)?
- Millistel alustel toimub andmetöötlus (mida peab katma leping, kelle vahel see sõlmitakse)?

Esimese etapi tulemusel selgub, kas ja millistel tingimustel on võimalik teise etappi edasi liikuda ja katseprojekti realiseerida.

Teine etapp: Andmete turvalise riskasutamise tehnoloogilise lahenduse kavandamine, elluviimine ja testimine kokkulepitud ühe või vajadusel mitme katseprojekti alusel

Töö eesmärk

Eesmärk on rakendada esimeses etapis koostatud raamistikku ja välja töötada tehnoloogiline lahendus, mis täidab töö eesmärgi konkreetse katseprojekti näitel. Töö eesmärgi saavutamiseks ei piisa prooviversioonist või minimaalsest elujõulisest tootest; eesmärk on saavutada toimiv versioon, mida saab loodavas teenuses kasutusele võtta.

Kui mobiilpositsioneerimise andmete kasutamine vajalikul detailsuse tasemel ei ole mingil põhjusel võimalik, lepitakse Pakkuja ja Hankija vahel kokku alternatiivne lähenemine, mis täidab esimeses etapis analüüsitud raamistiku ja katseprojekti eesmärgi kõige lähemalt. Samuti võib analüüsitöö tulemusena osutuda vajalikuks mitme katseprojekti realiseerimine sarnastel alustel.

Esmatähtis on tagada andmete turvaline töötlemine, kus andmete sisu jääb teisele osapoollele nähtamatuks, säilitades täielikult andmete privaatsuse ja konfidentsiaalsuse. Andmetöötluse tulemuseks peavad olema agregeeritud statistilised andmed.

Teostatavad tööd

Tehnoloogiline lahendus

- Vastavalt esimeses etapis analüüsitud tehnoloogilistele lahendustele tuleb realiseerida väljavalitud lahenduse riist- ja tarkvaraline teostus, mis muuhulgas peab sisaldama:
 - äriprotsesside ja töövoogude kirjeldust, mida tuleks rakendada osalevate asutuste poolt;
 - üksikasjalikku arhitektuurijoonist koos selgitustega, sh andmete liikumise kirjeldust;
 - tarkvarakomponentide kirjeldust;
 - juhiseid kogu krüptograafilise materjali (võtmed, sertifikaadid jne) turvaliseks käsitlemiseks;
 - logimise protsessi ja logide väljundite kirjeldust.
- Riskide kirjeldamise ja hindamise tulemusena võib lahendus olla pilvepõhine.
- Katseprojekti jaoks kasutatav taristu peab tulema Pakkuja poolt, koos võimalusega jätta see testimise jaoks avatuks ka peale hankelepingu lõppu kokkulepitud ajaperioodiks.
- Lahendus peab vastama kõikidele vajalikele infoturbe ja andmekaitse nõuetele; sealhulgas tuleb tagada lahendusele turvauuendused, turvapaigad või muud parandused, kui katseprojekti käigusoleku jooksul avastatakse haavatavused, sissetungid, rikkumised või muud turvasündmused.
- Lahendus peab tagama korrektsed logimis- ja auditeerimisfunktsioonid, mis muuhulgas peavad võimaldama täiendavatel välistel audiitoritel, kes on töötlemisosapooltest sõltumatud, kontrollida rakendatud funktsioonide õigsust ning tagantjärele teostada järelevalvet.
- Loodav lahendus peab arvestama riigis kasutatavaid parimaid praktikaid, nt X-tee ([link](#)) ja ristfunktsionaalsed nõuded ([link](#)).

Andmete kaasamine ja tähelepanekud

- Koostöös pakkujaga on **hankija ülesanne** kaasata vajalikud andmed. Esimese etapi tulemuste põhjal tuleb enne andmete hankimist pakkuja poolt määratleda nende nõuded, sealhulgas vajalik detailsus katseprojekti eesmärkide saavutamiseks.
- Kui mikroandmete töötlemine on võimalik, tuleb tagada linkimiseks kasutatavate tunnuste kvaliteet. Agregeeritud andmete puhul tuleb välja töötada ja rakendada seostamise ja agregeerimise metoodika ning kehtestada reeglid, mis võimaldavad andmeid turvaliselt siduda.
- Andmetöötlusülesande tulemuseks peavad olema agregeeritud statistilised andmed. Tehnoloogiline lahendus peab tagama, et ükski muu teave peale lõplike statistiliste (anonüümsete, mitte-isikustatud) andmete ei avaldu ega leki ühelegi osapoollele (sealhulgas teistele sisend/väljund osapooltele ja töötlemisosapooltele) ning et andmetöötlusülesande tulemus avaldatakse ainult väljundosalpool(t)ele, kes on määratletud ülesande konfiguratsioonis.

