6 – Why should companies be interested in MyData?

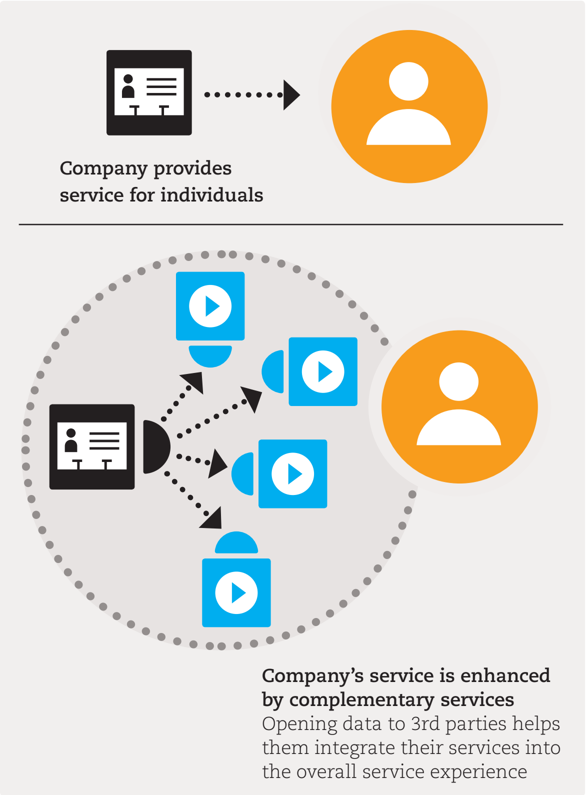

Company provides
service for individuals
Company's service is enhanced
by complementary services
Opening data to 3rd parties helps
them integrate their services into
the overall service experience

Figure 6.1: Conventional service versus service extended with MyData-based complementary service integration

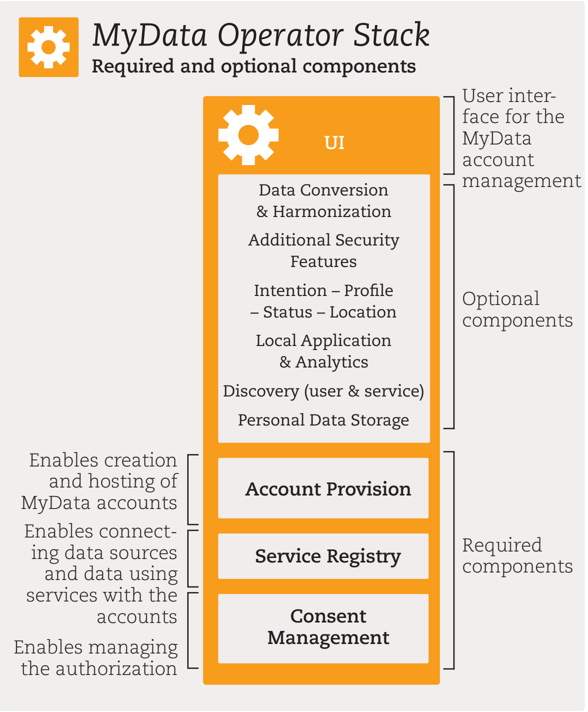

MyData Operator Stack
Required and optional components
UI
User interface for the MyData account management
Data Conversion & Harmonization
Additional Security Features
Intention – Profile – Status – Location
Local Application & Analytics
Discovery (user & service)
Personal Data Storage
Optional components
Account Provision
Service Registry
Consent Management
Required components
Enables creation and hosting of MyData accounts
Enables connecting data sources and data using services with the accounts
Enables managing the authorization

Figure 6.2: The MyData operator stack shows the required and optional functionalities of the MyData operator. Consent management is the baseline service for an operator, but there are multiple complementary value added services an operator can provide in MyData infrastructure for the individual

Companies can improve their business operations with MyData. Optimizing resource allocation, creating service pathways, providing personalized services, and producing recommendations are generic service improvements that many services can offer through better access to personal data. In addition, the MyData infrastructure would enable new kinds of services, such as vendor relationships management (VRM), people discovery, and personal data services related to large-scale research data banks and behavioral analytics.

The primary incentive for companies to create a MyData API that gives their customers and authorized third parties access to certain datasets is that it would expand their overall value proposition to customers (see Figure 6.1). Third-party vendors can collaborate more effectively with companies that hold the original data sources if they have authorized access to datasets that contain personal data.

