Edited by:
Joss Langford
Antti 'Jogi' Poikola
Wil Janssen
Viivi Lähteenoja
Marlies Rikken

Understanding MyData Operators

Thank you

MyData Global (mydata.org) represents hundreds of individuals and dozens of organisations as members in more than 50 countries. We want to thank the members that have, through their membership contributions, made it possible to produce and publish this paper.

The following MyData Global members have supported the editorial work and production of this paper:

Coelition
InnoValor
Sitra

At the time of publication, the following proto-operators were members of MyData Global:

1001 Lakes
comuny
Cozy Cloud
Datafund
DataSign
DataYogi
Diabetes Services
Digi.me
esatus
fair&smart
Gravito
Healthbank cooperative
iGrant.io
JLINC
Meeco
MIDATA
Mydex
MyLife Digital
NTT DATA Corporation
Numbers
Ockto
Own Your Data
Peercraft
Polypoly
Posti
Qiy Foundation
Schluss
Smart Species
Vastuu Group
Younode

A full list of MyData Global organisational members and the opportunity join as a member is available at: https://mydata.org/organisation-members

Contributors and the MyData Operators Thematic Group

This paper is a work product of the *MyData Operators Thematic Group* which is part of the MyData Global organisation. MyData Global is a registered association whose mission is to advocate for a human-centric approach to personal data.

The purpose of the MyData *Operators Thematic Group* is to develop the definition and processes associated with the MyData Operator, as described in the MyData declaration (2017, see mydata.org/declaration). The group gathers individuals and organisations with deep experience in the fields of interoperability and human-centric management of personal data. The following people have actively contributed in the development of this paper:

Benjamin André (Cozy Cloud), **Henrik Biering** (Peercraft), **Lal Chandran** (iGrant.io), **J Cromack** (MyLife Digital), **Matthias De Bièvre** (Visions), **Dominik Deimel** (comuny), **Olivier Dion** (Onecub), **Katryna Dow** (Meeco), **Johannes Ernst** (Indie Computing), **Adrian Gropper** (HIE of One), **Iain Henderson** (JLINC Labs), **Marie-José Hoefmans** (Schluss), **Jonathan Holtby** (Dataswift), **Harri Honko** (Vastuu Group), **Mika Huhtamäki** (Vastuu Group), **Wil Janssen** (InnoValor), **Kai Kuikkaniemi** (S Group), **Vladimir Kuparinen** (SmartPaper.fi), **Viivi Lähteenoja** (MyData Global), **Joss Langford** (Coelition), **Xavier Lefevre** (fair&smart), **Jan Leindals** (Diabetes Services), **Mark Lizar** (OpenConsent), **Lotta Lundin** (iGrant.io), **Alan Mitchell** (Mydex CIC), **Antti 'Jogi' Poikola** (MyData Global), **Gaston Remmers** (Mijn Data Onze Gezondheid), **Marlies Rikken** (InnoValor), **Mikko Sierla** (Vastuu Group), **Dixon Siu** (Personium), **Maurice Verheesen** (Schluss), **Paul Wang** (ICON), **Kaliya Young** (Identity Woman), **Isabelle de Zegher** (b!loba).

As the MyData Operators Thematic Group, we seek to promote the MyData operator approach to human-centric personal data management and to contribute to a common understanding of that approach both within the MyData community and more widely. We bring together the best minds to provide thought leadership to inform technological and business initiatives. We focus on practical aspects of technology and governance to make the operation of infrastructures for personal data sharing, use and management easier and more human-centric, with the long-term goal of establishing full interoperability between operators.

We meet regularly and create publications to support operators, other MyData members, and the global personal data community. We seek to inspire the development of human-centric operator technologies, business models, and public policy that embody the MyData principles and to identify opportunities for collaboration.

Table of contents

Executive summary

This is an introductory paper to **MyData operators**: actors that provide infrastructure for human-centric personal data management and governance. An increasing number of businesses, legal experts, technologists, policy makers, and civil society actors are turning towards the general idea of approaching personal data use and management from a human-centric perspective. In addition to laws and regulations, infrastructure for the management of personal data is also key to moving towards human-centricity in practice. The actors operating the infrastructure can guard the limits on what kind of activity is, and is not, possible or allowed.

The concept of **MyData operators** was introduced in the MyData white paper (Poikola, Kuikkaniemi and Honko, 2015) and the **MyData declaration** (MyData Global Network, 2017), but it has been empirically explored only at limited scale (European Commission, 2016; Lehtiniemi, 2017). For this paper, we have taken the **MyData principles** as a starting point and we have studied existing examples of initiatives and organisations that are in one way or another either performing the role of an operator in personal data ecosystems or who offer related tools, services, or technologies. These **proto-operators** can be considered **'trusted intermediaries'**. There is extensive literature and practice around trusted intermediaries of many forms and with many names: **infomediaries** (Hagel and Singer, 1999), **vendor relationship management tools** (Project VRM, 2008), **life management platforms** (Kuppinger, 2012), **personal data stores** (World Economic Forum, 2013), **personal information management services** *PIMS* (Ctrl-Shift, 2014), **personal information management systems** (Abiteboul et al., 2015), **information fiduciaries** (Balkin, 2016), **mediators of individual data** *MID* (Lanier and Weyl, 2018), **information banks** (MIC Japan, 2018), **data trusts** (ODI, 2018), **personal data co-operatives** (Hafen, 2019), or **providers of personal data spaces** (European Commission, 2020).

This paper has been developed in close collaboration with many of the existing **proto-operators** and it presents the current 'state of common understanding' of what being a MyData operator entails. In the paper we present the **initial minimum requirements** to be considered a **MyData operator.** Common understanding and a shared language are essential for progressing towards the envisioned human-centric personal data infrastructure and to ensure interoperability between operators.

One of the central ideas of the **MyData operator** model is that there will be a large number of actors providing personal data management services, and that those services should be interoperable and substitutable as well as technology agnostic as far as possible. Competing service providers should work together to create a global network for human-centric personal data transfer in a similar way to how different banks form a network for payments or mobile operators for phone calls. We recognise that this kind of interoperability is a journey where every step has positive impacts for people and service providers. Our ambition is that this paper, supported by the **proto-operators**, is the first step on this journey and that many more organisations will join to shape the future work needed.

Paper outline and research questions

The introduction describes the background to the concept of MyData operators as infrastructure providers in personal data ecosystems. Also in the introduction, we define ecosystem roles, what is expected from operators for them to demonstrate their adherence to the MyData principles, and the idea of mutually interoperable operators. This is done based on the MyData declaration and other prior work.

We have gathered and analysed examples of over 40 proto-operators from a dozen countries and engaged many of them in the process of compiling this paper. Our key questions when studying the landscape of the proto-operators have been: *What are the functions a MyData operator should fulfil and what responsibilities should it have? What is needed to create interoperability between the operators? What are the roles of legislation and governance frameworks in ecosystems and how can operators bring better governance to human-centric data sharing? What are possible operator business models?*

These questions are addressed in the results section where we present functional elements of the proto-operators studied as a reference model and where we start to define multi-operator interoperability, human-centric governance and operator business models.

Reference model: The MyData operator reference model provides a structure within which to analyse operators' offerings and characterise their functional elements. The reference model creates a baseline for expectations for an operator from individuals, other operators, and other actors in the ecosystem.

Interoperability: Interoperability is key to realising the many benefits of the MyData vision. We describe different aspects of interoperability, recognising how these are currently prioritised by the proto-operators studied and indicating the role that MyData can play in enhancing human-centric interoperability as ecosystems mature.

Governance: The governance of human-centric data sharing ecosystems is discussed in the contexts of legal and voluntary frameworks. We consider how governance should be formulated and enacted, taking into account transparency, the responsibilities of operators towards individuals, and how the nature of who controls an operator impacts this relationship.

Business models: We study parameters of the business models options available to and currently used by the proto-operators, covering fundamental design criteria from the perspectives of human-centricity and financial sustainability.

Many more essential questions and important items to study further were raised during the work conducted for this paper and these are addressed in the future work section of the paper. We conclude by summarising the MyData operator minimum requirements, and by laying out a roadmap for progressing on the journey of interoperability with growing numbers of collaborating proto-operators.

1. Introduction
– MyData operators

Since the early days of the World Wide Web, the Internet has evolved from being a unidirectional broadcasting system, where companies showcased their products and services, to a multi-modal system with increased user engagement. This evolution has given rise to a situation where many technology giants, on the pretext of providing improved services, have begun to track every action of every user with little or no transparency provided to individuals about the use of personal data so gained about them. Further, new business models have emerged based on selling data about people to third parties without consent from the individuals in question and with no means for them to opt out. The result has been that clicking 'Agree' for consent was dubbed the internet's biggest lie (Obar and Oeldorf-Hirsch, 2018) and incidents of data misuse such as unsolicited calls, spam, and deliberate manipulation have resulted in a massive trust deficit.

Opportunities for innovation and efficiency have also been lost. The same data about the same individuals is collected over and over again and this data is siloed and poorly maintained. Individuals cannot keep track of where data about them is held and it rarely flows between platforms. And individuals are not the only ones to be harmed. The platforms and large corporation systems now dominate markets to such an extent that many smaller companies, media organisations, and other market participants are finding it difficult to opt out of these incumbent systems. Public actors, such as cities (Karhu et al., 2020), also face problems in managing the personal data they collect, share, and use across their services or with contracted private actors. Public actors are not looking for ways to monetise data, but need tools to process personal data in an ethical manner with their citizens in control.

1.1. Human-centric personal data

Organisations and initiatives are independently converging towards similar ideas about personal data infrastructure, management, and governance, where the people themselves would be in the driver's seat regarding the use and sharing of data from them and about them. This human-centric perspective promises to be the best and most inclusive approach to address the ills of the current data economy and, at the same time, to seize the opportunities for better use of personal data. Some examples of early communities focused on this topic area include the Internet Identity Workshop[1], the Personal Data Ecosystem Consortium[2], and the Open Data & MyData Working Group under Open Knowledge Foundation[3].