Kokkuvõte katseprojektist

Pakkuja koostab **metoodikaraporti**, mis hõlmab ülevaadet järgnevast:

- kasutatud andmete kirjeldus, sh nõuded sisendandmetele ja nende kvaliteedile;

- rakendatud privaatsuskaitse tehnoloogiad, andmekaitse- ja turvameetmed;
- andmete seostamise ja agregeerimise meetodid;
- andmetöötluse etapid;
- väljundi kontrolli kirjeldus;
- õppetunnid, probleemid ja piirangud, mis katseprojekti testimisel ilmsid, koos võimalike lahendustega.

Teise etapi tulemusel peab konkreetse katseprojekti klient/väljundosaaj (transpordiamet) saama talle vajalikud kvaliteetsed ja usaldusväärsed andmed nii, et sisendandmete privaatsus ja konfidentsiaalsus on kaitstud.

Teise etapi tulemusel selgub, kas ja millistel tingimustel on võimalik kolmandasse etappi edasi liikuda.

Kolmas etapp: Teostatud tehnoloogilise lahenduse laiendatavuse ja tasuvuse analüüs, et kujundada välja andmete riskasutamise teenuse pakkumise kontseptuaalne terviklahendus

Töö eesmärk

Toetudes katseprojekti kogemusele, on kolmanda etapi eesmärk koostatud raamistiku, selle põhjal ellu viidud katseprojekti ning teostatud tehnoloogilise lahenduse laiendatavuse ja tasuvuse analüüs, mille pealt moodustub andmete riskasutamise teenuse pakkumise kontseptuaalne terviklahendus.

- **Laiendatavuse** (ehk skaleeritavuse) all peame silmas välja pakutud taristu võimet kohandada suureneva andmemahu ja kasutajate arvuga, säilitades samal ajal jõudluse, tehnoloogilise võimekuse ja turvanõuded kompromissideta. Hinnatakse, milline oleks süsteemi laiendatavus ka erinevates sektorites, sealhulgas tervishoiu-, haridus-, ja sotsiaalvaldkonnas, kus andmete riskasutus võiks tuua lisaväärtust.
- **Tasuvuse analüüsi** käigus hinnatakse, kui palju maksaks andmete riskasutamise teenuse pakkumine, sealhulgas taristu, halduse ja privaatsuskaitse tehnoloogia kulud. Samuti analüüsitakse, kuidas teenust rahastada ning millist majanduslikku ja sotsiaalset kasu või ressursside kokkuhoidu see kaasa tooks. Analüüsi tulemus hõlmab hinnangut süsteemi jätkusuutlikkusele tervikuna. Eesmärk on luua toimiv ärimudel, mis hõlmab lahenduse tasuvust, äristrateegiat (sihtrühm, nendeni jõudmine, tellimuste tagamine) ning määratleda, kes võiks teenust pakkuda (riigiasutus või erasektor) ja millistel tingimustel.

Teostatavad tööd

- Tehnoloogiliste parameetrite, sh taristu ja tarkvarade kaardistus, mis on vajalikud katseprojekti kogemusele tuginedes uute sarnaste andmetöötlusülesannete elluviimiseks tulevikus;
- Õiguslike ja tehnoloogiliste parameetrite laiendamise võimalused teistele andmetüüpidele, võimalikult standardsel kujul;
- Tasuvushinnang, mis keskendub loodava süsteemi majandusliku ja sotsiaalse kasu hindamisele, võrreldes seotud kuludega. Hinnatakse loodava süsteemi kasutatavust ja seda, millist väärtust see loob;
- Katseprojekti näitel koostatud hinnastusmudeli ja ressursimudeli täpsustamine ja teenuse pakkumise tarbeks kohandamine;

- Osapoolte rollid, vastutused, volitused ja tegevused uue teenuse loomise juures;
- Uue teenuse loomise protsessijoonis, arhitektuurijoonis ja ajaline teekaart.

