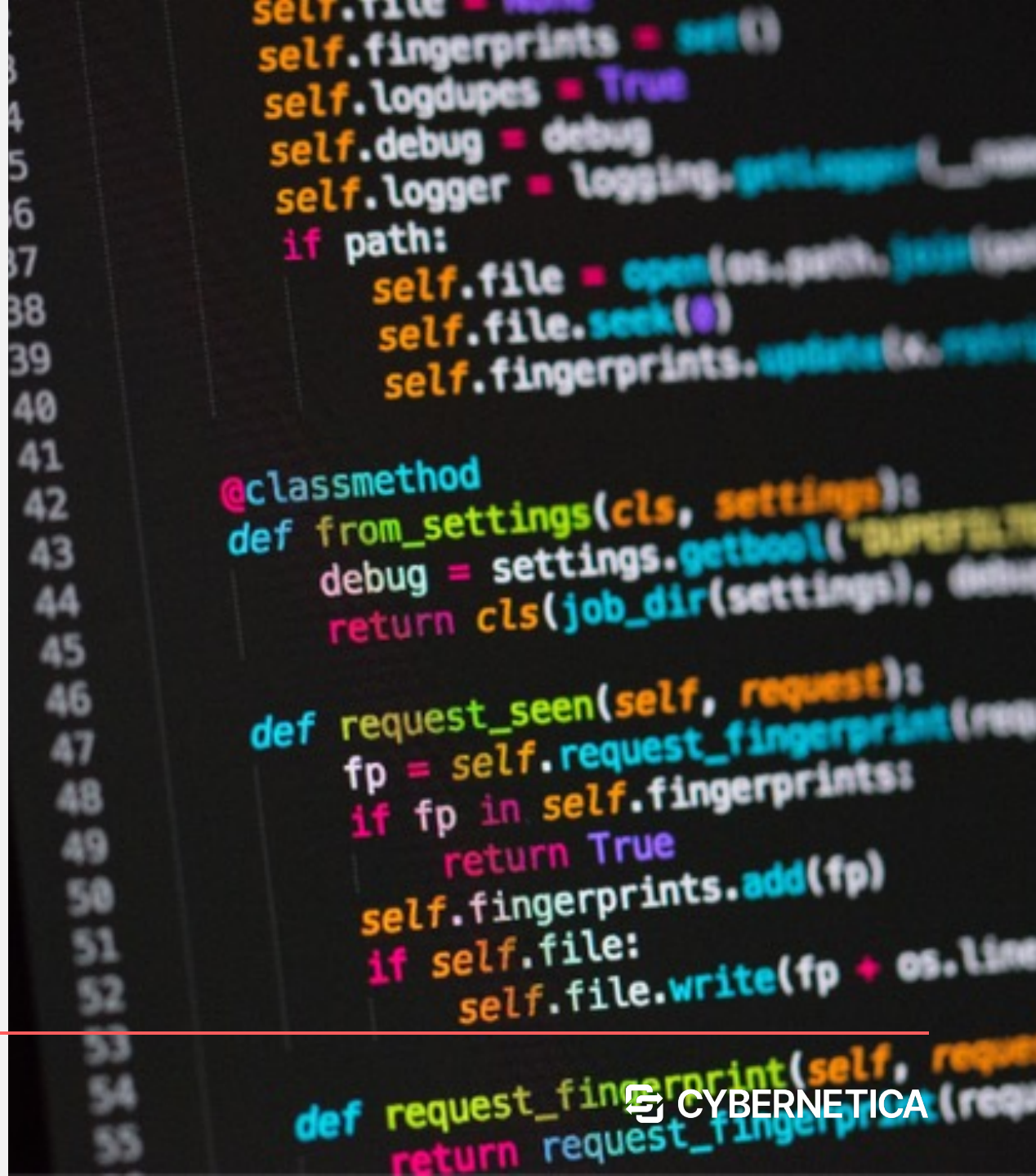
Privaatsuskaitse tehnoloogiate kontseptsioon ja teekaart