Beginning with and facilitated by a series of international meetings and conferences from 2015 onwards, the MyData community has emerged as uniting supporters of the human-centric paradigm. The MyData declaration was published in 2017 as the joint understanding of the direction for MyData, the following year an international nonprofit organisation MyData Global was established. The human-centric MyData paradigm is aimed at a fair, sustainable, and prosperous digital society where the collective benefits of personal data are maximised, by fairly sharing them between organisations, individuals and society. It seeks, on the one hand, to ensure that people get value from data about themselves and are able to set the agenda for how it is used. On the other hand, MyData aims to establish the ethical use of personal data as always the most attractive option for organisations.

1 https://internetidentityworkshop.com
2 https://pde.cc
3 https://personal-data.okfn.org/index-13.html

1.2. Ecosystems and infrastructure operators

Personal data is created, copied, moved, and used in ecosystems of individuals, data sources, data using services and actors in other roles. These ecosystems rely on infrastructure and infrastructure providers, who are crucially important in turning human-centric thinking into reality. Within any transaction, there will always be at least one actor operating the infrastructure that guards the limits of data processing by the actors involved. The MyData declaration asserts that this role must be carried out in such a way that individuals are able to securely access, manage, and use the personal data about them, as well as to control the flow of this personal data (MyData Global Network, 2017).

An operator of infrastructure is positioned to connect the person and all other roles in the ecosystem. To enable viable use cases, participation of individuals, data sources, and data using services are all needed in partnership with these operators. If any one of these is missing, the case cannot exist. In business terms, the operators are in a multi-sided market position. The value propositions of the operators should be viewed at the same time from the perspective of individuals and organisations:

For individuals: Operators provide transparency, understandability, and convenience to individuals when they share data or receive services using data about them. Operators provide an aggregated view to an individuals' personal data, allow them to control who can use the data and for which purpose, and transparently expose past data use and sharing. Other benefits include intuitive user interfaces, enhanced security, and the tools for managing relationships with different services that process personal data.

For organisations: Operators provide easy, legally compliant connectivity to an ecosystem of data sources and data using services as well as a relevant base of potential users. Operators facilitate access to high quality, up-to-date data in real time, offer tools and mechanisms for legal compliance such as logging and audit trails of permissions, and offer outsourced tools for complying with data portability requirements.

1.3. MyData principles for operators

While the MyData principles are highly aligned with data protection regulations in many countries and regions, they seek to empower people and communities with data, far beyond mere compliance with legislative requirements in any one jurisdiction.

The MyData declaration describes six principles for moving towards a human-centric vision of personal data. These principles imply the following requirements for the relationships between operators and individuals and other actors.

Human-centric control of personal data: This principle requires that any personal data transaction by an operator always involves[4] the individual. It also requires that the actions required of and performed by the person, such as giving permission, are very easy for individuals to understand.

Individual as the point of integration: Operators deliver the integration of services and data to the individual and, therefore, have a responsibility towards the individual (a duty of care).

4 Individual involvement may take place in the form of setting preferences prior to the actual data transaction.

Individual empowerment: This principle requires operators to support a shift from an individual merely giving permissions when asked, to them having a wide range of real choices, the initiative regarding data about them, and the ability to negotiate terms.

Portability – access & re-use: This principle allows individuals to go beyond control of their data to create their own uses for personal data. Operators must support individuals to re-use personal data about them.

Transparency & accountability: Adopting these principles, operators must be prepared to deal with intended as well as unintended consequences of personal data use in a manner that creates trust and mitigates potential risks. Without transparency, personal data sharing practices cannot be inspected or contested.

Interoperability: Interoperability requires that individuals are able to move between operators and to transfer data within the ecosystem without the need for transformation or interpretation. Operators must work together, and with other actors, to achieve this.

1.4. Mutually interoperable operators

Operators are not the end goal in themselves. Rather, they serve a role in the creation of sustainable and human-centric data management infrastructures for personal data ecosystems. Different ways to organise personal data infrastructures exist and some of them are more aligned with the MyData principles than others.

It is easy to imagine at least four different high-level scenarios for organising personal data infrastructures. These are not to be considered mutually exclusive, as co-existence and hybrids are possible.

Fragmented: Markets where many small operator-like entities compete to build small-scale use cases without interoperability between them.

Monopolistic data platforms: A few platforms provide connectivity and data sharing inside their ecosystems with little competition and no incentives for interoperability between the platforms.

Fully decentralised: A peer-to-peer world where standardised technical infrastructure and protocols enable data connections without any specific operator entities. In the decentralised model, the individual manages data flows directly from the end services or by having personal cloud-based applications on their own devices or hosted for them.

Competition-based interoperable operator network: Similar to the current network of telecom operators, energy providers, or banks where many mutually competing providers are interoperable and together provide global-level connectivity.

There is a common understanding that the first two scenarios (fragmented and monopolistic) are not desired states from the MyData perspective. It is hard to see human-centric principles sustainably maintained in them, however, they do describe the current starting point of the journey towards the more desirable scenarios (decentralised and competition-based). There are many proto-operators in the market that are not interoperable yet, but aim to be. There are also proto-operators that may

evolve to build critical infrastructure for the decentralised scenario, for example by integrating or embedding operator functionalities such as permission management seamlessly into service providers without the need for operators.

The ongoing debate over the relative advantages and disadvantages of the fully decentralised scenario is full of examples of both. Going fully decentralised may give developers the greatest flexibility to design or augment open-source software solutions that do not depend on trusting a third-party. Technology should, in the near future, allow also for self-sovereign peer-to-peer cloud storage. Counter-arguments for full decentralisation maintain that, even if technical infrastructure could be peer-to-peer, there are other reasons that operators would be beneficial as trusted intermediaries. From the societal perspective, the fully decentralised scenario could overly burden individuals with responsibility. Further, collective safeguards and regulatory oversight might be easier to establish in a model where there are clearly identifiable, and possibly certified or licensed, operator entities.

The competition-based interoperable operator network scenario would be comparable to telecom operators which, through shared standards and roaming arrangements, can provide global connectivity. A system of mobile telephony is far more beneficial for users than a fragmented system where one could only call phone numbers within the same mobile operator network. In such multi-operator networks, operators provide value to each other in addition to their value propositions to individuals and organisations. In an ecosystem with multiple mutually interoperable operators, this value is created from network effects and diminishing costs through collaboration, risk sharing and standardisation. If each operator makes their connections to individuals, data sources, and services accessible to a common ecosystem, these operators collectively can then more quickly demonstrate a credible market and wide connectivity.

In the MyData community, there is strong support for the competition-based scenario. However, it is possible for the last two scenarios (decentralised and competition-based) to co-exist without compromising the MyData principles. This is possible if proper protocols exist for discovery and communication between the parties in the decentralised model and the operator network. In some cases, these two scenarios may even mix within the same offer.

1.5. From ecosystem roles to actors and functionalities

An ecosystem is composed of actors holding one or more of the main roles as described in the MyData declaration:

Person: The role of data subject as represented digitally in the ecosystem. Persons manage the use of personal data about themselves, for their own purposes, and maintain relationships with other persons, services, or organisations.

Operator: The role responsible for operating infrastructure and providing tools for the person in a human-centric system of personal data exchange. Operators enable people securely to access, manage, and use personal data about themselves as well as to control the flow of personal data within and between data sources and data using services.

Data Source: The role responsible for collecting, storing, and controlling personal data which persons, operators, and data using services may wish to access and use.

Data Using Service: The role responsible for processing personal data from one or more data sources to deliver a service.

In addition to the four roles above, originally described in the MyData declaration, we recognise also a role for **Ecosystem Governance**. This role is for actors that are responsible for managing, developing, and enforcing the governance frameworks for the ecosystem.

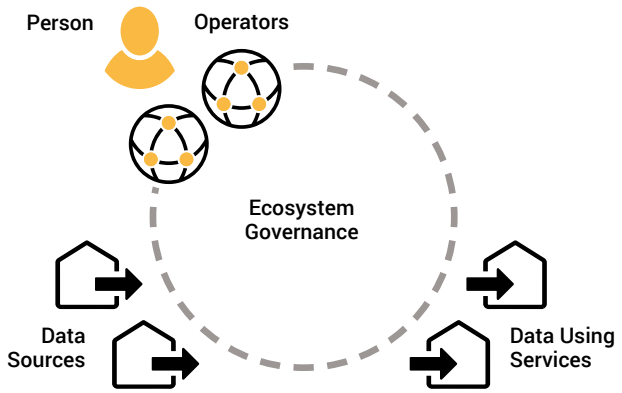

Figure 1: Illustration of a multi-operator ecosystem with the five roles of Person, Operator, Data Source, Data Using Service and Ecosystem Governance.

In practice, people and organisations do not get services from abstract roles, they get services from real-life actors. Different kinds of actors like governmental organisations, private companies, and even individual people can take the roles of operator, data source, data using service, or ecosystem governance.

Example of a data transaction in a multi-operator ecosystem: A *person*, whose debt has grown beyond what they can manage, seeks debt counseling from their municipality. This debt counseling process can be supported by a specific *operator* for this purpose, which facilitates data gathering from multiple *data sources* (such as creditors, employers, tax authorities etc.) and the secure and controlled data transfer to *data using services* (such as the municipality and social security administration). It might even be the case that more than one operator is involved. For example, a specific operator focussing on health care costs may be used.

The role of an operator can have a wide range of functions associated with it. In this paper, we explore these functions and how those can be delivered in line with the MyData principles to further understand the notion of a MyData operator.

2. Methodology — studying the proto-operators

This paper is the result of over a year's work by many members of the MyData community. In the call for proposals preceding the 2019 MyData conference in Helsinki, several groups requested a workshop to explore the roles and definition of the MyData operator. An open working group convened on a bi-weekly basis to prepare a briefing paper for the conference workshop (Janssen et al., 2019). The half-day workshop in September 2019 was attended by over 30 delegates and addressed a series of polarising questions that attempted to define the scope of the MyData operator (MyData Global, 2019). Following the conference, the bi-weekly open calls continued with the aim of creating this white paper on understanding MyData operators by consolidating the learnings from the group of contributors.

