mydatashare

Empowering sustainable and human-centric innovations!

A MyData Operator White Paper

The right of an individual to control their personal data easily and securely is one of the main topics present in a global discussion concerning digitalisation, data usage and platform economy. This white paper introduces a way for data providers and data consumers to collaborate transparently in the best interest of all parties. This new offering, MyData operator platform called MyDataShare, is available globally for all entities and organisations in need of a human-centric and transparent tool to facilitate their needs for secondary-use personal data collection, sharing and access, as defined in the global MyData Principles.

In this paper we cover the reasons and need for a MyData operator, the elements the service includes and how the parties can take MyDataShare into use.

MyDataShare is a service provided by Vastuu Group Oy, Finland. Vastuu Group's mission is to create better living conditions for people by enhancing digitalisation between cities, companies and people. As Finland's first MyData operator and founding member of MyData Global we want to empower individuals by enabling their personal data management.

vastuu group

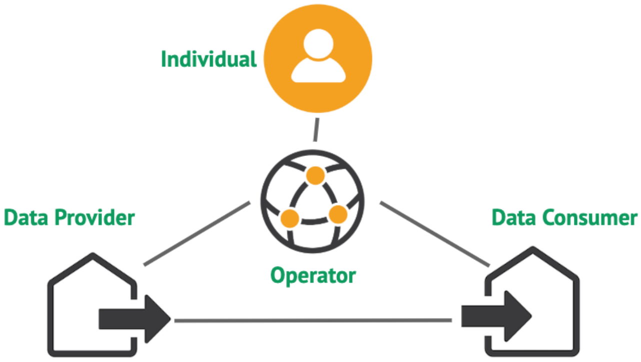
Table of Contents

[1] Some figures in his paper utilise and are derivative works from "MyData Graphics" icons by MyData Global, licensed under CC BY 4.0.

The Essence and Approach of MyDataShare Product as a Personal Data Operator

Individuals need to be better positioned to be aware of and control their personal data use in different services and organisations. This is the aim of MyData Global[2], a non-profit organisation that promotes individuals right to control their personal information.

Personal data usage today often doesn't survive a close scrutiny or may not be known to us at all. According to MyData initiative, the individual shall be equipped with digital decision-making tools to choose by whom and through which terms their existing personal data can be (re-)used. These tools shall offer a digital control mechanism, be a balancing act between understanding and trading the personal benefits of providing access to data to third parties versus the controlled loss of privacy that results from this action. This is where the personal data operator, or MyData operator, comes in: The operator plays the role of a trusted and neutral intermediary between data providers and data consumers within an ecosystem, which is built on increasing trust among its players - including the identified individual in the key position. An individual may not own data (as no entity can) but has the power of control over the use of their data in this ecosystem. *MyData declaration of principles*[3] defines the following roles for the ecosystem members:



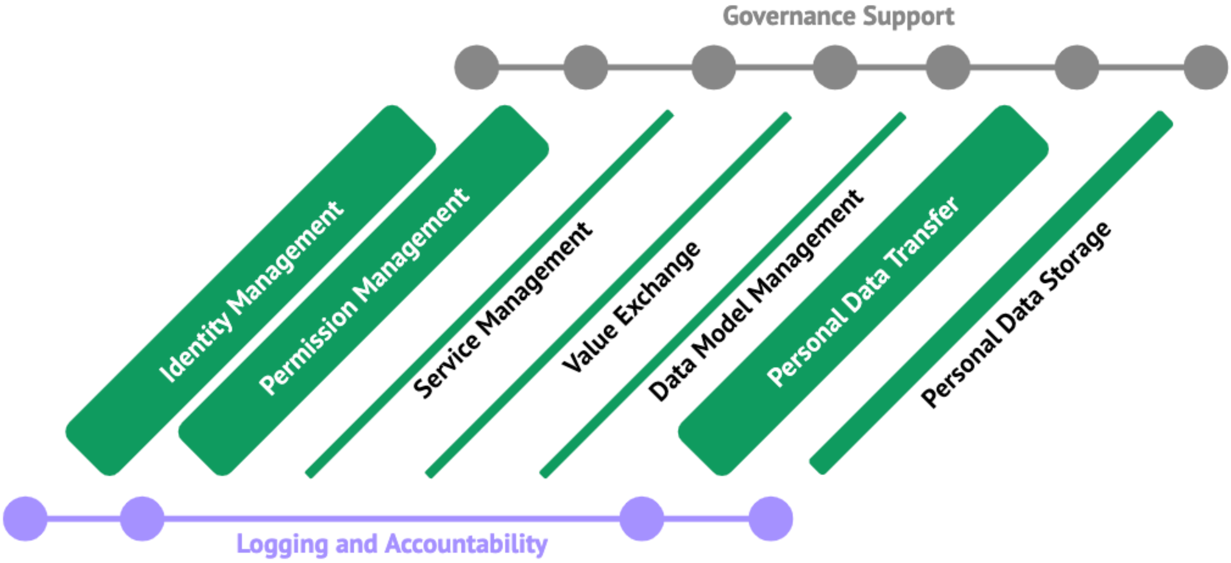
- **Individual/person** manages the use of their own personal data, for their own purposes, and maintain relationships with other individuals, services or organisations
- **Data provider** collects and processes personal data which the other roles (including persons) may wish to access or use for purposes outside the original processing purpose.
- **Data consumer** can be authorised to fetch and use an individual's personal data from one or more data providers for their well-defined purpose.
- **MyData operator** enables individuals to authenticate, securely access, manage and use their personal data, as well as to control the flow of personal data with, and between, data providers and data consumers. The operator puts the person on the driver's seat doing the decisions on what the data should be used for. An operator enables entities to register data providers and data consumers as ecosystem's services, which can conduct transactions within the MyData ecosystem.