Studies show that more and more people are becoming aware of the ongoing exploitation of their personal data without their consent. If a company's behaviour is considered shady or unacceptable, it faces the risk of public criticism, lawsuits, and users opting out of services on a massive scale. Implementing MyData principles would give companies a marketing advantage. Companies can improve their customer relations by engaging with customers in new reciprocal ways, sharing data back to customers, or even generating enhanced datasets based on information that customers voluntarily choose to provide.

Currently data is sold implicitly so that the individual gets a "free" service, but willingly, or in many cases, unknowingly gives personal data to the service provider in exchange for services. The MyData infrastructure provides a simple and transparent mechanism for making data sales visible and explicit in ways that benefit both parties – either through enhanced services or direct monetary profits. Operators can facilitate data sales and share revenues with both data sources and data subjects.

For the MyData ecosystem to flourish, it is crucial that there are viable business models for MyData operators. MyData operators could charge account and transaction fees. MyData operators could also generate profits by charging a marginal rate on data sales. Value-added services operators may offer, for example, secure storage, local applications, and a marketplace for data-centric applications (see Figure 6.2).

For the overall viability of the MyData approach, it is also important to set organizational and business level standards, especially for the MyData operators. Such standards are currently developed in an open operator alliance. The alliance can also facilitate the standardization of technical functionalities that enable account interoperability.

For Companies MyData will:

- help to integrate third party complementary services into their core services
- simplify operations within current and forthcoming regulatory landscapes and enable data use for exploratory purposes
- enable the creation of new business based on data processing and management

3 – Why is MyData an infrastructure level approach?

MyData reforms the personal data ecosystem at the infrastructure level – but are such high-level reforms necessary? Wouldn't it be easier to simply open personal data APIs to all services and let organizations negotiate and connect directly amongst themselves?

Having access to personal data via APIs is critical for most MyData-based service scenarios. The "API economy" is already developing into an organically expanding ecosystem of services that exchange personal data over point-to-point connections. However, organizations struggle to manage their API integrations, while individuals are lost with the big-picture view of their personal data flows between services. In the long run, some systemic restructuring will be a necessity. The current API economy can be seen as an incubation stage for the forthcoming data economy. However, we will need also a more robust infrastructure on top of the mere APIs.

As the situation currently stands, personal data aggregators are emerging within specific sectors, such as Validic and Human API in the health sector, in addition to the well-established data powerhouses such as Google, Facebook and Apple that are streamlining the flow and interoperability of personal data within their own ecosystems. The data aggregator model is naturally evolving out of the API economy, but it presents two fundamental drawbacks. First, the lack of interoperability between data aggregators means individuals and companies become locked into specific data service providers and the data market is fragmented in a way that stifles innovation and inconveniences people. Secondly, the current crop of data aggregators do not necessarily acknowledge privacy or engage in a transparent manner with the individuals who are their data subjects. There are several initiatives that aim to create a more open and privacy aware model (such as Qiy, The Good Data, Respect Network), but in the absence of a common infrastructure these also suffer from a lack of interoperability.

The key concept in the proposed MyData infrastructure is the MyData account. For an individual, the MyData account is a single hub for personal data management. Via the account individual can give services the authority to access and use his or her personal data. The account stores information on how the individual's personal data is connected to different services and the legal permissions and consents for using the data.

Adopting the MyData approach could ultimately lead to a systemic simplification of the personal data ecosystem. Nonetheless, MyData is not an all-or-nothing approach. Rather, it can be developed and deployed in stages concurrently alongside the evolving API economy and the existing data aggregator model.

We need infrastructure as it:

- anticipates wide adoption of APIs and overall increased demand for personal data logistics
- enables individuals to have practical and comprehensive control over their digital consents
- can facilitate human-centric monetization of personal data.