In February 2020, the *MyData Operators Thematic Group* was approved by the MyData Global board to provide a structure for the ongoing initiative (MyData Global, 2020). The MyData Operators Thematic Group gathers a diverse range of individuals and organisations with long-standing experience in the interoperability and sharing of personal data. Many participants of the group run organisations that have proto-operator functionalities, are involved in the technical or service design of proto-operator offerings, and have deep knowledge of how these functionalities are delivered across many sectors.

Working together, we compiled the list of 48 proto-operators from 15 countries shown on the next page. The list is by no means exhaustive, rather it is illustrative and reflective of the methodology of this paper. During our work on this paper, we approached organisations that we knew could qualify as 'proto-operators'. We requested them to read and comment on the paper draft and subsequently indicate if they wished to be included as proto-operators in the final version. We here only mention those who explicitly responded to the request. There are many others which we do not know of yet and some who did not react to our initial request.

Analysing the examples of proto-operators collected, we see a wide variety of different kinds of actors in various stages of maturity with different technical approaches, business models, primary functionalities, offerings, and domains of activity. This diversity is a logical consequence of the early stage of evolution of personal data ecosystems and it shows that the field is in a phase of rapid innovation and convergence, where standardised approaches are likely to emerge as the maturity of the field grows.

Our method has been to uncover aspects of what is commonly understood among the various proto-operators, constantly validating our findings with the group of contributors. Obviously, what can be said about the state of this common understanding is more general than the state of the art of individual proto-operators.

Figure 2: Examples of proto-operators throughout the world (see Appendix 1: proto-operators studied for this paper). This landscape will be updated regularly on the MyData operators webpage https://mydata.org/operators

3. Results — the state of common understanding

The results are presented under the broad categories of a reference model, interoperability, governance, and business models. These results have been derived empirically from our observations and analysis of the identified proto-operators. Further, the results have been cross-checked and validated with these proto-operators. They also reflect the current state of discussion in the MyData community. They are not intended to be normative guidelines, but rather frame the debate so that more exact guidelines can be formulated. At some future point, these guidelines may then contribute to binding rules.

This paper is not a call to tear down the offerings that currently populate the field of personal data management, but a challenge to make their functional elements visible to allow for digital rights to be exercised and to enable a fully functioning market. It is a call to action for those architecting new systems and applications using personal data to think clearly about who is performing the operator role and how they are empowering people.

In order to better understand the commonalities and differences between operators, the *MyData operator reference model* describes typical functional characteristics present in many of the proto-operators. A crystal-clear picture of a MyData operator archetypes is not immediately evident by studying the proto-operators as they have different configurations of similar functionalities. The reference model has been structured to surface the differences of the proto-operators studied, develop a shared vocabulary to discuss them, and to provide context for future harmonisation.

We use the metaphor of a 'journey of interoperability' throughout and lay out its initial roadmap with the *minimum interoperability criteria* for operators. At every stage in this journey of interoperability, MyData operators will be expected to assist people, in whatever way they can, to exercise their rights and to be empowered with their data. They must also always strive to work towards and within open networks, while innovating and creating differentiated offerings in a competitive market.

Balanced and fair relationships between people and organisations do not emerge automatically in personal data ecosystems. There needs to be some explicit methods for human-centric governance to guarantee that MyData principles are followed. In the *governance of human-centric data sharing* section, we start to address questions regarding the extent to which it is the responsibility of an operator to 'create the balance' and to guarantee human-centricity. And if it is not the operator's responsibility, then what other options are available?

Finally, the current state of *proto-operator business models* is discussed with design criteria for future operators outlined. As the underlying business model strongly influences the functions and modes of activity of operators, it is important to define what kinds of business models are aligned with the MyData principles and which models might not be.

Under the sections of interoperability, governance and business models we present the initial minimum requirements to be considered a MyData operator.

3.1. The MyData operator reference model

The MyData operator reference model describes nine core functional elements of operators. These elements affect how easy it is to utilise personal data, how transparent and human-centric the utilisation of personal data is, and how well the infrastructure supports open competition. The choice of elements supported, their configuration, and the manner of their implementation are also important but they fall outside the scope of this paper.

In the rich and complex landscape of proto-operators, a basic common understanding of the types of functionalities offered is needed to allow a transition from a fragmented landscape of solutions to sustainable personal data ecosystems. The reference model is a tool for the proto-operators to describe their own functionalities using a shared terminology.

This reference model is the result of iterative synthesis from studying the wide range of functions that existing proto-operators currently support. All the elements described are present in many of the proto-operators and they are commonly considered as important or even essential for realising sound and sustainable personal data ecosystems. The empirical understanding gained from our research has been validated against previously presented conceptual models of key technical solutions for human-centric personal data management (Poikola et al., 2015; Rikken et al., 2019; Sitra, 2020).

We acknowledge that there are also important properties, such as information security, which are not included in this model. We have selected elements for inclusion in the reference model based on the criteria that they are relevant in the context of MyData, help to differentiate between proto-operators, and are directly valuable to individuals.

The reference model should not be thought of as a monolithic template for direct implementations. We emphasise that not all elements of the reference model need to be part of all operators. Value exchange, for example, may not be an important aspect in many ecosystems but can be essential in a commercial setting and, in those settings, it needs to be implemented according to the MyData principles. Functionalities can be also distributed or even duplicated over the different roles in the system: not everything resides with an operator in isolation, and some functions might apply to all roles (e.g., logging).

Technologies and standards related to each one of the functionalities in the reference model are being developed independently of each other and independently of MyData. We deliberately do not reference any particular technology or standard as we acknowledge that the development rate of proto-operators is fast and any technology choices of today are subject to change in the future. Evolving legislation, technology, standards, and organisations operating in the field of personal data management all affect how operators eventually implement the functionalities presented in this reference model.

A summary of the nine core functional elements follows and a more detailed description of each element, is provided afterwards.

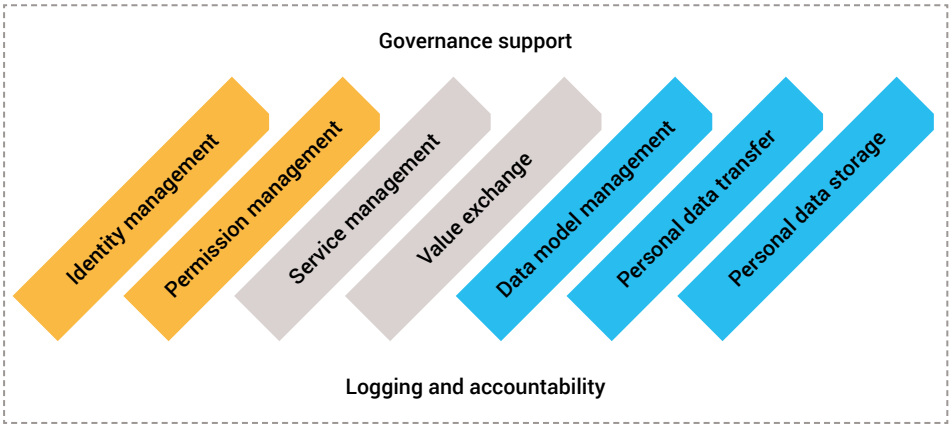

Figure 3: Functional elements of a MyData operator. The first two (yellow) pillars mediate data transactions in terms of participants and permissions. The middle two (grey) pillars describe what services are enabled in the ecosystem and how value can be exchanged between ecosystem participants. The right-hand three (blue) pillars manage data, its meaning, its exchange, and its storage. 'Governance support' and 'Logging and accountability' provide context for the other functional elements and are critical for transparency and trust in the ecosystem.

Identity management handles authentication and authorisation of individuals and organisations in different, linked identity domains and links identities to permissions.

Permission management enables people to manage and have an overview of data transactions and connections and to execute their legal rights. It includes maintaining records (notices, consents, permissions, mandates, legal bases, purposes, preferences etc.) on data exchange.

Service management uses connection and relationship management tools to link operators, data sources, and data using services. Data can be available from different sources and can be used by multiple data using services.

Value exchange facilitates accounting and capturing value (monetary or other forms of credits or reputation) created in the exchange of data.

Data model management is about managing the semantics (meaning) of data, including conversion from one data model to another.

Personal data transfer implements the interfaces (e.g. APIs) to enable data exchange between the ecosystem participants in a standardised and secure manner.

Personal data storage allows data to be integrated from multiple sources (including data created by a person) in personal data storage (PDS) under the individuals' control.

Governance support enables compliance with the underlying governance frameworks to establish trustworthy relationships between individuals and organisations.

Logging and accountability entails keeping track of all information exchanges taking place and creating transparency about who accessed what and when.

Identity management

Managing the identities of individuals and confirming identities of other actors in the ecosystem makes it possible for individuals to act as the 'point of integration' regarding data about them.

Individuals can have different identities, or profiles, with different data sources and data using services. For example, they can have public as well as private identities, or self-sovereign identities. The concept of self-sovereign identity *SSI* (Wang and De Filippi, 2020) is well aligned with human-centric personal data management. It provides a model for managing digital identities in which an individual or an organisation has the sole ability to control their accounts and personal data without the need for intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world.

Some operators also copy (cache) identity attributes, allowing them to function as a log-in tool. There is a grey area between operators and authentication-only tools, as some data attributes are also exchanged when identifying a person during authentication processes.

Permission management

Permission management covers the technical functionalities required for human-centric *control* of personal data, such as the user interfaces and underlying data data structures for individuals to view, understand, grant, revoke, and modify different kinds of permissions related to data flows.

The term 'permission' is used in a broad sense to cover the means that the individual has to take control of data flows. These means can be based on legislation (executing legal rights) or go beyond that. Part of the permission management functionality is that the operator only allows execution of such data transactions where the permission is valid.