[2] https://mydata.org/

[3] https://mydata.org/declaration/

MyDataShare as a Transparent Data Flow Controller

Another white paper, *Understanding MyData Operators*[4] published by MyData Global brings in a thorough analysis of the early personal data operator space. It introduces a reference model for operators, with nine core functional elements that are design components to be considered for any entity taking the role of an operator. All components don't need to be part of a particular operator, as its chosen operational design may not justify a need for a particular function.



An operator can include functions dealing with storing personal data of the individuals, or be a pure access, transparency and data flow controller, with very limited access to personal data of the individuals it serves. MyDataShare is currently designed to focus on **permission and identity management and personal data transfer** components, limiting the data it holds to the identities, identifiers, permissions and access logs the individuals need in managing services and data shares through their personal **MyDataShare Wallet**. By intentional design, this kind of operator will not be a central 'honey pot' or profit centre based on opportunity of selling personal data bound by their consent or other processing related actions. **The personal data from the provider or consumer side never transfers via the MyDataShare operator itself** - the operator functions detached from data flows it manages for the individual. The three core elements of MyDataShare are explained in subsequent sections on MyDataShare ID, Consent management and Connectivity starting from page 8.

While waiting for a broader MyData operator rulebooks and labelling templates to be published by MyData Global, we've highlighted the core rules you can always assume to be followed in MyDataShare's operator design.

MyDataShare as an operator will:

[4] https://mydata.org/operators

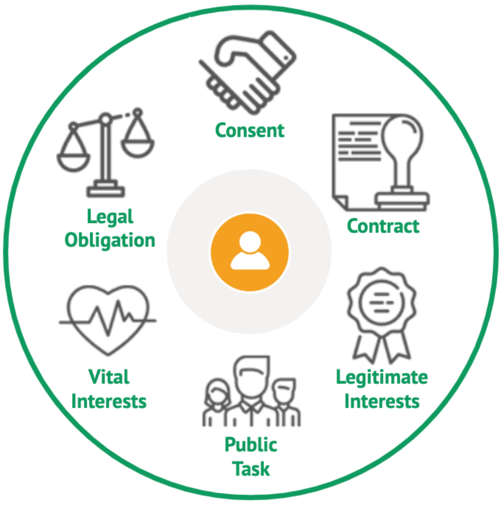
- Always use appropriate technical and organisational measures to protect the personal data being processed by the data operator, taking into consideration the risks of such processing.
- Pursue and support for maximal data portability for the types of personal data it keeps for an individual, especially what comes to moving this data to other similar operators.
- Ensure that all parties acting in the ecosystem (such as organisations, their services, individuals, etc.) can be identified and that they can authenticate themselves at the level appropriate for the task at hand.
- Ensure that transparency to the processing taking place by different ecosystem parties can be provided through collecting auditable information
- Never leak, sell, maliciously use itself, or provide for other than trusted parties any access to individual's data unless data operator has binding legal obligation to disclose such information.

There may be role-specific rules and responsibilities for an organisation as an ecosystem member - data provider or data consumer - will have to adhere to when signing up to work with MyDataShare. More of those on the latter part of this document and in our future Onboarding Guide.

Focus on Consent but Serve Beyond It

Consent is the most human-centric tool for deciding if certain data is to be processed or not. There's a history of focus on actionable and unambiguous consent as data re-use enabler - as **"Consent Approval Wall"** - on MyData principles, aside the other EU-wide defined legal bases of personal data processing. Through an understandable consent process an individual can weigh in between privacy-loss and the added value they get from giving consent.

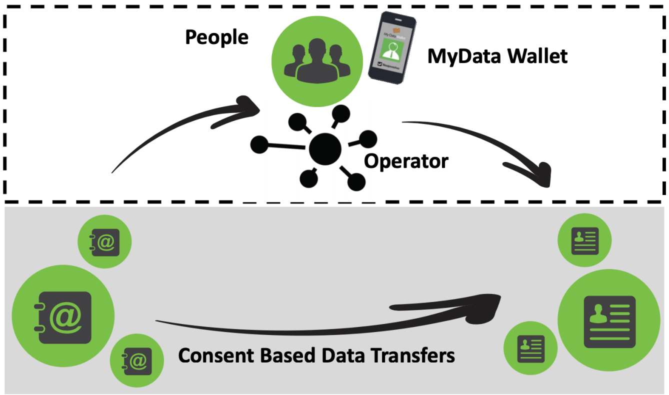
It is also important to remember that in order for a consent to be considered valid it has to follow the GDPR requirements and in many cases, consent may not be the most suitable basis for lawful processing. For example, when valid consent cannot be given due to significant power imbalance between the controller and data subject.