Liina Kamm
Dan Bogdanov

CYBERNETICA

Tänane kava

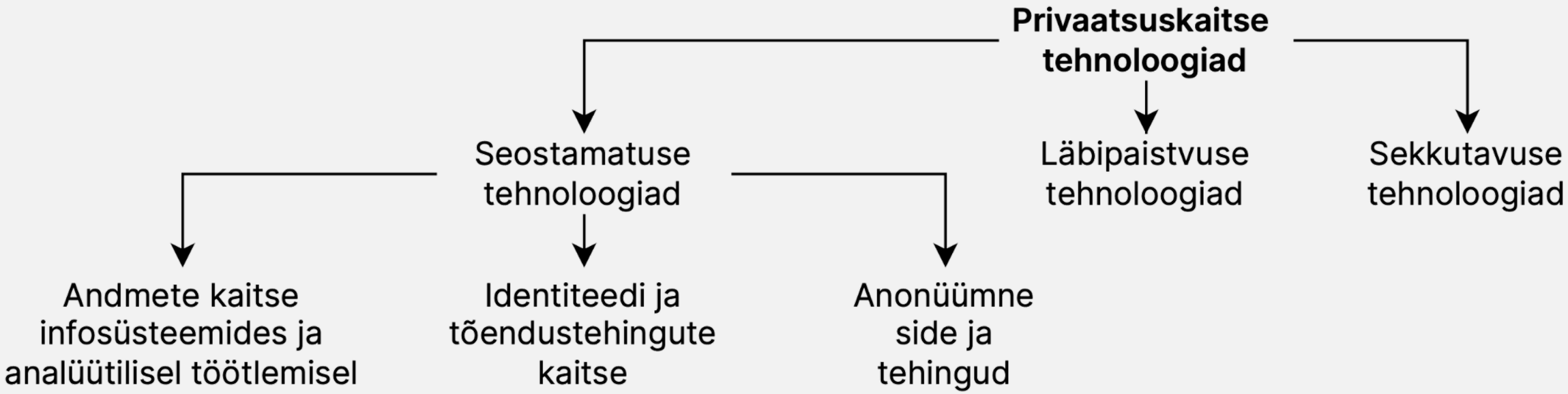
- Mis on privaatsuskaitse tehnoloogiad?
- Milleks need Eestile vajalikud on?
- Kuidas neid e-riigi süsteemides juurutada?
- Ülevaade aruandest
  - tehnoloogiate kirjelduste lugemisjuhend,
  - ülevaade riikide kogemusest,
  - e-riigi kasutusjuhtude lugemisjuhend.
- Ülevaade intervjuudest riigiasutustega
- Väljavõte teekaardist
  - Platvormid ja taristu
  - Täiendavad ideedd



CYBERNETICA

Mis on privaatsuskaitse tehnoloogiad?

- **Privaatsuskaitse tehnoloogiad** on info- ja side- tehnoloogilised meetmed, tooted või teenused, mis kaitsevad privaatsust andmete välistuse või vähendamisega või isikustatavate andmete tarbetu ja/või soovimatu töötluse vältimisega, samas säilitades süsteemi võimed.



Milleks meile privaatsuskaitse tehnoloogiad?