Several proto-operators focus primarily on permission management, providing a way for people to orchestrate the specific data that can be shared (or disclosed) between parties, for which purposes, and for how long. These proto-operators often have the value proposition of facilitating legal compliance for the data sources and data using services involved in the data transactions.

The term 'consent' is human-centric, codified in law over centuries, and captured in technical implementations. The 1964 Helsinki Declaration (World Medical Association, 2018) advanced explicit human consent as a policy, ensuring individuals were informed and knowledgeable. The legal basis of consent for data processing in the GDPR demands informed and unambiguous legal clarity of that consent state, but every legal basis for processing enumerated in the GDPR also has an aspect of a meaningful human consent type (e.g., implied consent) associated with it. All legal justifications also require notice as a prerequisite for any type of consent. Within a framework for consent, permissioned tools can be distributed, and permission frameworks extend consent into digital contexts. Permissions maintain direct relationships between actors, and all are subject to the same notice and consent governance. All the considerations of consent, notice, preferences, and permissions are captured by the wider definition of 'permission' used in this functional element and throughout this paper.

Service management

Operators live in an ecosystem with data sources and data using services. Navigating this ecosystem requires the linking of actors through an operator: this is the purpose of the service management functionality. The human-centric manifestation of service management is the possibility for individuals to manage the relationships and connections to different data sources and data using services in the ecosystem.

Service management enables dynamic linking of data sources and data using services (permissioned by the individual) so that data can be available at different sources and can be used by multiple data using services.

In a multi-operator environment, it is a significant decision whether the operators use a shared service registry (potentially still distributed) or if each operator manages services separately. This is a topic that will evolve in future work; currently, there is limited standardisation or convergence in this field.

Service management encompasesses both access control and technical connection management. However, the delivery of these functionalities is largely determined by the data sources. Operators may support these to a greater or less extent through, for example, key management services.

Value exchange

Sustainable business models are a requisites for ecosystems in general (Haaker et al., 2006). This means that all of the actors in the ecosystem need to have more benefits than costs in the long run. Both benefits and costs can be also non-monetary in nature. For individuals, time and effort spent can be a big cost and benefits often come in the form of services. Our base assumption is that personal data ecosystems exist to lower transaction costs and, in total, an ecosystem enables the creation of more value than the overall costs incurred by the participants collectively. However, value creation does not happen equally in all parts of an ecosystem and mechanisms for distributing value are needed.

As operators provide technical infrastructure for making multi-party data transactions possible, they are also in a natural position to keep track of such transactions for the purposes of payments and billing or creating other forms of rewards, such as loyalty and bonus points. Operators may provide a standard 'accounting' mechanism which transparently keeps a log of the data transactions so that the different parties in the ecosystem may use it as the base for payments between the parties.

Using data as the means of payment and paying individuals for their data are contentious issues. The MyData operator reference model does not intend to solve or move that debate in any direction.

Data model management

In a world with different data sources and data using services, differences in data models are inevitable. Harmonisation of personal data models strengthens options and potential for data portability and increases usability of data. Data models related to data transactions also need standardisation to achieve interoperability between operators. For example, log data syntactics and permission models. Depending on the domain, semantic data standards are more or less evolved. Until widely adopted standards exist, translations between different data models are a necessity.

Data model management as an operator functionality facilitates translation of one data model to another. As many data standardisation processes are not human-centric in nature, data model management as an operator functionality can also facilitate interpreting standard data models to individuals. Personal data management without data model management is possible, but limited in terms of scalability, interoperability, and usability of the data.

Some proto-operators have taken the approach of offering data harmonisation as a service while some others are focusing more on the data transfer and leaving the data model management for the data using services.

Personal data transfer

Personal data transfer, through an operator or facilitated by an operator, is key to portability, access and re-use of personal data. This functionality realises the interfaces to allow data exchange between data sources, data using services and operators in a standardised and secure manner. Data transfer can follow different models: data can flow through an operator, or an operator can facilitate the direct transfer from data source to data using service under a valid permission.

'Data sharing' is a catch-all term that hides a multitude of variations. In most cases, there will be an original or 'master' version of the data that may be held by an organisation or an individual. Operators need to manage the transfer of personal data in line with permissions to ensure that data is not unnecessarily duplicated and can be updated easily across any copies when required.

Personal data storage

Many proto-operators provide personal data storage (PDS) for storing data originally created at the data sources and data created or asserted by the person. Such PDS functionality allows data to be integrated from multiple sources – harmonising, using and re-sharing it under the individuals control. The PDS can be implemented so that the operator does not have access to and does not know what data the person actually stores.

Using PDS as an 'intermediary station' for personal data configures the connections in the data ecosystem so that data sources and data using services can connect via the person, but not directly to each other. This configuration may simplify legal liabilities as well as the implementation of permission management.

As the person with the PDS is technically in the center of the data transactions, it can be considered also a highly human-centric approach for data transactions. Ideally, people would hold up-to-date 'personal master data' for many commonly used attributes and data types, such as contact and preference profiles. This would reduce the need of having the same data duplicated (and often outdated) in many places. The PDS approach works best for relatively static attribute types of data and for data that originates from the individual. They are less well suited to dynamic data that originates from other data sources.

From a principle-based standpoint, it can be argued that a PDS should be considered a separate data source controlled by the individual instead of a functionality provided by the operator. In practice, however, operators are very well positioned to offer a PDS and it is a common functionality of the existing proto-operators. If the operator provides personal data storage, it should be technically and functionally separated from the other operator services in a similar manner as banks internally separate banking services from financial advisory services.

Governance support

Human-centric governance helps mediate the relationships between people and organisations. This dedicated functionality in an operator can guarantee that MyData principles are followed and enable compliance with underlying governance frameworks.

All operators, to some degree, need to operate within a framework of governance in order to be transparent about assurances to individuals concerning the quality and trustworthiness of their services. Operators may be able to select governance frameworks within which to work or they may have to respond to mandatory requirements within their sector and jurisdiction. Governance requirements translate into responsibilities for the operator which can then, in a well governed ecosystem, result in liabilities. In a governed transaction, a specific liability can be agreed upon or transferred. The governance support element contains the functional counterparts of the ecosystem governance frameworks discussed later. Operators may enhance and deliver this functionality.

Accountability and logging

Transparency and accountability are important principles and prerequisites in many legislations. Accountability can enhance assurance and logging can mitigate risks of misuse or unintended use. Logging is not the sole responsibility of the operators and has counterparts in data sources and data using services.

Accountability arrangements may flow from the rules and regulations in the underlying governance framework, but many proto-operators work without an explicit governance framework. Even in those cases, operators have to comply with the relevant legislation that often includes logging and accountability obligations.

In general, governance implies some accounting obligations; but if no explicit governance applies, logging and accountability are still needed for auditability and transparency.

3.2. Minimum interoperability requirements

The MyData community holds strong expectations for operators to co-operate and work towards interoperability. It is thought that even actors functionally similar to MyData operators will not be considered as such if they do not embrace the vision of future interoperability between operators. Operators should be proactive on the journey to interoperability to allow for ecosystem growth, and share resources.

There are many dimensions of interoperability and clarity on specific objectives is required to make progress on our journey. We need to understand both the means for achieving interoperability and our ambitions for it. In the context of an interoperable MyData operator network, we identify four areas of focus:

Transparency and usability: Turning formal rights into actionable rights for people. This means using control vocabularies and semantics for transparency and common elements of user experience such as recognisable icons and labels.

Standardising interfaces for personal data: Enabling ecosystems to scale fast and for data portability to become seamless.

Enhancing roaming possibilities: Enabling the routing of data transactions via multiple operators so that there is no need for all people and all services to link to a single operator.

Enabling substitutability: Supporting easy switching of operator services and, ultimately, fungibility of base functionalities which are entirely interchangeable with indistinguishable inputs and outcomes.

Interoperability provides overall system benefits at different, distinct dimensions that can and should be developed concurrently: technical (connectivity), semantic (informational), and organisational (governance, business models etc.) (Tolk, 2010).

Technical level: Definitions of connectivity, syntactics, and protocols for data exchange (e.g., APIs) and data storage that underpin basic integration. The first objective here is to enable the easy connection of new data sources and data using services to an operator and their mutual interoperability, where operators can work with each other technically.

Semantic level: Harmonised information with shared data models and mutually agreed content. The pragmatic approach here is to identify the categories of data where common data models are most essential for MyData. These could be semantic models for data control and governance (e.g. data transaction records, consent records purpose categories) or widely used attribute data types and domain specific data models.

Organisational level: interoperability in more mature ecosystems goes beyond the technical and semantic levels, encompassing shared objectives and policies between organisations. These objectives and policies will cover issues such as responsibilities, liabilities, business models, and governance structures.

While we will work with other organisations to address opportunities for legal interoperability, for example, in the European Interoperability Framework (European Commission, 2017), it is currently beyond the scope of this paper and future work.

Organisational, semantic, and technical interoperability are all essential if we are to achieve ecosystems with multiple operators, data sources, and data using services that can work together to deliver human-centric services for people. Interoperability between the different actors in different roles is required in order to enable effective data flows in the ecosystem. People should not be locked into services but should be able to choose to move when they want to. The ability of the person to change their operator without barriers, or to use multiple operators, further requires that there is interoperability between operators.

By understanding the ecosystem roles and using the reference model for architecting the implementations, we can reach a degree of technical modularity that enables the separation of concerns (SoC). This is an approach where each module addresses a different aspect, or concern, of the overarching system. When concerns are well separated, there are more opportunities for transparency and good governance.

The MyData community is uniquely placed to develop and drive the adoption of frameworks for interoperable human-centric data sharing. We have both the skills and the mindset to ensure that interoperability questions related to personal data are correctly framed around the needs of the person rather than the organisations that should be serving that person.

Delivering human-centric interoperability requires agreement, alignment, and significant effort beyond just drafting rules or technical specifications. This journey towards convergence can be guided by an evolving roadmap where the immediate steps can be easily seen already, and further plans can be made as the situation unfolds.

Common goal: The first step of agreeing on a common goal has already been taken as our objectives are defined in the MyData declaration.