Flexible control over consent process is also on the side of the individual - processing can be stopped as easily as it was allowed through the use of GDPR-enforced **consent withdrawal right**. In reality, this is only possible if the consent process is implemented with proper user experience and is easy to find when needed. MyDataShare promotes ethical and sustainable data business by providing effective tools for the data subjects to use their rights under the GDPR, and by providing better transparency and auditability to personal data processing in general. These tools are useful in cases where the lawful basis of the processing is not based on consent but on contract, legal obligation, legitimate interests, vital interests or public interest. Examples of this kind of tools are listed in the table below.

GDPR-set right of a data subject	**Realisation for a user of a MyDataShare Wallet / Operator**
Right to be informed	In their personal MyDataShare Wallet data subjects receive notifications concerning their personal data. The Wallet can be used as a method to contact data subjects and provide them with all required information. Using this kind of tool allows data subjects to have a centralised view over processing of their personal data and may make previously "hidden" processing more visible.
Right to data rectification	The users can preview their data held by a data provider or data consumer. 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 this through the Wallet (when applicable, as this right does not apply to all legal bases of processing.)
Right to data portability	Users could be allowed to extract their information (in services and the operator) in machine readable format with tools provided by the Wallet and operator ecosystem.

MyDataShare Tackles Current Personal Data Sharing Problems

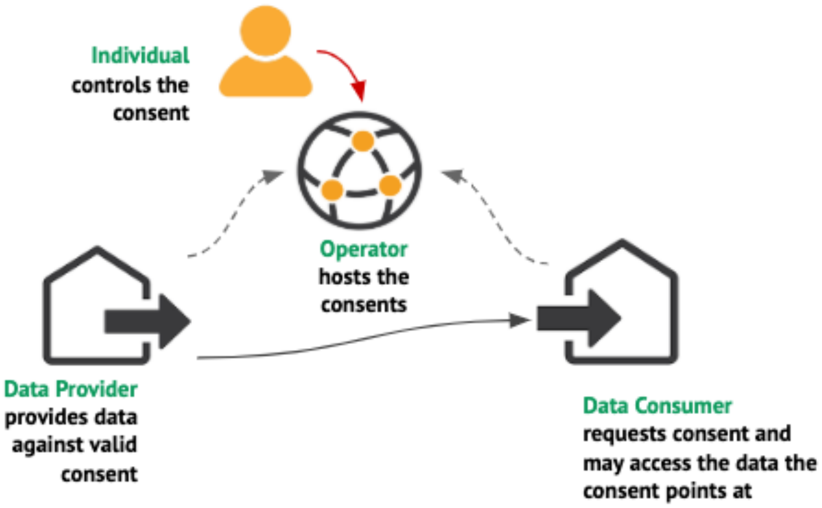


MyData initiative proposes a very different picture of the data re-use integrations familiar to service providers today. They are now orchestrated point-to-point (i.e. agreed, implemented and tested between two parties) and thus difficult for the individual to remember and control. Each provider has to cater for their own consent notice and authorisation functionality. As a result, everything fragments: user experiences and contexts vary, identities used for authentication and authorisation per service vary, authorisation request and consent notices vary in understandability.

These are complications that can be remedied with a careful design and use of common tooling and infrastructure that MyDataShare provides, whilst it offers overall improved privacy controls and transparency to the individuals.

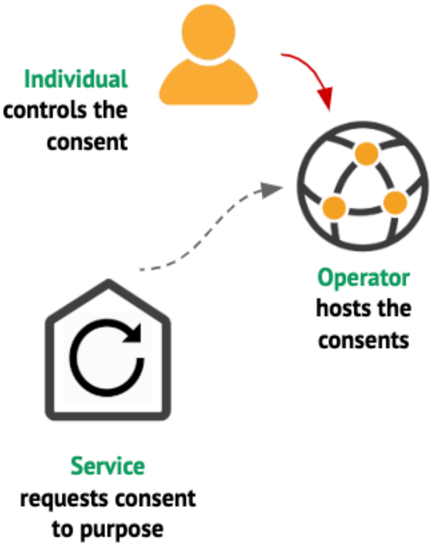
Use Cases and User Stories

Our operator product MyDataShare initially provides support for consent management with a few various flavours. As a common starting point, a data consumer, which from regulatory perspective is a new controller-to-be for the data to be processed, can initiate a consent request to an individual. The consent proposal, the end user actions, and following consent record maintenance are managed via MyDataShare.


Individual
controls the consent
Operator
hosts the consents
Data Provider
provides data against valid consent
Data Consumer
requests consent and may access the data the consent points at

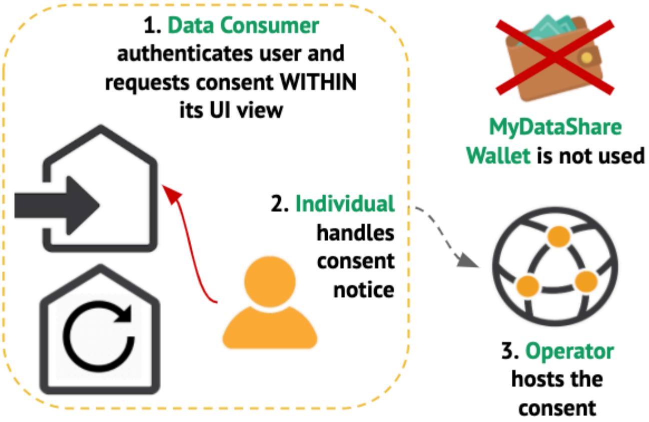
The archetype MyData use case is where certain personal data is located **outside the requestor** (data consumer), in which case the data access to the provider's application programming interface serving the data out is authorised by MyDataShare.