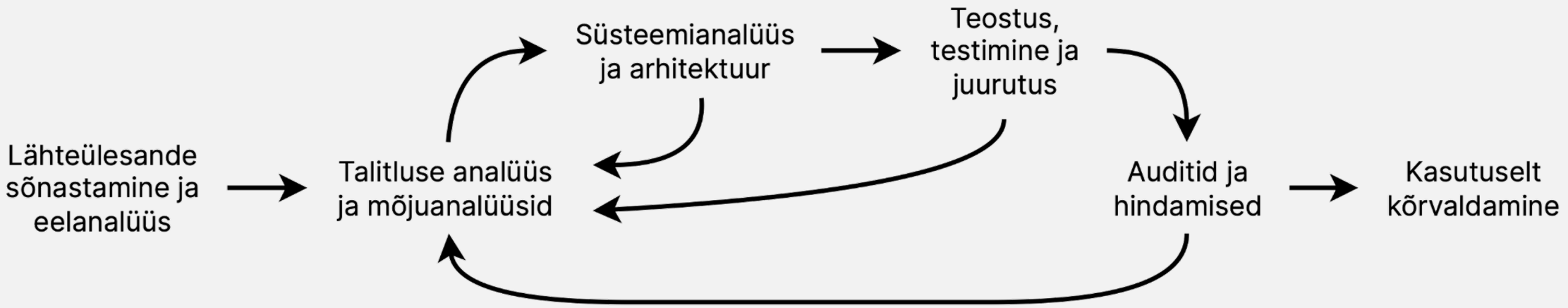
1. Eesti Vabariigi digiühiskonna arengukava aastani 2030:
   - põhiõiguste, sh privaatsuse kaitse on üks digiühiskonna põhimõte
   - inimkeskse digiriigi areng on üks arenguhüppe võimalus
2. Privaatsustehnoloogiad võimaldavad uute teenuste loomist.
3. Privaatsustehnoloogiad kaitsevad ka ettevõtete andmeid.
4. Privaatsustehnoloogiad toetavad lõimitud andmekaitset
   - (vt isikuandmete kaitse üldmääruse artikkel 25)

Väärtusahelad ja tulud Eesti riigi jaoks

(Kõigi seostega version on uuringu aruandes)

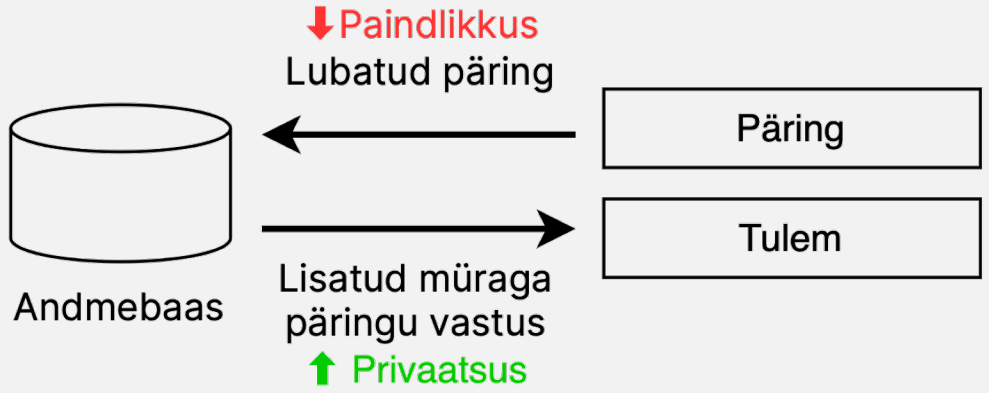
CYBERNETICA

Privaatsustehnika süsteemide elutsüklis



- **Uutes süsteemides** peab privaatsustehnika ja -tehnoloogiate rakendamise panna **lähteülesandesse ja nõuetesse**.
- **Olemasolevates süsteemides** tuleb uued privaatsustehnika nõuded lisada **süsteemide uuendamise käigus**. Selleks sobivat hetke peab vastutav töötleja ise tähele panema!

Iga PETi kohta on ülevaatetabel ja pikem tekst

Diferentsiaalprivaatsus *(differential privacy)*	ANDMED
Lühidalt: Diferentsiaalprivaatsus teeb päringu vastused juhuslikuks nii, et küsija ei saa aru, milliste isikute andmete pealt päring tehti.	**Arenduse keerukus:** kõrge **Ülalpidamise keerukus**: madal **Täpsus**: ebatäpne (sõltub lisatavast mürast) **Privaatsusgarantii**: matemaatiliselt tõestatav **Tehnoloogia küpsus**: keskmine
Ülevaatlik mudel:  	**Turvaeeldused ja jääkriskid**: ... **Õiguspraktika**: ... **Rakendusvõimalused**: ... **Tuntumad rakendused**: ...