Lisaks peab kolmanda etapi analüüs vastama järgmistele küsimustele:

- Millised on võimalikud tuluallikad (nt tõhususe kasv, parem otsustusvõime, suurem turvalisus, sotsiaalne ja majanduslik kasu)?
- Mis on selle süsteemi potentsiaalne kasutajate hulk ja nende valmisolek süsteemi kasutusele võtta?
- Milline on süsteemi loomisega kaasnev kasu võrreldes riskidega, mis kaasnevad turvaliste lahenduste puudumisega?

Ootused pakkumusele

Ootame tervikpakkumuse esitamist, kus:

- Esimese etapi kohta on esitatud projektiplaan suurte tegevuste komponentide kaupa kuude lõikes, koos toodud komponentide elluviimiseks vajalike tegevuste kirjeldusega;
- Tervikkirjeldus kõigi töö etappide üleselt, kus oleks välja toodud terviklik nägemus projekti realiseerimise võimalustest ja Pakkujale olulistest ettepanekutest.

Ootused I etapi projektiplaanile

- Projektiplaanis on toodud tegevuste jaotus koos teostatavate tööde kirjeldusega, vajadusel on tööd jaotatud alametappidesse; teostatavate tööde kirjeldus peab võimaldama aru saada, millised on nende tööde tulemid;
- Tegevuste jaotus on ajaliselt toodud kuude lõikes, ühtlasi on välja toodud I etapi realiseerimiseks kuluv koguaeg. Koguaeg võib olla esitatud ajavahemikuna, kuna töö ajaline kestus sõltub regulaarsetest aruteludest ja agiilsete iteratsioonide tulemustest;
- Projektiplaanis on välja toodud maksumused ja/või maksumuse vahemikud ning peab olema selgelt aru saada, kuidas hind on moodustunud;
- Projektiplaanis on välja toodud ressursside jaotus ja kasutus;
- Projektiplaanis on viited kasutatavale metoodikale nende tegevuste juures, kus see on võimalik;
- Kommunikatsiooniplaan, mis kataks nii regulaarse kommunikatsiooni Hankijaga, vajaliku kommunikatsiooni partneritega ning teiste osapooltega; vajadusel võib Pakkuja lisada ajakavva juba ette täiendavaid arutelusid Hankija ja Pakkuja vahel, kui ta peab seda täiendavalt ja töö iseloomust tulenevalt vajalikuks.

Ootused tervikkirjeldusele

- Tervikkirjeldus peab katma Pakkuja arusaama Hankija vajadusest, töö ülesannetest ja töö lõppeesmärgist;
- Pakkuja nägemus kaasamiskavast, milles on välja toodud huvirühmade nimekiri ning planeeritud kaasamistegevuste indikatiivne ajakava ja seos töö tegemise etappidega;
- Riskide kaardistus, kus on toodud projekti spetsiifikat arvestavad asjakohased (sh lahendusest tulenevad) riskid, nende tõenäosuse ja mõju hindamine ja riskikäsitlemise kirjeldus;
- Pakkuja nägemus koostööst Hankija ja projekti partneritega ning teiste seotud osapooltega;

- Pakkuja projektimeeskonna koosseis, kogemus, kompetentside kirjeldus ning tööjaotus.

Tähtajad

Töö indikatiivsed tähtajad etappide kaupa:

- I etapi tulemite tähtaeg on maksimaalselt 5 kuud hankelepingu sõlmimisest;
- II etapi tulemite tähtaeg on maksimaalselt 6 kuud I etapi tulemite üleandmisest Pakkujalt Hankijale;
- III etapi tulemite tähtaeg on maksimaalselt 2 kuud II etapi tulemite üleandmisest Pakkujalt Hankijale;

Ootused Pakkuja meeskonnale

- Õigusliku ja tehnoloogilise analüüsi koostamise pädevus;
- Kogemus privaatsuskaitse tehnoloogiate rakendamisel või vastavate lahenduste pakkumine;
- Kogemused andmetöötluse ja majandusanalüüsi valdkonnas, et tagada põhjalik ja objektiivne hinnang süsteemi tasuvusele ja laiendatavusele;
- Infoturbe alased teadmised ja kogemused, et hinnata lahenduse turvalisust;
- Pädevus mobiilpositsioneerimise andmete töötlemise metoodika vallas ning oskus hinnata erineva detailsusastmega mobiilpositsioneerimise andmete linkimise täpsust, uurida metoodilisi keerukusi nende seostamisel ja valitud meetodite mõju analüüsi tulemustele.