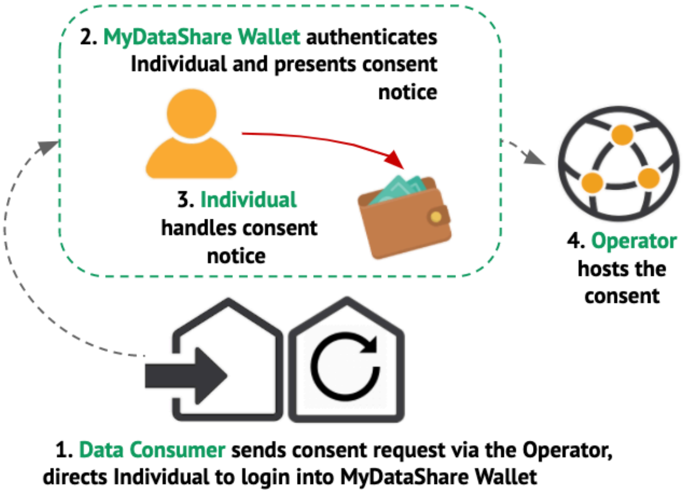
Alternatively, a data consumer may request consent to a **new processing purpose that requires personal data** previously collected under other purpose. Also, new purpose could trigger collection of new personal data that they don't previously have in their possession (e.g., location information on a mobile app). Here there are no 3rd party data access issues to cover, but MyDataShare acts as the registry documenting consents on behalf of the requesting service/organisation.



Using the MyDataShare Wallet

Regarding integration of user actions and user interface, MyDataShare allows the context and user experience of consent management to be kept familiar for the individual through **embedding** the user interface of privacy control to Data Consumer's own service and style & design. Remote MyDataShare components serve the actual service functions behind the embedded privacy controls user interface.


1. Data Consumer authenticates user and requests consent WITHIN its UI view
2. Individual handles consent notice
3. Operator hosts the consent
MyDataShare Wallet is not used


2. MyDataShare Wallet authenticates Individual and presents consent notice
3. Individual handles consent notice
4. Operator hosts the consent
1. Data Consumer sends consent request via the Operator, directs Individual to login into MyDataShare Wallet

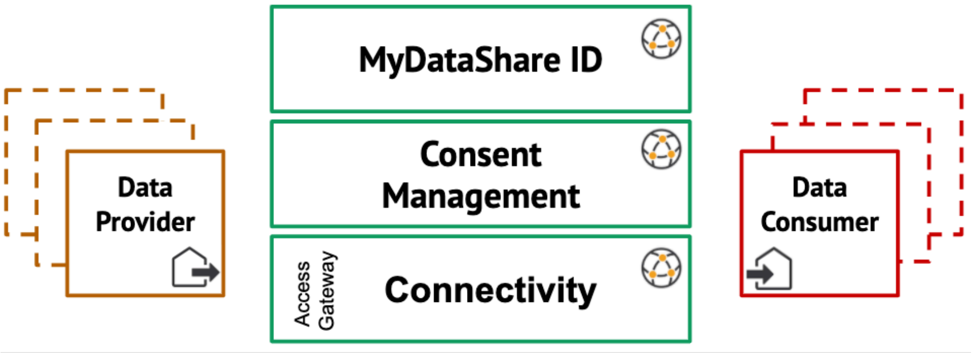
MyDataShare hosts a see-it-all **MyDataShare Wallet** view (a separate web service with user login) for those individuals that find it useful to have a centralized personal data dashboard. This view can be used for consent request handling by data consumers not wishing to embed the functionality to their own web service. Typically, the individual needs to re-authenticate at the wallet view, unless the data consumer is using MyDataShare ID for authentication also internally. During first-time login to the wallet the individual will be informed about the role of MyDataShare and gets to approve the contractual terms of service.

The goal of MyDataShare is to simplify and standardise management of data sharing and consent management in various contexts for the individuals, while providing a flexible data integration service for data provider and consumer organisations. Integration is possible with lowered development effort, if the organisation chooses to invest for the all-inclusive integration package available for both data providers and consumers.

MyDataShare Core Functions – Identity, Consents and Connectivity

MyDataShare MyData operator has three core functions:

- **MyDataShare Identity** (an identity provider that can be combined with external identity provider services),
- **Consent Management** and
- **Connectivity** services.



Regarding the integration of the MyDataShare functions to an existing digital service or system, a relying party for MyData operator services can use the product embedded under their own user interface, context and branding. But they can as well link their individual users to a separate MyData privacy dashboard service[5] a.k.a. MyDataShare Wallet application that collects together user's consents across any personal data management contexts they may have linked to this operator instance.

Identity – MyDataShare ID

This is the MyDataShare's identifier and authentication management function, powering end-user onboarding and operator's core functions, i.e. consent management, usage logging, linking user's active identities, and other available features for e.g. user profile management.

Ability to bind an identity (arguably, in some cases the person/user could be anonymous, the service context allowing) is essential to personal data management. Identity must link simultaneously to

- the consents and data authorisations of a natural person, and
- a known user identifier at the impacted services (data provider and consumer) holding personal data linked to this identity.