Andmete kaitse analüüsil

- Pseudonüümimine
- Anonüümimine
- Piirangutega päringuliidesed
- Analüütiku töökohad
- Diferentsiaalprivaatsus
- Liitõpe
- Sünteetiliste andmete genereerimine
- Usaldatavad täitmiskeskkonnad
- Homomorfne krüptograafia
- Turvaline ühisarvutus

Photo by Ryoji Iwata on Unsplash

CYBERNETICA

Photo by Chris Yang on Unsplash

Identiteedi kaitse

- Pimesignatuurid
- Rühma ja ringisignatuurid
- Atribuutkrüptograafia
- Nullteadmustõestused

CYBERNETICA

Anonüümne side

- Turvaline vestlus
- Mikservõrgud
- Sibulmarsruutimine

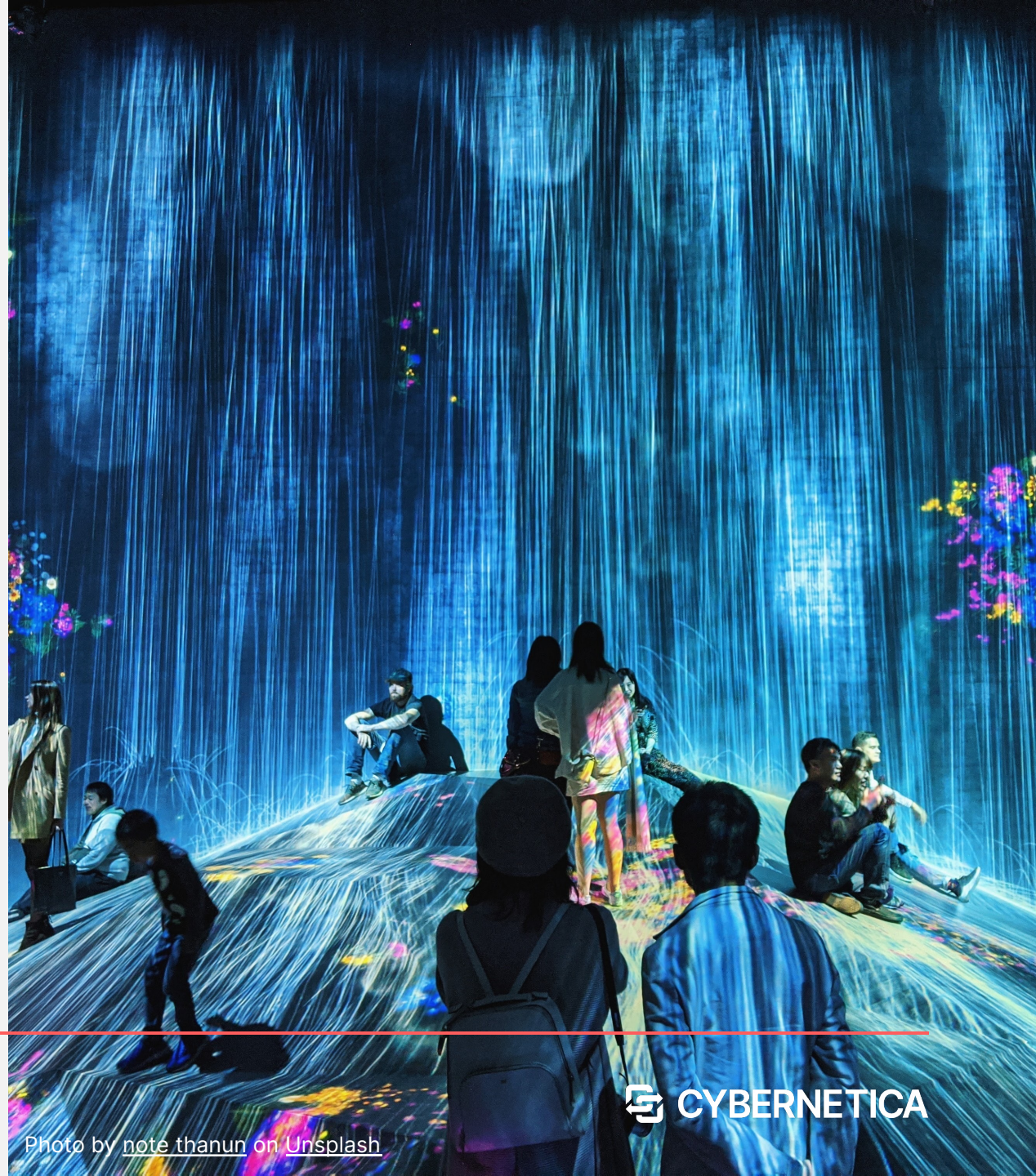


Photo by note thanun on Unsplash

CYBERNETICA

Photo by James Haworth on Unsplash

Läbipaistvus ja sekkutavus

Läbipaistvus

- Dokumenteerimine
- Logimine
- Osapoolte teavitamine

Sekkutavus

- Privaatsus- ja andmetöötluspaneelid ning iseteenindused
- Dünaamiline nõusolekute haldus

CYBERNETICA

Ülevaade teiste riikide rakendustest

- Uuringus kaetud riigid
  1. Ameerika Ühendriigid
  2. Holland
  3. Jaapan
  4. Kanada
