Privacy, security and trust for digital living

Mika Huhtamäki
Deputy CEO / Vastuu Group Oy

CxC Festival 2022
12 January 2022
Trust is more!

Business
Legal
Tech
Ethical
Trust in the smart city context
-Human centric data flows inside the city and 3rd parties

- Cities have multiple units - a collection of private-public organizations
- Sharing the data between those organizational units is vital for smooth services
- MyData operator and consents gives the required legal and tech connectivity for better services
What GDPR offers for trust
-six legal bases of processing personal data

Consent
- Can be withdrawn by data subject at any time
- Cornerstone for MyData

Contract and legitimate interests of the controller
- Limited right to withdrawal
- For example contract of employment
- Deniable only by terminating the agreement / not signing the agreement
- Some rights to access the data may remain after termination

Legal obligation, public task and vital interests
- No withdrawal right
- Obligation for companies for labor safety regulation, etc.
- Government's right to collect and access personal data for compliance with a legal obligation
- Processing is necessary to protect someone's life
Separate permission services
Permissions as a service?

• Growing and increasingly fragmenting data complicates the consent managements for the users
• Separate consent management services per data sources is not usable nor human centric approach
• Consent management as a service could be one solution
Changing current state with consent

Right to give, deny or revoke Purpose for the usage

Person

Data source

Consent requester
MyData operator does not touch or store the data!!

separation of concerns (architectural)

Identity Layer (Authentication)
- BankID, MobileID, FreijaID etc.

MyData Operator Layer (Permissions)
- Identity linking
- Registered data sources
- Registered data consumers
- Permission management services

Data Transfer Layer (Data operations)
- Data controllers and data processors
- Substance related obligations
- Data transfers
- Consent requests
- Data removal
Stakeholders and main capabilities of a MyDataShare operator platform

People

MyData Operator

Identity Services

Permission Management

Connectivity

Data Source

Data Using Service

Operator has responsibilities towards each actor!
Identifiers – “Distributed Privacy” – how separation promotes privacy

Organization A

MyData Operator
- Actual of identifiers e.g. social security number (SSN)
- Generated random identifier
  - Linked to the actual SSN

Operator has confirmed Identifiers but no actual Data

Organization B

Data Using Service
- Personal data
  - with generated id
- Generated identifier
  (by MyData Operator)

Service provider has Data but no actual Identifiers

Data linked to generated id
Distributed Privacy: obfuscation of real identity of the consentee from the consentor

Need to acquire consent for processing, real ID of data subject is NOT desired to be known/stored

Onboard & explain the Service

Authenticate with eID

Give permission

Return only Pairwise ID & Permission ID

ID linking (eID + pairwise ID + permission ID)

Proceed to intended processing/data collection

Data Using Service

MyDataShare Operator
Building Trust

Agreed roles and rules between the organizations

- Common agreement for the roles in the ecosystem
- Commercial rules and agreements

Legal framework

- Data operator, practical clarification and strong support from both public and private
- Flexibility to the legal framework, we are facing something new that no one knows exactly

Technology standards

- Common interoperability on conceptual level
- Shared interoperability components
- Minimal low level interoperability 1st
Thank You!

Mika Huhtamäki
Deputy CEO / Vastuu Group Oy
mika.huhtamaki@vastuugroup.fi
+358 400 616 253

www.mydatashare.com