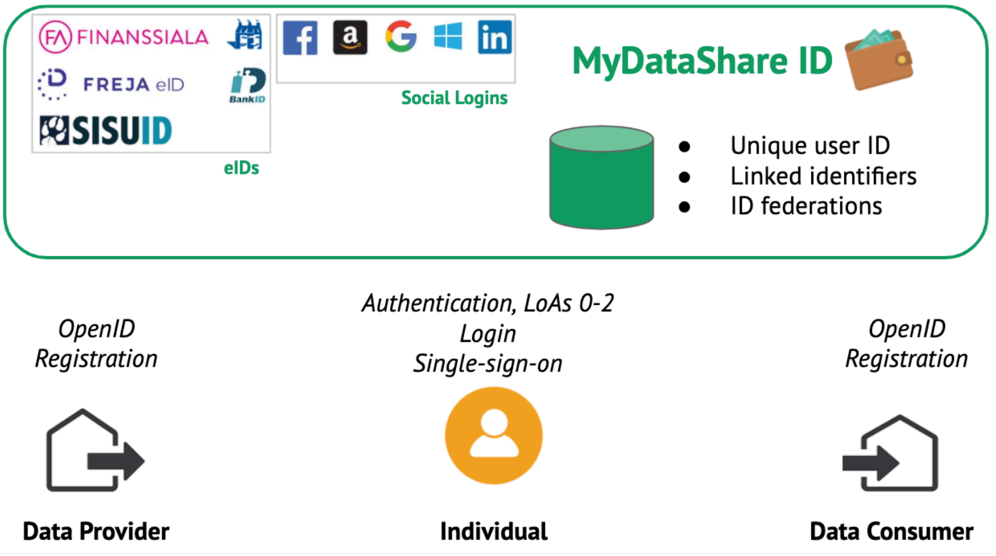
This is required to serve both the benefits of the individual and the regulatory interests of the services (as controllers, defined in GDPR) involved.

[5] MyDataShare Wallet service can be tried through Finnish Trust Network -compatible authentication at https://demo.muntiedot.fi/front

Core purpose of a person's account in the operator's ID system is to act as a master identifier between linked services, and to map the user's local user identifiers in these services with their consents hosted in MyDataShare under the first-mentioned root identifier (see later Consent Management).

Technical Details

Level of end user authentication assurance[6] (**LoA**) required for authorisation of data transactions can vary based on the type of personal data in question, and this is usually linked to user-perceived complexity of the authentication and the following authorisation management process. Thus, MyDataShare ID must have the capability to serve identity authentication demands with various LoAs.



The MyDataShare ID system is built originally to depend on strong authentication. In authenticating the person onboarding the relying party service for managing data shares and consents. The solution works through several federated electronic identity[7] (**eID**) providers with eIDAS substantial-level LoA (e.g. BankID, Finnish Trust Network FTN). Once established onto the MyDataShare, this person's base identity can be linked with other common identity provider services, e.g. the social login IDs – Google, Facebook, Twitter, Office365, GitHub, etc. to simplify use of the app. This comes through our future ID federation feature, along with single-sign-on (**SSO**) functionality[8] that together can greatly simplify the user experience of invoked data authorisation and consent management actions. Internally the MyDataShare ID works through a custom OpenID Connect[9] Provider (**OP**) service with the most relevant (and new, when necessary) authentication federations brought into the service's ID portfolio. Data providers and consumers will get the necessary credentials through onboarding & registration.

[6] https://ldapwiki.com/wiki/Level%20Of%20Assurance

[7] https://en.wikipedia.org/wiki/Electronic_identification

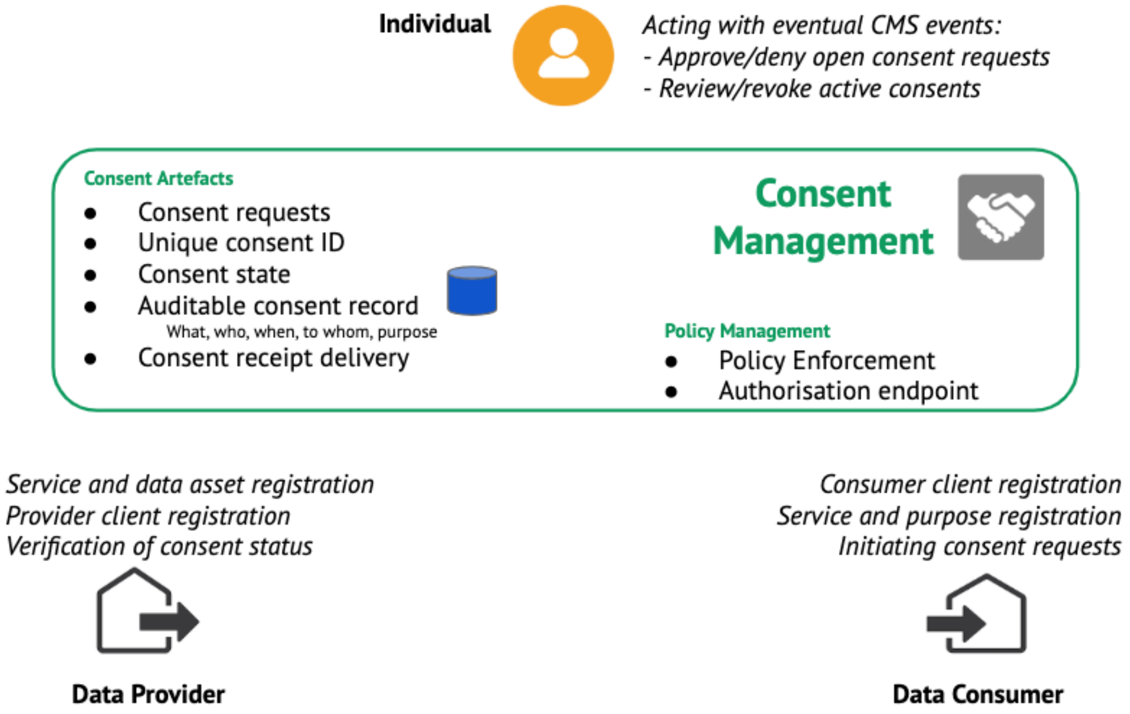
[8] Federation, SSO and configurable LoA are part of the ID extension feature roadmapped for the first half of 2020.