  5. Prantsusmaa
  6. Singapur
  7. Ühendkuningriik
  8. Šveits

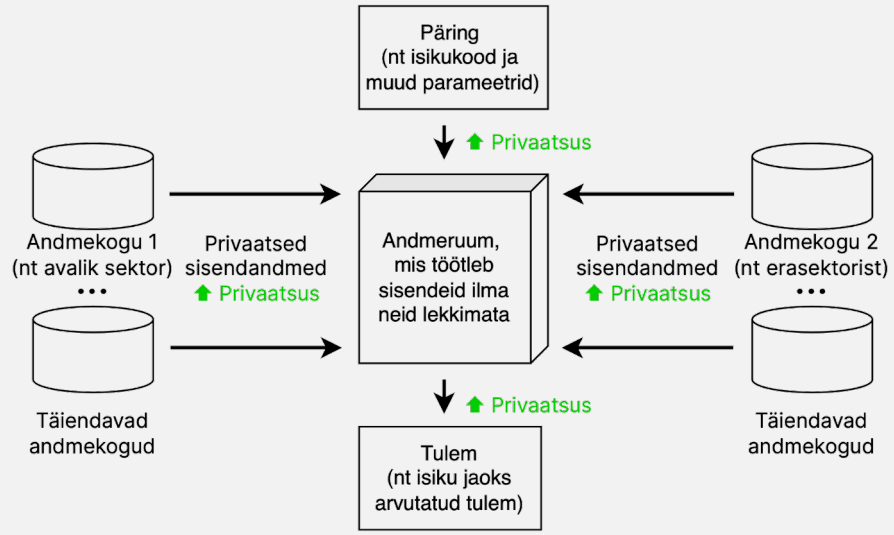
- Märkimisväärsed leiud
  - Ameerika Ühendriikide ja Ühendkuningriigi privaatsuskaitse tehnoloogiate programm
  - Singapuri privaatsuskaitse tehnoloogiate liivakast
  - Privaatsuskaitse tehnoloogiad Hollandi krüptograafia teekaardil

Üldised kasutusvõimalused Eesti digiriigis

Turvaline andmeruum avaliku ja erasektori andmetel põhinevate teenuste loomiseks

Lühidalt: Mitme (nt avaliku või erasektori) andmebaasi sisu põhjal osutatakse üksikisikule e-teenust.

Ülevaatlik mudel:



Sobivad privaatsuskaitse tehnoloogiad:

1. usaldatud käivituskeskkonnad
2. turvaline ühisarvutus
3. homomorfne krüptograafia

Tekkiv lisaväärtus:...

Privaatsuskaitse rakendamise eelised: ...

Konkreetsed rakendused:

1. Vajaduspõhised energia- ja muud toetused
2. Erasektori tervishoiuteenuse osutajate tervi-seandmete kaasamine riigi teenustesse
3. Positiivne krediidiregister
4. Digitaalne majutuskaart

Näidisrakendused: ...