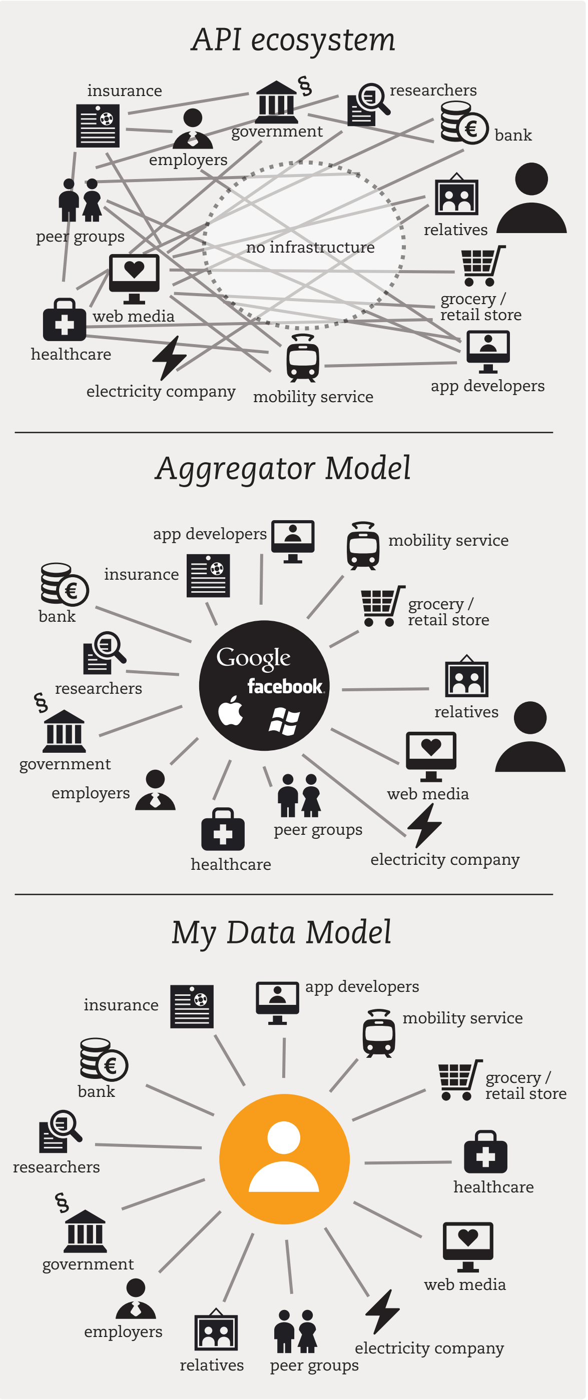
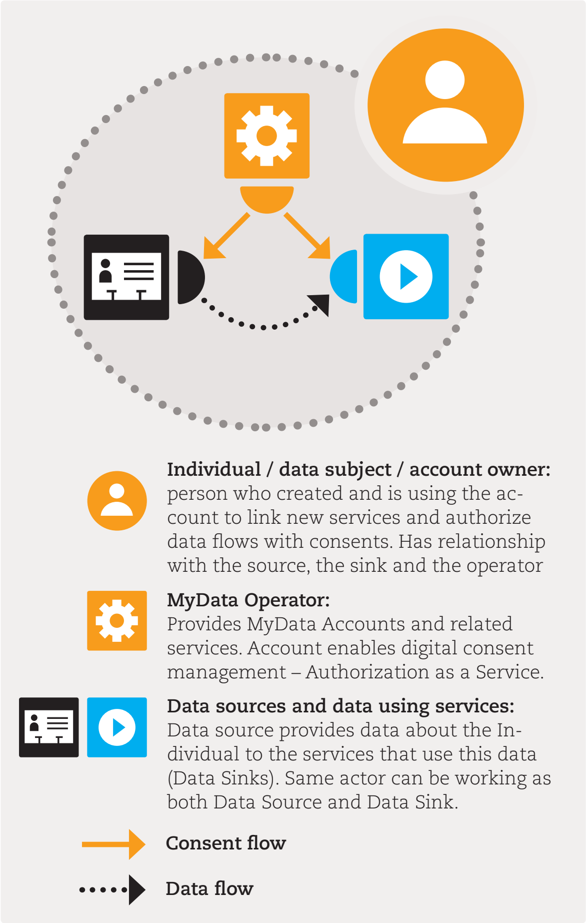


Figure 3.1: In the current structureless API economy, if the number of services grow, then the number of connections between them grow at a faster rate (top). Aggregating data control would make life easier for organizations and individuals, but different aggregators do not have a built-in incentive to develop interoperability between them (middle). Compared to the aggregation model, MyData is resilient system because it is not dependent on a single organization or technical infrastructure (bottom).

4 – How does MyData approach work in practice?



Individual / data subject / account owner: person who created and is using the account to link new services and authorize data flows with consents. Has relationship with the source, the sink and the operator

MyData Operator: Provides MyData Accounts and related services. Account enables digital consent management – Authorization as a Service.

Data sources and data using services: Data source provides data about the Individual to the services that use this data (Data Sinks). Same actor can be working as both Data Source and Data Sink.

Consent flow

Data flow

Figure 4.1: Four defined roles within the MyData architecture include 1) individual, 2) MyData operators, 3) data sources, and 4) the services using data. The flow of consents or permissions to use the data is separate from the actual flow of data.