[9] https://openid.net/connect/

Currently MyDataShare ID onboards all users by default through strong authentication (using eIDs). After the ID federation feature becomes available, the set of identity providers to be used in a particular use case becomes more a matter of configuration. Applicable identity provider should depend on the authentication strength requirements set by the data to be provided: Data provider's expectation for authentication strength and use case (sensitivity) of the requesting data consumer. Sharing a less-sensitive data asset or attribute for a low-value, low-risk business transaction can be dealt with social login ID only, if agreed through the operator configuration.

Consent Management

The MyDataShare **Consent Management** functionality forms the data access control and the auditing function of the system. The function is responsible for all lifecycle management, actions and data persistence (permanent storage of critical data). **The data transport and related authorisation mechanism on the Connectivity layer (APIs) is built to rely on validating the status of Individual-provided consent at each data request.** These requests come from a known, identified data consumer, and are linked to data available from a known, identified data provider. For meeting the regulatory requirements of a valid consent (freely given, specific, informed consent), the consent request will contain complete information of the identities of the controllers, specific processing purposes and other required information It is brought (both visually and textually) to the individuals for an explicit decision making through a **consent request.** This consent request can be approved or declined – and the consent withdrawn easily later. The consent request function can be used by the data consumer to check the status of consent requests it has initiated via MyDataShare.



Individual
Acting with eventual CMS events:
- Approve/deny open consent requests
- Review/revoke active consents
Consent Artefacts
Consent requests
Unique consent ID
Consent state
Auditable consent record
What, who, when, to whom, purpose
Consent receipt delivery
Consent Management
Policy Management
Policy Enforcement
Authorisation endpoint
Service and data asset registration
Provider client registration
Verification of consent status
Data Provider
Consumer client registration
Service and purpose registration
Initiating consent requests
Data Consumer

Technical Details

Actions and decisions that need to take place on side of a service or entity that is considering their consent management to be provisioned with MyDataShare are listed below:

1. A data provider (service with outbound-available data and API of its own) is provided with an alternative, MyDataShare -provided trusted authorisation layer (an **API proxy**, a.k.a. **Access gateway**) to complement their existing local API access control. Alternatively, the data provider can adapt their existing API and authorisation layer within to additionally[10] to rely on MyDataShare on consent status validation prior to providing 3rd parties access to this data.
2. The data provider has to decide which data is to be opened for consent-based authorisation via MyDataShare. This data needs to be registered with MyDataShare.
3. Any data consumer will have to register itself to the MyDataShare system as a data consumer client to enable secure communications between services within the ecosystem; they also are expected to deliver meta-level information of the data consumption use case for construction of the consent request with necessary end-user descriptions. These include declaring identities of the data provider and data consumer specific purpose of processing, lawful basis of processing and other information that is required for freely given, specific and informed consent.
4. Any service utilising MyDataShare without a data provider will have to register itself to the MyDataShare system as a service client to enable secure communications between the service and the MyDataShare functions; they also are expected to deliver meta-level information of the data processing use case for construction of the consent request with necessary end-user descriptions. These include declaring identity of the service, specific purpose of processing, lawful basis of processing and other information that is required for freely given, specific and informed consent.

We expect that data consumers will face more regulatory control in onboarding the production ecosystem, as the operator and data providers may set their ecosystem partners' services that pursue data access under a careful audit scrutiny. More about this and joining the MyDataShare Partner Programme as the starting point will be available in our separate Onboarding Guide.

Consent Token Explained

After the individual's consent is acquired, the Consent Management layer documents this down as an active consent record and provides the data consumer behind the request a **consent token** for consequent use. This token, resolving to the data provider and individual it includes, is thereafter used by the data consumer as a 'key' in data access requests towards the data provider, similar to Oauth2 access tokens used in context of Oauth2-protected data resources.

[10] The intention of introducing MyDataShare as an access control service to provider's data is not to hinder the provider serve the data as they used to, via their own existing data access controls and policy.

Only a valid consent token opens a data transfer. The data provider must run a validation process (introspection) for the token against the remote MyDataShare's Consent Management function any time it receives a data request through the Connectivity layer operations. A token becomes invalid either after a use case driven, defined expiration period, or if defined as non-expiring, at conscious consent withdrawal action of the individual. Facing token expiry, the data consumer needs to send the individual a new consent request via MyDataShare.