Intervjuud riigiasutustega

1. Andmekaitse Inspektsioon (30.01.2023)
2. Justiitsministeerium (09.02.2023)
3. Majandus- ja kommunikatsiooniministeerium ja Transpordiamet (22.02.2023)
4. Maksu- ja tolliamet ning Rahandusministeeriumi Infotehnoloogiakeskus (14.02.2023)
5. Rahandusministeerium ja Finantsinspektsioon (03.02.2023)
6. Riigi Infosüsteemi Amet (31.01.2023)
7. Siseministeerium, Politsei- ja Piirivalveamet, Päästeamet ja Siseministeeriumi Infotehnoloogia- ja Arenduskeskus (08.02.2023)
8. Sotsiaalministeeriumi ja Tervise ja Heaolu Infosüsteemide Keskus (09.02.2023)
9. Statistikaamet (21.02.2023)
10. Tartu Ülikooli genoomika instituudi Eesti Geenivaramu (20.02.2023)
11. Tervisekassa (06.02.2023)

Intervjuude metoodika

- **Küsimused intervjueeritavatele**
  1. Kuidas teie organisatsiooni/valdkonna igapäevategevusse puutub privaatsuskaitse (või ka andmekaitse)?
  2. Missuguseid privaatsuskaitse lahendusi täna rakendate ning miks?
  3. Missuguseid teie asutuse/valdkonna (ka piiriülese koostöö) tänaseid väljakutseid võiks lahendada privaatsuskaitse tehnoloogiate abil ja mida positiivset see Eesti ühiskonnale kaasa tooks?

- **Tulemid**
  - Ülevaade asutuste kogemustest
  - Õigusruumi ülevaade ja poliitikasoovitused
  - Teekaart suurimatest vajadustest ja ühisest taristust

Teekaardi peamised süsteemid

Taristu	Rakendused	Loodav lisaväärtus
Personaliseeritud sündmusteenuste platvorm	1. Personaliseeritud otsetoetused 2. Sündmusteenused eriliigilistel andmetel	1. Erasektori andmete kaasamine 2. Kokkuhoid täpsematest andmetest 3. Sarnased teenused valmivad kiiremini
Andmekogudeülese analüütika platvorm	1. Ennetustöö 2. Uute teenuste arendus 3. Poliitikaanalüüs	1. Terve rahvastiku andmete koondamisel kahandavad PETid märkimisväärselt riske 2. PETid aitavad kaasata erasektori andmeid ja ka erasektori (ning välismaa) analüütikuid
Avaandmete taasisikustamise riski langetamine	1. Uute teenuste arendus 2. Teadus- ja õppetöö	1. Moodsad privaatsuskaitse tehnoloogiad lubavad isikustatavust mõõta ja võrrelda 2. Kaitse pikaajaliste ja linkimisrünnete eest
Digitaalse identiteedi logid ja analüütika	1. Autentimis- ja kehtivuskinnituste logimine ja analüütika	1. eIDAS 2.0 regulatsiooni andmekaitsenõuete saavutamine 2. Isikute profileerimise vältimine
Digiriigi sünteetiline teisik testimiseks	1. Teenuste arendamine ja testimine	1. Uute süsteemide kiirem testimine ja arendus 2. Isikuandmete vältimine arenduses ja testimises

Täiendavad ideed teekaardil

- **Uute asjade proovimine**
  1. Privaatsust säilitav kratiseansi klassifitseerija ja marsruutija pilootprojekt
  2. Privaatsuskaitse tehnoloogiatele toetuvad andmesaatkonnad
  3. Privaatsuskaitse tehnoloogiate kasutamine eriliigiliste isikuandmete töötlemisel mitte-Euroopa andmekeskustes ja pilves
  4. Kolmanda osapoole personaalmeditsiini otsusetoe süsteemide ühendamine Eesti terviseandmete külge

- **Teadmuse arendus**
  1. Privaatsuskaitse tehnoloogiad Eesti infoturbestandardis (E-ITS)
  2. Juhendmaterjalid ja näidisprojektid
  3. Standardite tõlkimine

Suured tänud!

cybernetica
CyberneticaAS
cybernetica_ee
Cybernetica