vastuu^{group}

MyDataShare Overview

A Companion Presentation to MyDataShare White Paper

Consent is one of 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- Can be withdrawn by data subject at any time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 fro labour 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



MyData operator can bring more transparency and better control of personal data with all legal bases of processing

This to promote more sustainable personal data business

Wallet - transparency for personal data processing

| GDPR-set right of a data subject | Realisation for a user of a MyData wallet |
|-------------------------------------|--|
| Right to be informed | Users can review the data providers where their data is being stored. This may even reveal new data providers which the user may not have been even aware of. |
| Right to data rectification | The users can preview their data held in services. This makes it possible to see if there is a need for the data to be corrected. |
| Right to be forgotten | If the user wants the data to be removed altogether, they could initiate removal operation through the wallet when applicable. |
| Right to data portability | Extract and transfer user's information in machine readable format with tools provided by the wallet and the operator ecosystem. |

MyData operator with role as consent registry

Many types of operators will emerge carrying the 'MyData Operator' label.

MyDataShare, as an operator, is keeping only book of consents and controlling data access to 3rd parties, whilst it allows individuals full visibility and control to their consents. Personal data from data provider or consumer never transfers via the operator itself.

MyDataShare functions detached from the data flows it manages for the individual.



The problem with consents

Data integrations of service providers today are contracted, implemented and tested point-to-point, and thus difficult for the individual to remember and control as they're spread across the services they use.

Each controller has to cater for their own privacy notice and third party API authorisation functionality, thus everything fragments:

- Data requests and consent notices vary in human understandability and UX
- User IDs used for authentication and authorisation per service vary
- Tracking authorisations becomes hard



Image from Peter Gabriel's 'I Don't Remember' music video (1980)



Benefits of a consent operator

A trusted service for access authorisation and providing understandability over consent requests, which also takes care of documenting the consent per requirements of globally tightening privacy regulations.

The increase of trust provided by the operator covers both involved service providers (ecosystem) and data subjects who are given the power of control.

Integrations and UX can be simpler with shared use of MyDataShare's Identity Provider and Connectivity layers.



vastuu

Supported use cases



1

Individual's data is requested for re-use by a new 3rd party data consumer.

2

Additional processing and/or data is requested by existing service individual deals with.

3

Updates to processing (terms, data, purpose) on either 1 or 2 above.

The user experience

Embedded consent notice handling within UI and context of Data Consumer

(Operator still does the server-side heavy lifting, and Wallet gets to persist the consent notice outcome)



Invoking the MyDataShare Wallet service as the handling context for the consent notice





MyDataShare's Three Layers

MyDataShare ID

MyDataShare Consent Management

MyDataShare Connectivity

Identity provider -MyDataShare ID



Legal entities need to register clients for the IdP APIs

Authentication Login (Single-sign-on)



Individual

MyDataShare Consent Management

Consent Artifacts

- Consent requests
- Unique consent ID
- Consent state
- Auditable consent record What, who, when, to whom, purpose
- Consent receipt delivery





Policy Management

- Policy Enforcement
- Authorisation endpoint

Consumer registration Service and purpose registration

Initiating consent requests



Service and data asset registration Provider registration

Verification of consent status



Wallet initiation (implicit)

Approve/deny open consent requests Review/revoke active consents



Individual

MyDataShare Connectivity

Access Management APIs (operative)

- Local API endpoint for provided data
- (Local Access Gateway as API proxy)
- OpenID Connect and OAuth2 endpoints at MyDataShare
- Consent Introspection + Consent Request endpoints at MyDataShare

Administration & Maintenance

 Administration API endpoint at MyDataShare

Authentication of data requests Authorisation via token introspection

Consent requests + data requests

Logging of data access



API credentials management Redirection & notification URI management



Data Consumer



Integrating services with MyDataShare

Data provider integration option 1 - API Proxy



Proxy handles also ID linking and access logging for the provider

a trusted client towards

the API's access control

Data provider integration option 2 - own API

Existing own API of the provider may be adapted to work with the OpenID & OAuth2 and Consent Introspection endpoints of MyDataShare

Access logging and ID linking needs to be done internally in the API controller logic



Data consumer integration - new consent



Data consumer integration - existing consent

With an existing active consent for requested ID and provider service, the consumer acquires the consent token from the MyDataShare

Token will be used in data requests towards the provider

Provider API/API proxy validates the token as described earlier





Thank You!

Contact information:

https://www.mydatashare.com/#contact