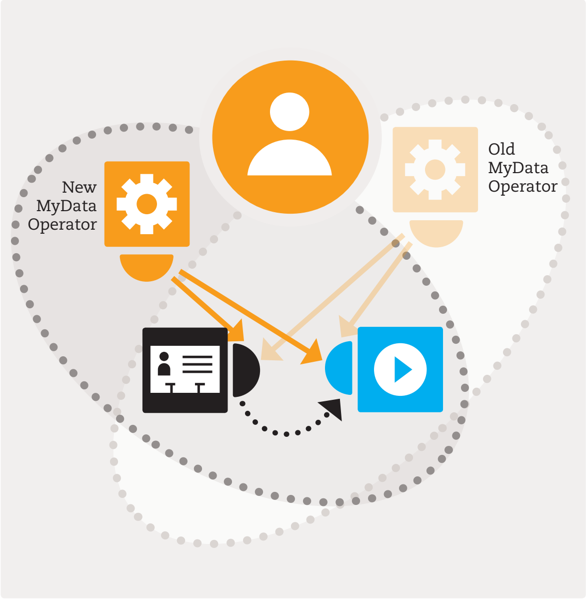


Figure 4.2: Individuals can change their MyData operator without losing their MyData account content. This mechanisms increases trustworthiness of MyData approach and encourages people to create data flows.

The MyData architecture is based on interoperable and standardized MyData accounts. The account model provides individuals with an easy way to control their personal data from one place even while the data is created, stored, and processed by hundreds of different services. For developers, the account model facilitates access to data and removes dependencies on specific data aggregators. MyData accounts will generally be provided by organizations that act as MyData operators. For organizations or individuals willing to be operator-independent, it will also be technically possible to host individual accounts, just as some people currently choose to host their own email servers.

In the MyData architecture, data flows from a data source to a service or application that uses the data. It is important to understand that within the MyData infrastructure, the flow of consents or permissions is separate from the actual flow of data (see Figure 4.1). The MyData account should not be confused with personal data storage (PDS) solutions, that enable storing data in a secure place under the direct control of an individual custodian. The primary function of a MyData account is to enable consent management – the data itself is not necessarily streamed through the servers where the MyData account is hosted.

Application Programming Interfaces (APIs) enable interaction between data sources and data users. MyData-compliant APIs provide data in a machine readable format and also enable the data sources and users to exchange information with the MyData account. As a result, it is possible to build a centralized dashboard where the individual may grant access and give or cancel permissions for multiple data sources and services. Any service provider can build a MyData API and enable their service to be connected with MyData accounts directly. If the service does not have a MyData-compliant API, it can be connected via a MyData proxy service.

Standardized MyData architecture makes the accounts interoperable and allows individuals to easily switch operators. This is major element contributing MyData's trustworthiness. Interoperability is the core advantage provided by MyData, but it is also the core challenge. Interoperability within the data management system can be understood as functioning similarly to interoperability in mobile telephone networks. Both systems require a common network that connects distributed nodes. Global interoperability and transferability of MyData accounts (and thus individual's consents) between operators requires further standardization and design on e.g. trust networks, data formats, and semantics.

MyData approach works in practice:

- MyData accounts hold consents that determine how data can flow from data sources to data users in an authorized system.
- For personal data management it is sufficient for the authorization consents to be centralized in the MyData account. Data can flow directly between the source and the user.
- Due to account portability, individuals can easily choose and change their MyData operator service. The service provider lock-in is minimal.

5 – Why is MyData focused on consents?

MyData intends to build trust in personal data services through a combination of transparency, interchangeability, public governance, respectable companies, public awareness, and secure technology. Consent management is the primary mechanism for permitting and enforcing the legal use of data. Via MyData accounts individuals can instruct the services to fetch and process data in accordance with consents that the individual has granted to data services. In technical and legal terms, consent is equivalent to authorization.