Any data consumer client requesting data against this token – done through the data provider's new API proxy (or their own equivalent API behaving similar to the proxy) – will expose its service identity and details of the data requests for validation by the MyDataShare as a trusted 3rd party, and all transactions are logged for eventual audits. Logs shall include all consent handling interactions by the individual, and actual data access events through the API proxy element – or its equivalent, if integration is done in-house at the data provider side.

Connectivity – Power of The Ecosystem

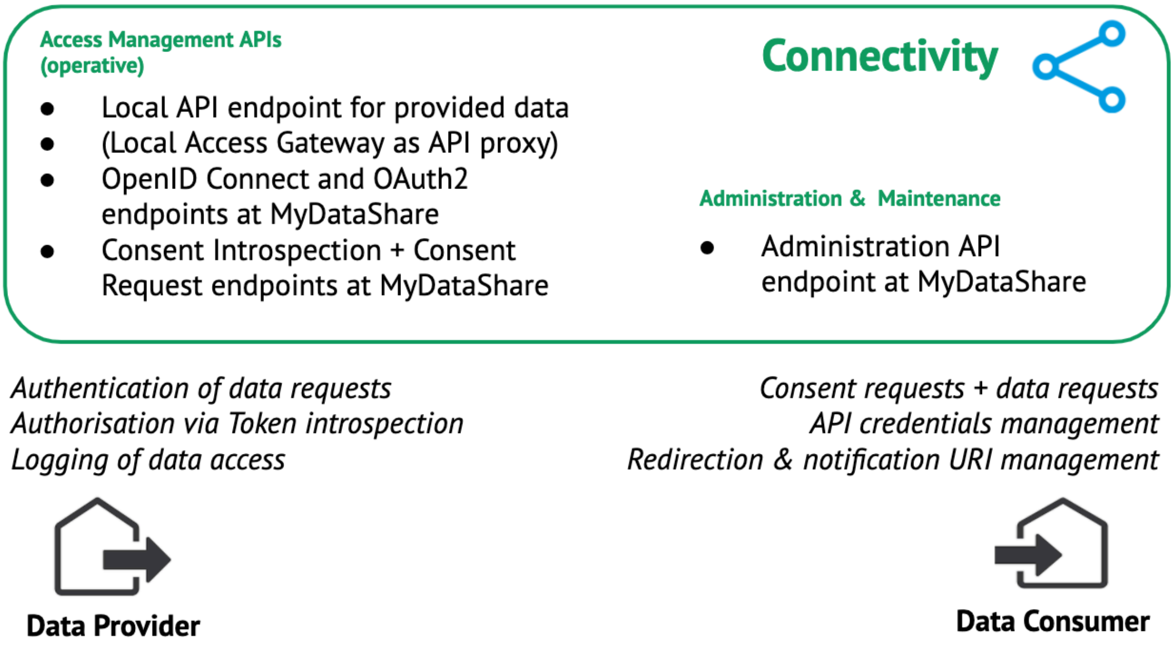
Connectivity covers the different **data connectivity services and consent management interfaces** (APIs) necessary in utilising MyDataShare as ID provider, consent management and data access authorisation service.

Ecosystem power of the operator comes directly from the connectivity layer. The number of data reuse scenarios within a particular operator (in this case MyDataShare) emerge from the sheer volume of its services, both providers and consumers. Therefore, the goal here is to make system integration as uncomplicated as it can be.

Technical Details

As already surfaced in the MyDataShare ID introduction, the services onboarding the ecosystem will need registration and integration with the OpenID provider of the operator's identity provider service. This is done first in order to manage matching of user identifiers between parties, and secondly to provide authentication and single-sign-on service for their end users that are invoked to use MyDataShare's privacy management features.

MyDataShare ID acts simultaneously to the identity provider function as an Oauth2 authorisation server (**AS**) to ensure secure access to the Consent Management layer for the services. Services will need to deploy an OpenID/Oauth2 client according to the MyDataShare developer documentation available upon request.


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
Connectivity
Administration & Maintenance
Administration API endpoint at MyDataShare
Authentication of data requests
Authorisation via Token introspection
Logging of data access
Consent requests + data requests
API credentials management
Redirection & notification URI management
Data Provider
Data Consumer

Most effort with MyDataShare Connectivity layer integration falls to data providers, as they have to adapt their existing API access controls to either work directly with MyDataShare's **Consent Introspection API** or equip the API with an API proxy taking care of integration to the operator. Adaptation needs to also ensure that appropriate data access logs are available to the operator (for audit trail and e.g. eventual visualisation for the end user as transparency feature of the wallet) as needed. Necessary actions and options for providers are explained with more detail upon request.

Data consumers and services using data operator for consent hosting are essentially forced to deal with two MyDataShare interfaces after they have been registered into this role. First, they will enable the MyDataShare ID use for their users either through an embedded consent management view, or via the MyDataShare Wallet application login route. Secondly, they can initiate consent requests, or query statuses of their active requests via the **Consent Request API** using the credentials given at registration phase. More details on available actions and options to realise this as data consumer is explained the Onboarding Guide.

MyDataShare's service onboarding process takes care of providing the necessary environment credentials and parameters to joining entities. For all service-side roles, a do-it-yourself management tool[11] will be available for managing different provider or consumer side credentials, needed descriptive text elements and local API details. Examples of the last are e.g. provider base URLs and consumer redirect/logout URLs for authentication and authorisation use cases within MyDataShare ID. Until the tool is available the registration process is handled through the MyDataShare product team.