Common understanding and definitions: The next stage is to create 'a state of common understanding' by defining agreed terms, as we do throughout this paper, and by describing systems and methods, as set out in the future work section.

Common processes: The output of this descriptive stage then allows us to identify common existing processes and common tasks.

Harmonising processes: We can then agree which tasks in which functional elements of the reference model are the best targets for initial harmonisation efforts. Selection criteria may be their linkage (or lack of linkage) to other elements, their impact on the overall functionality of the ecosystems, or the ease or difficulty of the harmonisation task. Ultimately, however, the selection will come down to people and organisations wanting to take on any specific task.

Common governance: In parallel, the position of MyData with respect to governance frameworks will need to be agreed.

This early roadmap follows an action standard approach, where compliance is defined by completing the specified steps rather than being a quality standard.

The initial minimum interoperability requirement for the proto-operator to be considered a MyData operator is to **describe the systems for personal data management with respect to the MyData operator reference model**. Proto-operators will need to show the modularity of their approaches as required by SoC. There will be aspects of a proto-operator's service that are proprietary and other aspects that can form templates of best practice for open standardisation. The functions of proprietary service components must be described and the operation of non-proprietary components must be transparent. The interfaces between modules should be de-

scribed in detail. This will allow us to identify the basic tasks commonly performed by most proto-operators and build interoperable components from there.

This phase of describing the proto-operator systems based on the common reference model and terminology will encourage the open sharing of practices and processes that have a common aim. The learnings from this phase will inform the development of the roadmap towards interoperability described above and, ultimately, the emergence of rulebooks, auditable specifications, quality standards, and test tools. Mutual interoperability is inherently supported by this iterative way of working and the shared knowledge will help operators to innovate faster, better, and with lower risks to privacy.

3.3. Governance of human-centric data sharing ecosystems

Governance should be targeted at facilitating trust and opening up the ecosystems for innovation. Individuals should be protected, empowered to benefit from the data that organisations hold about them, and endowed with control over and visibility of how the data about them is used.

The ecosystem created by operators, working with data sources and data using services, is always part of a broader, social and economic system of individuals, communities, public organisations and private companies. Therefore, the ecosystem functions within the wider context of legislation, regulation, and social norms. Legislation is necessary for the creation of trust, but it is not sufficient. In order to create a level playing field in the market, rules of engagement between the different roles and actors fulfilling those roles are needed. This is often captured in an ecosystem governance framework (also called trust framework (Makaay et al., 2017)) which is binding at the ecosystem level.

Whether legal jurisdiction provides enough protection for an individual or not, governance codifies the explicit formulation of the re-balancing power that individuals are provided with by an operator. The level of an operator's responsibility towards the individual depends on the ecosystem. For example, in some ecosystems there is no strong governance structure in place, so a MyData operator has a correspondingly bigger responsibility of setting and enforcing the human-centric rules. As the MyData principles are independent of legal jurisdiction and the specifics of an ecosystem, they provide a universal guide to the setting of such human-centric rules.

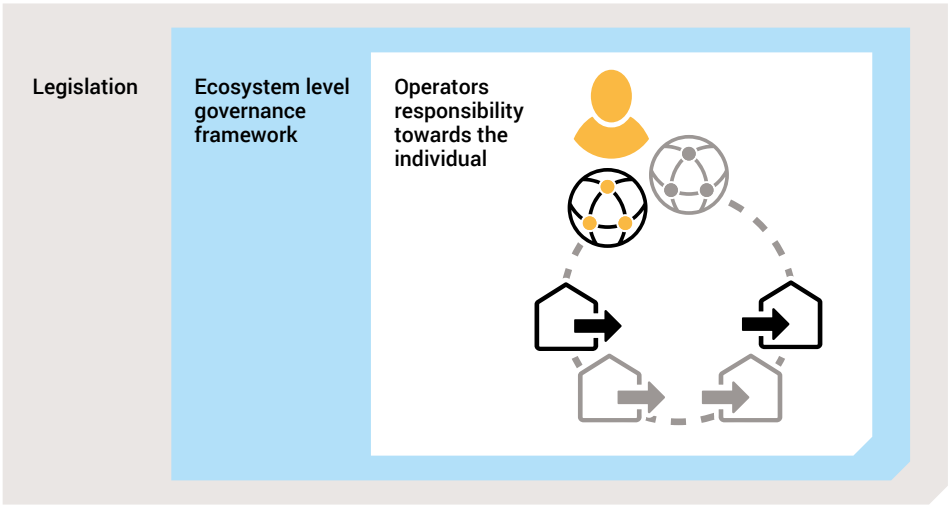

Figure 4: The tiers of governance in human-centric data sharing.

Legislation governing personal data ecosystems

In the European Union, the GDPR provides the authoritative basis for data exchange and privacy protection. Similar legislations have been introduced from Chile to Japan, from Brazil to South Korea, from Argentina to Kenya (European Commission, 2019). Beside general privacy and data protection laws, various sector-specific regulations also govern data exchange, especially in health and financial sectors in many jurisdictions. The recently published EU Data Strategy also indicates that some level of regulation of novel data intermediaries such as providers of personal data spaces can be explored in the context of the upcoming Data Act legislation (European Commission, 2020).

Ecosystem governance frameworks

The governance of mature ecosystems is typically based on rulebooks and underlying contractually enforceable agreements between parties in the ecosystem. Such a governance framework describes the binding, ecosystem-wide rules and specifications (business, legal, technical, social) and also defines the borders of the ecosystem contractually. Such governance frameworks may specify sanctions, auditing, and enforcement mechanisms for the rules. They can also help to regulate data standardisation, validate sources of data, manage permissions, enhance the portability of data, and establish ways in which individuals may exert influence on the governance structure itself. Well-known examples in other domains beyond personal data management include credit card systems such as Visa, domain name registration systems governed by ICANN, or telecommunication frameworks governed by GSMA and the ITU-T. In the context of personal data management, Qiy (Netherlands) and HAT (UK) are early examples of governance frameworks for personal data.

An operator's responsibility towards the individual

An operator is always an infrastructure provider and an enabler for all participants of the ecosystem within which it operates. Operators have a duty to care for the individual's bespoke interest and should facilitate a more balanced and fair relationship between people and organisations. The degree of responsibility that an operator holds towards the individual will vary depending on the types of functionality they deliver, the strength of the applicable personal data legislation, and the maturity and kind of ecosystem governance in place.

We consider it most likely that there will ultimately be different degrees of operator responsibility. In every case, operators will need to determine the appropriate degree of responsibility towards the individual, in balance with the strength of ecosystem governance and applicable regulations. It is illustrative here to consider the two extreme scenarios possible for degrees of responsibility: an operator with strong responsibility on the one hand and a more neutral operator on the other.

In the first scenario, there are cases where an operator is serving the individual with a very high level of responsibility. One approach is for operators to assume a fiduciary duty where, as fiduciaries, they must always put the person's interests ahead of their own (Balkin, 2016). Full fiduciary responsibilities restrict the choice of business models and may need to be backed by regulation (as seen with doctors and lawyers) to maintain a level playing field. Approaches with a voluntary, near-fiduciary degree of operator responsibility may be relevant to guarantee human-centricity

in weakly governed ecosystems with little externally enforced regulation or commonly agreed rules to protect individuals' rights and interests.

At the other end of the spectrum, the operator is a more neutral actor with a lower degree of responsibility in setting or enforcing rules to guarantee human-centricity. This approach is relevant when strong ecosystem governance, strict regulation, or an effective combination of the two is in place. The legislator or the governance body then becomes the ultimate guarantor of human-centricity and operators must follow the rules and regulations. The shared systems of governance and regulation increase confidence for the person while simultaneously reducing risks for operators and thus reducing costs and stimulating innovation.

Among the proto-operators currently, there is a general understanding that it is easier to start by having operators developing separate use cases and, in such situations, the operators should hold strong responsibility towards the individuals. The minimum requirement at this stage for the MyData operators is to **demonstrate alignment with the MyData principles**. In the future, the development seems to be towards governed ecosystems and thus more neutral operators.

Who controls the operator?

The control of an operator is a fundamental question when assessing how the principles of the MyData declaration will be applied and embodied. In our investigation into the different kinds of parties who might run an operator, we identified five broad categories. These categories are based on a classification of the kinds of relationships an individual might have with an operator. These categories are not mutually exclusive and, depending on their legal status organisations may fall into more than one category.

Business to person: Individuals are customers of the operators. For example, existing critical infrastructure operators such as banks, telecom operators, or utility companies could extend their services and become MyData operators. Also, new companies can be established based on this same commercial customer relationship.

Business to business: The individual has only an indirect relationship with the operator and this relationship is mediated by another service. For example, permission management functionality may be embedded in an end-user service that relies on an outsourced operator to provide that functionality.

Individual: Individuals themselves take responsibility for operating the infrastructure to interact with the rest of the ecosystem. This can happen, for example, by running their own personal data store (PDS) instance.

Collective: Individuals collectively support and manage an operator as members through the legal forms of associations, cooperatives, or data trusts. For example, existing patient associations, labour unions, or cooperative model companies could provide operator services to their members. Further, purpose-built data trusts and cooperatives are being experimented with in several places and domains.

Public: Individuals have a citizen relationship with an operator and the operator is run by public authorities. For example, cities or or other public entities could provide operator services especially to facilitate the flow of personal data in the context of public services.

Operators falling into different categories subsequently have different requirements for investment of financial and human capital. They also have different risk profiles across areas such as financial sustainability, privacy, and centralisation. However, it will be possible for MyData operators to be created and managed in all of them.

3.4. Operator business models

No operator can be sustainable in the long run without a solid business model, whatever their legal status or type of control. Operators can be run commercially, as nonprofits and NGOs as well as by public institutions.

In the long run, if true interoperability between operators is expected, there needs to be some convergence on business models so that they are compatible at the ecosystem level. Taking the example of telecom operators, they all work with the same basic business logic that the one who makes the call, pays for the call. If different operators had different value capture mechanisms (say, one charged the caller, another charged the receiver, and the third added advertisements before the call and charged the advertiser), then the interoperability needed to roam between networks would have been much more challenging to achieve.