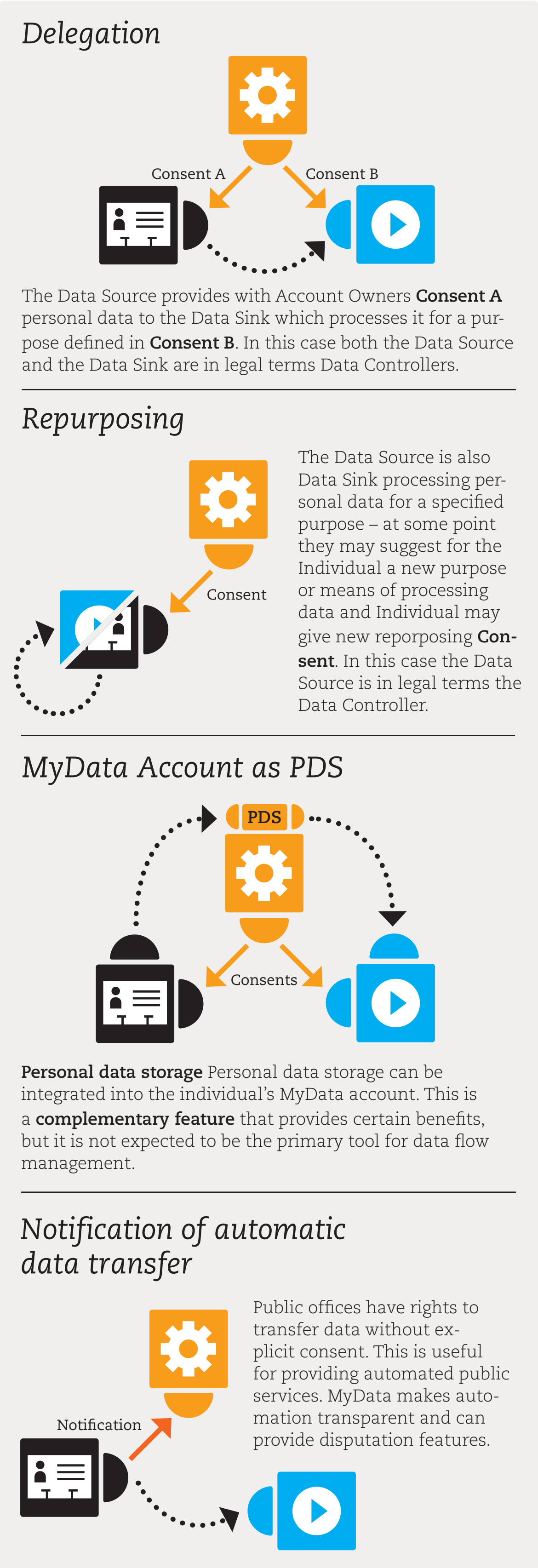
In the MyData model, consents are dynamic, easy for people to comprehend, machine-readable, standardized, and managed in a coordinated way. A common format will make it possible for every individual to delegate data processing to third parties or to repurpose the use of data in new ways (see Figure 5.1).

MyData consent management structures can be developed by using the open consent meta-format (Kantara Initiative). The open consent format is compliant with common consent regulations across jurisdictions and it is designed to operate smoothly also under the forthcoming EU data protection legislation (EU General Data Protection Regulation). The legislation is expected to require that data subjects give their explicit and informed consent to services that will use their personal data, unless a consent exemption or a legitimate interest takes precedent. In order for companies to both comply with tightening regulations and to continue to provide innovative services, it will be necessary to create a functional, interoperable, and easy-to-use consent management system.

Not all personal data usage requires the consent of data subjects. There has been critique that MyData could complicate the automation of services by focusing on detailed consent management, especially in cases where there is a legal base for personal data processing without consent. For example, public authorities are allowed to exchange data between each other without the consent of the data subject in certain circumstances. In such cases, the MyData infrastructure would not be used to enforce consent based data management, but it would act instead as a transparency tool to notify end-users of the use of their data. It benefits everyone if public authorities are able to exchange personal data in a transparent way. The MyData infrastructure may also act as a channel for ordinary citizens to opt out of services that involve the use and exchange of their personal data by public authorities and in more granular contexts than they deem to be acceptable.

MyData is focused on consents because:

- consents are the primary (but not the only) legislative framework that defines information processing from the human-centric perspective
- the same consent management framework can also be used with minor modification for notifications and assignments
- human and machine readable standardized consents unite technical data management systems, legislative frameworks, and the human perspective



Delegation

The Data Source provides with Account Owners **Consent A** personal data to the Data Sink which processes it for a purpose defined in **Consent B**. In this case both the Data Source and the Data Sink are in legal terms Data Controllers.

Repurposing

The Data Source is also Data Sink processing personal data for a specified purpose – at some point they may suggest for the Individual a new purpose or means of processing data and Individual may give new reporposing **Consent**. In this case the Data Source is in legal terms the Data Controller.

MyData Account as PDS

Personal data storage Personal data storage can be integrated into the individual's MyData account. This is a **complementary feature** that provides certain benefits, but it is not expected to be the primary tool for data flow management.

Notification of automatic data transfer

Public offices have rights to transfer data without explicit consent. This is useful for providing automated public services. MyData makes automation transparent and can provide disputation features.

Figure 5.1: Examples how MyData approach can support different kinds of data flow use cases such as delegation, repurposing, notification and data flow through the personal data storage (PDS)