[11] Administration tools are a feature roadmapped for the first half of 2020.

Future Items

MyDataShare is a new product with several features still on drawing board or development queue. Here are some of the future features.

Federated Identity Management in Context of MyDataShare

Onboarding (identification and account creation) of the individuals to MyDataShare happens for now automatically with strong authentication (eIDAS Substantial-level notified eID). The roadmap includes means to connect other OpenID providers, not necessarily with as strong LoA, for creating the account for the user.

This shall provide generally more flexibility to available login providers such as social login IDs, Office 365 etc. often used by the services, and support for single-sign-on between them and the MyDataShare dashboard. This will also create room for more identity management features for the users in the MyDataShare Wallet once introduced. A core feature within this is the ability to decide (as an individual or as data provider/consumer) if personal data under processing at a data consumer should be pseudonymised or not.

Handling of Contracts and Other Legal Processing Bases

The Consent Management function is developing onto a general permissions and processing bases related function. In first phase of this track, the MyDataShare and the wallet will be able to manage and keep status of contracts (terms of service, user agreements) entered in force between individuals and data consumers.

Administration Portal Tool

Much of the required registration-time business and technical information is initially collected through manual interaction between Vastuu Group and joining providers and consumers.

As the information regarding registration is sure to change over time, the whole process can be transitioned to be executed as DIY work by responsible users with appropriate access rights to MyDataShare's customer portal. This familiar approach is used widely in the software industry for API, cloud environment or product subscription management purposes, and makes scalable configuration management less independent of service provider's scarce human resources. Aside portal as the first-tier management tool, an email helpdesk will be available for troubleshooting and issuing customer service tickets.

Portability of MyDataShare Account Data

Part of the Connectivity layer is also the future data portability promise we give for the individuals: your consents shall be transferable to a similar operator function in an open, reusable format (at some point). This may not be yet an obvious thing as industry standards for personal data records and trust structures for operator interconnectivity are just starting to evolve. First step towards this is an accessible data export function that is to be included in the MyDataShare Wallet service for the individuals.

Decentralised Identity Support

Vastuu Group is a founding member of **Findy consortium**[12], which targets launching a new decentralised identity and credential management utility. This will be based on use of **decentralised identifiers**[13] **(a.k.a. DIDs)**, a standard recently completed in W3C, together with a national distributed ledger as the public trust infrastructure with own governance agreements. Identity attributes are issued to a DID holder in another W3C-defined format, cryptographically formed **verifiable credentials (VCs)**. Term self-sovereign identity[14] (**SSI**) is nowadays used to describe this fresh and different approach to identity management which with its technology and trust structures has traditionally been very centralised (though identity federation could be seen as decentralisation to an extent) in nature.

Many of the services provided by Vastuu Group to its partner programme companies today - trust services for employers, certificate verification, legal verifications of employers and employees/professionals - are logically **transferable to equivalents in the verifiable credential domain**. We envision this new, more privacy-preserving identity and credential management paradigm to be ready for market deployment in a few years' time. Several ambitious SSI pilots exist already around the world.

A stepwise transition covering both companies with their official, authority issued identities and credentials, as well as individuals' equivalents, will be linked to MyDataShare roadmap. First goal is to bring company credential issuance and relying party verification (verifiable credentials regarding company/entity attributes, issued by Vastuu Group, verifiable cryptographically through the public ledger by the relying business service or other in a verifier role) available for the members of our partner programme. Vastuu Group will host the necessary service infrastructure to its members. Company credential system will be accompanied with a related credential governance agreement stipulating the trust structures involved and developed in the context of the future Findy governance framework.

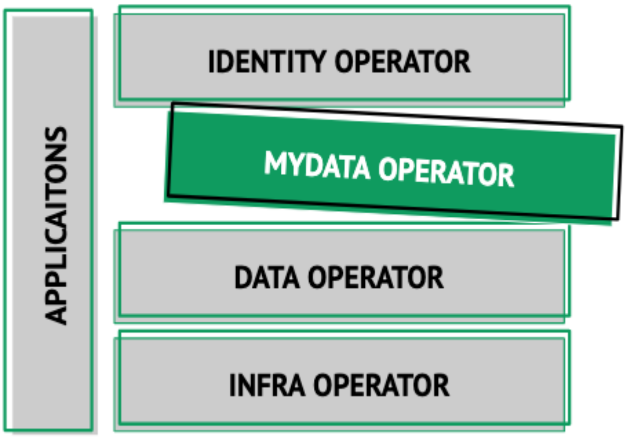
[12] https://findy.fi

[13] https://www.w3.org/TR/did-core/

[14] https://hackernoon.com/self-sovereign-identity-what-is-the-business-value-uq6l36wh

Why Us?

Background of Vastuu Group since 2010 is in built environments related data and professional's management. We operate identity management, professional certifications verification, data integrations and applications/services for our partners in the Nordic and Baltic region. As we already host the data of more than 600 000 individuals and 62 000 companies under their trust, entering onto more comprehensive personal data management is not an extraordinary step for us.


APPLICAITONS
IDENTITY OPERATOR
MYDATA OPERATOR
DATA OPERATOR
INFRA OPERATOR