Taking again telecom operators as an example, we have seen that the breakup of the national telecom operator monopolies has resulted in a significant drop in call charges. Likewise, personal data ecosystems must provide individuals and organisations with options for mutual engagement that are superior to platform-based monopolies in terms of convenience and cost as well as privacy and ethics. The MyData operators and ecosystem participants must find similar opportunities to establish alternatives to monopolies that significantly remodel the cost and income structures of the incumbent market platforms.

The current business models of the proto-operators we studied are not always clear and their sustainability may be limited. This lack of clarity and limited sustainability are characteristics typical of a market that is yet to develop, where an ecosystem is still in the process of inventing itself. Many proto-operators have already advanced beyond the initial pilot phase but the scale on which they are used is often still limited, of course with some exceptions. Additionally, interoperability between operators is just emerging as a priority for the current proto-operators. So far, bilateral agreements between operators, data sources, and data using services have been the norm.

There are costs associated with running an operator such as provision of compliance and security (including availability, utility, integrity, authenticity, confidentiality, nonrepudiation). Studying the business models of existing proto-operators, we observe three models of covering these costs: (1) revenue streams directly generated within the ecosystem, (2) revenue generated from outside the ecosystem but related to the operator activities, or (3) the operator function may be subsidised by entirely different activities. Currently, the first model is in its infancy and many proto-operators rely on the revenue from outside the ecosystem or subsidise the operator activity by other means.

As the operator market matures beyond the initial development phase, it is highly desirable that more operators move from the second and third models towards greater financial self-sustainability. It is desirable because it removes commercial influence from outside the ecosystem and ensures that actors are not reliant on, for example, government subsidies. Moving towards this objective of financial self-sustainability and the first model of revenue streams generated within the ecosystem, there are a number of possible options for operators in terms of from whom and how that revenue is created.

Person: one-time onboarding fees, recurring account fees, or pay-as-you-go fees.

Other operators: roaming fees, or a share of transaction and connection fees.

Data source: one-time onboarding fees, recurring account fees, or sales commission.

Data using service: one-time onboarding fees, recurring account fees, transaction fees, or connection fees.

An operator may also need to share revenue with these actors or to utilise other methods of value exchange. Business models will be built by balancing these revenue streams against the costs of delivering services. It is important to recognise the separation between what is paid for the data itself and what fees are paid for the connectivity enabling data flows. In many cases, these will be combined at the point of billing but for the sake of transparency and to maintain separation of concerns, they must be unbundled in building or describing a business model.

It is important to consider that some MyData operator businesses should become profitable in time. The different control and governance models of the operators will result in differences in how the revenue is shared. We will need to judge if some control structures can be seen as more or less aligned with the MyData principles than others, but this remains future work.

In summary, there are a variety of operator business models currently in use and available in the future as the field matures. The minimum requirement, in terms of business models, for the MyData operators is to show that they follow the two criteria of **transparency** and **the person as the primary beneficiary**. Information about the revenue flows must be as visible to the individual as the data flows and, where profits are made, they must be declared. We also recognise that individual agency in a market context requires the ability to pay and to be paid. However, we believe that we should consider the agency of people to extend also well beyond the confines of the market. This is why a MyData operator will need to prioritise their duty of care for an individual over encouragement for that individual to monetise or overly share personal data. For example, a business model that emphasises the volume of data transactions might become unable to exercise their duty of care towards the person in cases where those transactions are not to the benefit of the person. As a result, we assert that the markets in which MyData operators exist should be markets for services rather than markets for data.

4. Future work

The objective of this paper is to create a common understanding of the functionalities and responsibilities of MyData operators, and start a journey towards interoperability. We have arrived at high-level descriptions of the most important functional elements that characterise an operator and we have done this by cataloguing and studying some of the many initiatives and services that embody these functionalities today. Further, the reference model provided here will allow the community of proto-operators to coordinate, focus, and share the work of building an interoperable network of operators.

Arising from this work is the need for unambiguous definitions that support current proto-operators in becoming MyData operators of the future. To answer this need, we will guide the proto-operators to self-describe their alignment with the minimum requirements, we will further specify the reference model, we will develop more robust criteria along all dimensions of interoperability, and we will initiate work to assess options for governance frameworks and operator certification schemes. The fundamental aim is to make the operation of infrastructures for personal data use easier for people and more human-centric in general. Our work to advance on the journey of interoperability has immediate benefits for individuals as interfaces, processes, and communications become standardised - reducing the effort required to adopt new services.

As part of the future work, we will collaborate with the other MyData thematic groups on areas such as health, governance and design. For example, assessing the design of interfaces for individuals to promote ease of use and harmonisation.

Templates for self-description

We will create templates, such as structured questionnaires and associated reporting tools to allow proto-operators to self-describe, as simply as possible, their alignment with the minimum MyData operator criteria:

- how their approaches embody the MyData principles,
- the modularity of their systems with respect to the reference model,
- operation of their technical modules and associated interfaces,
- the common processes that they can harmonise and,
- their business models, including data flows and value flows between actors.

Further interoperability requirements

We will continue to develop the depth and breadth of the reference model described in this paper and define requirements across the different dimensions of interoperability (technical, semantic and organisational). On the technical level, standardised and publicly documented APIs will be considered to ensure that individuals and organisations can switch between operator services and access new data sources and data using services with minimal effort. Discovery of various MyData operators' ser-

vices should be made as simple as possible through publishing them with internet standards intended for this purpose or registering the services to a public directory.

On the semantic level, we will lead and guide the adoption and creation of shared data models and semantics among operators to provide harmonised information exchange and communication. Where commonly accepted standards, ontologies, libraries, or schemas are available, they will be utilised and we will support original works as necessary.

We will also drive organisational interoperability by creating rulebooks for ecosystem operation aligned with governance approaches (e.g., Sitra, 2019). In such rulebooks and frameworks we will define more decisively, the correspondence between the functionalities, actors, and roles in personal data ecosystems according to the MyData principles. For example, certain MyData operator functionalities may be defined as mandatory, recommended, or prohibited for actors fulfilling certain roles.

Governance frameworks and certification

We will work for the inclusion of MyData principles in developing frameworks for governance. The MyData principles provide a proven starting point for the formulation of more exact rules, requirements and restrictions which should be imposed to create successful personal data sharing ecosystems. Wider discussion is needed to consider what role, if any, MyData Global as an organisation should have in these governance frameworks.

We will support the development of clear requirements that can form the basis for voluntary certification programmes for operators, specific functionalities, or governance frameworks designed to implement human-centric data governance. We consider certification schemes with binding rules as a promising method to allow other actors in a given ecosystem to see and verify if an operator qualifies as a MyData operator. The principle-based descriptions in this paper and the future work of rulebook creation will allow the auditing of an organisation, a functionality, or a process to a quality standard required for certification or labelling. An example of a certification approach specific to operators is the Japanese government initiated certification programme (not law) for Trusted Personal Data Management Services (Onga, 2019).

Further, we will work together to provide thought leadership that inspires new initiatives and informs policy makers to develop a regulatory environment supportive of human-centric personal data management.

Conclusion

The idea of human-centric personal data is gaining widespread traction globally. The MyData declaration defines the role of the MyData operator and sets out high-level principles for a human-centric approach to personal data. In personal data ecosystems, the infrastructure operators are in key positions to implement these principles and to make human-centricity work in practice.

The MyData vision highlights competition in an open ecosystem where there are multiple providers of infrastructure-level services and that these services are mutually interoperable and substitutable. We use the metaphor of the 'journey of interoperability' for the work needed to progress towards such a global network of many competing and mutually interoperable operators. To initiate this journey, MyData Global used its 'power to convene' to bring together organisations that today run and develop operator-like services and related products and technologies. This paper is the studied result of the interactions with these proto-operators.

As a 'state of the common understanding' among the proto-operators, this paper presents the MyData operator reference model and initiates discussions on operator interoperability, the governance of human-centric data sharing, and the business models available for operators.

The reference model lays out nine core functional elements an operator may have: (1) identity management, (2) permission management, (3) service management, (4) value exchange, (5) data model management, (6) personal data transfer, (7) personal data storage, (8) governance support, and (9) logging and accountability.

Interoperability between operators should be framed in terms of the needs of the person rather than the organisations in a given ecosystem. After acknowledging this as our goal, and describing some common tasks and our approaches to minimum interoperability requirements, more robust requirements will be co-developed based on the reference model.

Governance of human-centric data sharing can be conceptualised at different levels, where legislation is the widest and the least specific, ecosystem-level governance frameworks function within the legislative sphere and set more specific rules for the participants of a given ecosystem and, most specifically, operators have certain responsibilities towards the individual. The responsibilities of an operator will vary depending on the strength of the ecosystem governance and the regulation.

Operator business models should be made fully transparent and designed with individuals as the primary beneficiaries.

The initial minimum requirements to be considered a MyData operator are to **describe the systems for personal data management with respect to the MyData operators reference model** (interoperability), **demonstrate alignment with the MyData principles** (governance) and show that the operator business model satisfies the criteria of **transparency** with **the person as the primary beneficiary**.

This set of minimum requirements will evolve as the field matures, but based on these initial minimum requirements it will be possible to develop methods for the proto-operators to self-certify as MyData operators.

The results of this paper represent a substantial advance in thinking on the topic introduced as 'trusted intermediaries' and described throughout as MyData operators. The outcomes are rudimentary and we recognise that follow-up collaborations are needed to iterate, evolve, and make them even more useful. We hope that this paper will stand the test of time as the foundational, common basis for co-developing the idea and implementations of MyData operators and for guiding the journey of interoperability. At the same time, we believe that some aspects of this paper will very soon become outdated as the growing community of proto-operators and other actors in personal data ecosystems makes progress on the issues laid out in the future work section.

If you would like to comment on this paper, to learn more, or if you are interested in joining our community, we invite you to contact us:

Contact: operators@mydata.org
Operators page: https://mydata.org/operators

Glossary

Term	Definition
Actor	An organisation or an individual performing one or more *roles*.
Data governance	A system that employs interoperability components (standards and policies) to ensure the acceptable use and high quality of data within a specific ecosystem. Manages the availability, usability, consistency, integrity, and security of the data used.
Data portability	The ability of data to be easily moved across interoperable applications and domains. The legal right to data portability, granted in some jurisdictions to individuals, can be delivered through a range of technical mechanisms and varies in scope according to the jurisdiction. The MyData principle of data portability encompasses the ease of both access to and reuse of data.
Data source	The *role* responsible for collecting, storing, and controlling personal data which *persons*, *operators*, and *data using services* may wish to access and use.
Data using service	The *role* responsible for processing personal data from one or more *data sources* to deliver a service.
Ecosystem	The overall system created by the activities and connections of a set of *actors* and infrastructure interacting according to a common set of rules. Multiple ecosystems can exist, overlap, and collaborate.
Governance	A system of rules, practices, and processes used to direct and manage an *ecosystem*. The four pillars of good governance are transparency, fairness, accountability, and security.
Individual	A natural, living human being.
Interoperability	The ability of different systems to work in conjunction with each other and for devices, applications or products to connect and communicate in a coordinated way, without effort from the person. In this paper we use the Levels of Conceptual Interoperability Model (Tolk, 2010) with high-level classifications of technical, semantic and organisational interoperability.
Operator	The *role* responsible for operating infrastructure and providing tools for the *person* in a human-centric system of personal data exchange. Operators enable people securely to access, manage, and use personal data about themselves as well as to control the flow of personal data within and between *data sources* and *data using services*.
Operator network	A group of *operators* with some degree of mutual *interoperability*.
Person	The *role* of data subject as represented digitally in the *ecosystem*. Persons manage the use of personal data about themselves, for their own purposes, and maintain relationships with other roles.
Proto-operator	A product, service, or organisation that is in one way or another performing the *role* of an *operator* in personal data ecosystems or offers related tools, services, or technologies. Proto-operators come in many forms and under many different names and may cover one of more functional elements in the MyData *operator* reference model. They constitute the first generation of real-world MyData operators.
Role	A function or set of responsibilities for a particular purpose.
Separation of concerns (SoC)	A principle by which a modular approach to the development of a system is adopted. This approach entails each section addressing a different aspect (concern) of the overarching system. In the context of SoC in the personal data ecosystem, processing, storing, aggregating, displaying, governing data are concerns that need to be managed in a modular, transparent manner. SoC enables more opportunities for module upgrade, reuse, and independent development.
Self-sovereign identity (SSI)	A model for managing digital identities in which an *individual* or *organisation* has sole ownership over the ability to control their accounts and personal data without the need for intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world.

References

Abiteboul, S., André, B. and Kaplan, D. (2015) '*Managing your digital life with a Personal information management system*', Communications of the ACM. New York, NY, USA: ACM, 58(5), pp. 32–35. Available at: https://dl.acm.org/doi/10.1145/2670528 (Accessed: 22 April 2020).

Balkin, J. M. (2016) '*Information Fiduciaries and the First Amendment*'. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2675270 (Accessed: 14 April 2020).

Ctrl-Shift (2014) *Personal Information Management Services: An analysis of an emerging market*. Ctrl-Shift. Available at: http://www.nesta.org.uk/publications/personal-information-management-services-analysis-emerging-market (Accessed: 14 April 2020).

European Commission (2016) '*An emerging offer of 'personal information management services'* – Current state of service offers and challenges, Digital Single Market'. Available at: https://ec.europa.eu/digital-single-market/en/news/emerging-offer-personal-information-management-services-current-state-service-offers-and (Accessed: 19 April 2020).

European Commission (2017) '*European Interoperability Framework – Implementation Strategy*', EC COM(2017) 134 final. Available at: https://ec.europa.eu/isa2/eif_en (Accessed: 22 April 2020).

European Commission (2019) '*General Data Protection Regulation: one year on, European Commission*'. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610 (Accessed: 14 April 2020).

European Commission (2020) '*European Data Strategy*'. European Commission. Available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf.

Haaker, T., Faber, E. and Bouwman, H. (2006) '*Balancing customer and network value in business models for mobile services*'. Available at: https://doi.org/10.1504/IJMC.2006.010360 (Accessed: 21 April 2020).

Hafen, E. (2019) '*Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health*', in Krutzinna, J. and Floridi, L. (eds) The Ethics of Medical Data Donation. Cham (CH): Springer. Available at: https://link.springer.com/chapter/10.1007/978-3-030-04363-6_9 (Accessed: 18 April 2020).

Hagel, J. and Singer, M. (1999) '*Unbundling the Corporation*', Harvard business review. Available at: https://hbr.org/1999/03/unbundling-the-corporation (Accessed: 14 April 2020).

Janssen, W. et al. (2019) '*Discussion Paper What is the MyData Operator?*', MyData Global. Available at: https://mydata.org/wp-content/uploads/sites/5/2019/09/Discussion-paper-MyData-operator-final.pdf. (Accessed: 18 April 2020)

Karhu, K. et al. (2020) '*Proposal of minimum interoperability mechanism for personal data*', Open & agile smart cities OASC Minimum Interoperability Mechanism (MIM). Available at: https://oasc.atlassian.net/wiki/spaces/OASCMIM/pages/30179329/MIM4%2BPersonal%2BData (Accessed: 24 April 2020).

Kuppinger, M. (2012) '*Life Management Platforms: Control and Privacy for Personal Data*', KuppingerCole. Available at: https://www.kuppingercole.com/report/advisory-lifemanagementplatforms7060813412 (Accessed: 14 April 2020).

Lanier, J. and Weyl, G. (2018) '*A Blueprint for a Better Digital Society*', Harvard Business Review, 26 September. Available at: https://hbr.org/2018/09/a-blueprint-for-a-better-digital-society (Accessed: 11 July 2019).

Lehtiniemi, T. (2017) '*Personal Data Spaces: An Intervention in Surveillance Capitalism?*', Surveillance & Society, 15(5), pp. 626–639. Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6424 (Accessed: 19 April 2020).

Makaay, E., Smedinghoff, T. and Thibeau, D. (2017) '*Trust Frameworks for Identity Systems*'. Available at: https://www.openidentityexchange.org/wp-content/uploads/2017/06/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf (Accessed: 24 April 2020).

MIC Japan (2018) '*Release of the Guidelines of Certification Schemes Concerning Functions of Information Trust ver. 1.0*', Ministry of Internal Affairs and Communication Japan. Available at: https://www.meti.go.jp/english/press/2018/0626_002.html (Accessed: 18 April 2020).

MyData Global Network (2017) '*Declaration of MyData Principles*'. MyData Global Network (before the MyData Global association was established). Available at: https://mydata.org/declaration (Accessed: 14 April 2020).

MyData Global (2019) '*What Is the MyData Operator?*', Workshop at the MyData 2019 conference. Available at: https://mydata2019.org/programme-page/what-is-the-mydata-operator (Accessed: 14 April 2020).

MyData Global (2020) '*MyData Operators thematic group*'. Available at: https://mydata.org/groups/mydata-operators (Accessed: 14 April 2020).

Obar, J. A. and Oeldorf-Hirsch, A. (2018) '*The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*'. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757465 (Accessed: 19 April 2020).

ODI (2018) '*Defining a 'data trust''*, Open Data Institute: The ODI. Available at: https://theodi.org/article/defining-a-data-trust (Accessed: 14 April 2020).

Poikola, A., Kuikkaniemi, K. and Honko, H. (2015) '*MyData – A Nordic Model for human-centered personal data management and processing.*' Ministry of Transport and Communications. Available at: http://urn.fi/URN:ISBN:978-952-243-455-5 (Accessed: 14 April 2020).

Project VRM (2008) '*Project VRM – Berkman Centre*', Harvard University. Available at: https://cyber.harvard.edu/projectvrm/Main_Page (Accessed: 20 April 2020).

Rikken, M., Janssen, W. and Duits, I. (2019) '*Het landschap van Persoonlijk Data- Management*', InnoValor. Available at: https://drive.google.com/file/d/1IZDHRkOzGGOn_CzZxQxG4dB3lk9KAGtj/view, https://innovalor.nl/digitale-wendbaarheid/persoonlijk-datamanagement (Accessed: 17 April 2020).

Sitra (2019) '*Rulebook for Fair Data Economy – Rulebook Template for Data Networks*', Sitra. Available at: https://www.sitra.fi/en/news/a-new-rule-book-sets-out-the-guidelines-for-a-fair-data-economy (Accessed: 14 April 2020).

Sitra (2020) '*IHAN Blueprint 2.5*', Sitra. Available at: https://www.sitra.fi/en/articles/ihan-blueprint (Accessed: 22 April 2020).

Tolk, A. (2010) '*Architecture constraints for Interoperability and composability in a smart grid*', Power and Energy Society General Meeting, 2010 IEEE. Available at: https://www.researchgate.net/publication/224178883_Architecture_constraints_for_Interoperability_and_composability_in_a_smart_grid (Accessed: 14 April 2020).

Wang, F. and De Filippi, P. (2020) '*Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*', Frontiers in Blockchain, 2, p. 28. Available at: https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full (Accessed: 19 April 2020).

World Economic Forum (2013) '*Unlocking the Value of Personal Data*', World Economic Forum. Available at: http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage (Accessed: 21 April 2020).

World Medical Association (2018) '*Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects*', World Medical Association. Available at: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects (Accessed: 17 April 2020).

Appendix 1 – Proto-operators studied for this paper

Name and link	Country	Description (provided by the proto-operator)
OwnYourData	Austria	OwnYourData is a non-profit association and helps you to achieve unrestricted access to your data for your benefit.
Meeco	Belgium	Meeco gives people and organisations the tools to access, control and create mutual value from personal data. Privately, securely and always with explicit consent. Meeco provides the underlying technology to enable enterprises to become MyData operators, with interoperability across their B2B, B2B2C and Me2B services, whilst always adhering to the MyData human-centric principles.
Smart Species	Canada	Governance integration, WHiSSPR Auditors, Canadian OPN:Registrar, Smart Person, Smart City, Smart Nation. Consent DDE, Data Trust Governance for distributed transparency, DLC - digital ledger consent technology provider.
Diabetes Services	Denmark	Diabetes Services provides services for better health and quality of life for people with diabetes and makes it easy to handle personal data across digital services and medical devices. The data using services are personal apps and sharing data with healthcare professionals, researchers, and others.
Peercraft	Denmark	Currently a user-centric identity provider, Peercraft is working to become a purchasing agent for consumers via a fully decentralized business and service discovery protocol (opendiscovery.biz)
1001 Lakes	Finland	1001 Lakes enables trusted data sharing for people and organizations to realize more value together.
City of Helsinki	Finland	Helsinki wants to be the most functional city in the world by making full use of its data. Helsinki seeks to apply MyData principles in managing the personal data it collects and processes.
Findy	Finland	The Findy consortium is working towards launching a collaboratively governed and operated public-private not-for-profit decentralised identity network.
Gravito	Finland	Gravito is a cloud-based, real-time consumer profile which follows you automatically over domains and cross organizations. It allows you to define your domain specific multi-level consents and provides means to connect your profile to the surrounding device(s) and "things". It gives organizations access to real-time consumer profiles/segments where the people are themselves communicating their preferences and consents.
Posti	Finland	We at Posti believe in a fair, responsible, and transparent digital future. Embracing technologies and solutions that thrive the development towards human-centric data economy should be the interest for every company as it is for us. Posti is the leading postal and logistics service company in Finland with over 22,000 employees. Posti manages the flow of everyday life by offering a broad range of postal, logistics, freight and e-commerce services.
Startup Commons Global	Finland	Circle Pass is a service that is part of the ecosystemOS package provided by Startup Commons Global, focused on digitally connecting, visualising and benchmarking startup ecosystems for economic development and growth of entrepreneurship and innovation.
Vastuu Group	Finland	MyDataShare is a SaaS platform for MyData Operators - managing digital IDs, personal data sharing and permissions between individuals and compatible digital services.
Cozy Cloud	France	Cozy is an open PIMS combining a Personal Data Store and a sandboxed execution platform where services can leverage data without disclosing any information.
fair&smart	France	A turnkey Human-centric platform for the governance of personal data, allowing transparent, secure and GDPR compliant free flow of data. It features PDS (myfairdata), encrypted data transfers and permission management.

Onecub	France	Onecub is a portability tool based on consent. Onecub is an all-in-one tool (technical, legal and design).
Visions	France	Visions is a digital agent at the service of the individual, control your data and live your digital life on your terms. Visions starts by empowering people with their skills in a lifelong learning perspective, finding the right training at the right time.
comuny	Germany	With comuny, everyone in the digital world protects their identity and shares data self-determined.
esatus	Germany	esatus AG is a medium-sized German information security consultancy that wants to enforce Self-Sovereign Identity for everyone and everywhere.
Polypoly	Germany	Polypoly is a project of joint European interest. We're building a digital ecosystem that gives each individual sovereignty over their personal data, and creates a fair data market for companies where the customer is an equal partner.
DataSign	Japan	Operating the first certified Information Bank (Trusted Personal Data Management Service) in Japan that is called "paspit".
NTT DATA Corporation	Japan	We will provide a new infrastructure which is the platform for PDS platformers in various fields to realize a rich life for people in the digital age.
Personium	Japan	An open source interconnectable PDS server software project envisioning the Web of MyData. The project is mainly led and supported by Fujitsu, ltd.
Younode	Japan	Decentralized personal data sore which can work as a password manager also. Users can store it on their own device or Google Drive that you can manage.
Financieel Paspoort	Nether-lands	The Foundation Financieel Paspoort aims to improve the financial awareness and independence of all citizens. We develop digital tools that will enable the individual to gather all personal financial information from various sources in an easy, fast and safe manner. An overview of all financial information enables the individual to assess the personal financial situation, consider measures for improvement and connect efficiently with advisors. The foundation is fully independent and is solely focussed on the interests of the individual.
Holland Health Data Co-operative	Nether-lands	HHDC empowers its members (citizens) with an ethical check on requests for use of individual health data, based on the consent structure they have specified.
IRMA	Nether-lands	The Privacy by Design Foundation creates and maintains free and open source software in which the privacy of the user is the most important. The focus is the identity platform IRMA, an acronym of I Reveal my Attributes. With IRMA you can disclose properties (attributes) of yourself in a privacy-friendly and secure way - for example, I am over 18 years old - without disclosing other, non-relevant information about yourself. Using such attributes you can authenticate yourself to for example login on a website. Additionally, with IRMA you can create attribute-based digital signatures.
Ockto	Nether-lands	Ockto is the online method of collecting data for consumers who want to close a financial product. This solution enables consumers to collect financial information about their household in a quick and simple way. This data can be shared by the consumer with the bank, mortgage provider or other financial service provider.
Qiy Foundation	Nether-lands	Co-creation with market parties of a trust-based human-centric online ecosystem with individuals as a constitutional part in control over their data.

Name and link	Country	Description (provided by the proto-operator)
Schluss	Nether-lands	With Schluss you, and only you, decide who may know what about you. Schluss allows each individual on the internet to act as an operator themselves by providing the tools for this. Schluss provides a distributed personal data vault in which all personal information can be stored. From there you are able to decide what person or organisation you grant access to, for what reason and what period. And you keep overview on that. Schluss doesn't know anything about it's customers; not even who the customers are. Techniques are divided in three layers (identification, authorization and storage) and of course Open Source. Schluss is now a foundation which also has the goal to set up a cooperative where all Schluss are co owner of the organisation.
Datafund	Slovenia	Datafund is transforming data into assets by connecting data owners with data users in a privacy centric and fair data way.
iGrant.io	Sweden	iGrant.io is a cloud based platform that uses consents (aka user permissions), among others, as the legal basis to enable data exchange across organisations based on a data regulatory compliance framework. Apart from providing tooling for user consent management and regulatory compliance, all transactions (e.g. user consents and data exchange) are fully auditable by any third party.
Healthbank cooperative	Switzer-land	The global people-owned platform for managing your health and medical data in one secure database.
MIDATA	Switzer-land	MIDATA Cooperative has established a governance model and IT platform solution for citizen-centered and patient-centered health data aggregation, allowing citizens and patients to give dynamic and granular consent to data use. The MIDATA platform embodies modern data governance principles, enabling health research and health services, while at the same time ensuring citizens' and patients' sovereignty over their personal data. The platform is based on advanced database and encryption technologies developed at ETH Zurich. Its FHIR API enables interoperability and use of structured data. The platform acts as a hub for a mobile app ecosystem. The platform and app framework are operational and being further developed in the context of the SPHN initiative and further national initiatives.
Numbers	Taiwan	Numbers provides an open-source framework to capture and record the metadata of content and allows users to verify the data integrity using simple protocol.
Consentua	United Kingdom	Consentua lets organisations orchestrate their data processing based on the consent that they have from data subjects. Consentua collects, stores and updates consent records so that business processes can be automatically started and stopped, and provides a rich audit trail of consent collection and use.
Dataswift	United Kingdom	Dataswift is a technology company that develops data portability and processing tools leveraging the Hub of All Things (HAT) personal data account, enabling individuals and businesses to implement and benefit from the ethical storage and processing of data.
DataYogi	United Kingdom	DataYogi is a service built on top of the JLINC platform that will help people control and leverage their 'buying' related data.
Digi.me	United Kingdom	Digi.me facilitates individuals to share more & better data to enable businesses to provide more & better value, with 100% privacy, full security and consent. This is implemented with the individual owning and controlling their data themselves - digi.me does not see, touch or hold user data ever. Digi.me is an in-service platform. Individuals can access their health, finance, social, wearables and media data today - and a full developer suite is available for apps to build on the digi.me platform obtaining data through consent.
Hub-of-All-Things	United Kingdom	The HAT Community Foundation is devoted to advancing the Hub-of-All-Things (HAT) open source technology, and to advancing the interests of HAT owners everywhere. It acts as regulator for the HAT ecosystem, and operates the HAT-LAB, which functions as the research and innovation centre for the HAT.
Mydex	United Kingdom	Mydex CIC provides individuals with their own uniquely encrypted personal data store enabling them to use their own data for their own purposes.

MyLife Digital	United Kingdom	MyLife Digital is primarily a consent and preference management solution. MyLife Digital has developed a solution that brings people closer to their data. We empower individuals and organisations to work in partnership to understand, control and gain mutual value from that data for positive outcomes.
Powr of You	United Kingdom	Powr of You is a consumer data hub helping people make money from their data, with actual behavior data from mobile, browsers, social, lifestyle apps.
HIE of One	United States	HIE of One Trustee is a standards-based, Free / Open Source software suite for substitutable operators with decentralized governance. We use health information exchange (HIE) as the use case.
Indie Computing	United States	Your data on hardware you control. Indie Computing provides managed appliances to enable consumers, families, and organizations to manage their valuable data in place they control.
JLINC	United States	JLINC is a protocol for permissioned data sharing that enables multiple parties to co-manage data assets in a human-centric way.
Prifina	United States	Prifina is a user-held data platform that provides tools for developers to build direct-to-consumer applications and widgets, on superior data that never leaves the individual.
Spartacus	United States	Spartacus was incorporated in 2019 as Data Fiduciary Inc. We help our customers take back their privacy and protect their data and identity.
UBDI	United States	UBDI allows individuals to securely aggregate millions of data points about themselves from their social, financial, wearable, and health accounts and get paid for their time and attention when seeing relevant ads or for sharing insights from that data for market and financial research.

Citation: Langford, J., Poikola, A., Janssen, W., Lähteenoja, V. and Rikken, M. (Eds.) (2020) *'Understanding MyData Operators'*, MyData Global.

Graphic design: Kirmo Kivelä