9

Personal Data Management and MIM4

Michael Mulquin

MIMs Ambassador, Open & Agile Smart Cities, Belgium
Email: michael@oascities.org

Abstract

The chapter starts by listing some of the many initiatives that aim to put the citizen in charge of how data about them is used. It points out that the large number of these initiatives demonstrates the importance of this issue, but also that it has resulted in a fragmented marketplace with competing technical approaches and processes.

It then describes how Open & Agile Smart Cities is working with many of these initiatives to develop a minimal interoperability mechanism on personal data management (MIM4). This will identify an agreed set of capabilities to enable the different solutions to be compared, a common legal framework that all can sign up to, and a technical requirement that will enable "good enough" interoperability between them and thus help to bring consistency into the marketplace.

9.1 The Fragmented Marketplace

We have already seen how one of the key challenges in today's world is putting the citizen back in control of their data. There are many initiatives that are working hard to tackle this issue. Solid and MyData have already been mentioned elsewhere. Others include the following.

- A NewGovernance (aNG):[1] An association promoting and enabling human-centric personal data sharing. The aim is to support and

[1] https://www.anewgovernance.org/

coordinate the many personal data sharing ecosystems that are being developed by developing standards and a governance framework. It has a strong European base but is firmly global in vision.

- Disposable identities:[2] This is an initiative pushing for the use of digital wallets to enable individuals to access services and take part in smart contracts without disclosing personally identifiable data.
- Privacy by design foundation:[3] It creates and maintains free and open-source software in which the privacy of the user is the most important. The most important application of the foundation is the identity platform IRMA, an acronym of I Reveal My Attributes. The foundation also aims to generally improve the development and usage of open, privacy-friendly, and well secured ICT.

There are also several European Projects such as DataVaults[4] and KRAKEN,[5] along with a number of other initiatives, which are each developing their own technical solutions to provide personal data management solutions and are primarily in the pilot or development phase. The aims of the different initiatives overlap but are not necessarily identical. Some projects focus just on personal data management, and others, such as Rennes Urban Data Interface (RUDI),[6] aim to support wider data sharing ecosystems but with personal data management being a key feature.

The large number of agencies and projects working in this area demonstrates the importance of the issue. However, it has led to a fragmented marketplace, with many different technical solutions and business models.

MIM4 aims to tackle this issue by identifying the key capabilities required and developing points of interoperability between the different solutions to help build confidence and support implementation.

9.2 MIM4

MIM4 focuses on personal data management (PDM), in other words, how to provide easy to use methods for citizens/users to control which datasets/attributes they want to share with solution, application, or service

[2] https://disposableidentities.eu/

[3] https://privacybydesign.foundation/en/

[4] https://www.datavaults.eu/

[5] https://www.krakenh2020.eu/the_project/overview

[6] https://uia-initiative.eu/en/uia-cities/rennes-metropole

providers under transparent circumstances, enabling trust between the different parties.

Specifically, it will provide technical and other guidance to support cities and communities to put in place the products and services that will enable their citizens to be in control of their personal data within the local data ecosystem. It will do this in a way that will make it easy for them to integrate their services with whatever credible personal data management systems their citizens may wish to use.

MIM4 will define:

1. the capabilities that cities and communities need to put in place to enable citizens to have control of their data within the local data ecosystem;
2. the requirements to enable "good enough" interoperability between existing services and projects that offer solutions for personal data management.

The work will include reviewing how MIM4 can be integrated with the other MIMs to support the effective personal data management within a local data ecosystem.

MIM4 will also point to sets of recommended solutions that will enable cities and communities to comply with these requirements.

9.2.1 Capabilities

MIM4 will address needs and requirements from two perspectives:

- that of individual citizens in terms of transparency and privacy preferences collection;
- cities and data using services (data controller/processors) in terms of authorisation and data usage control and enforcement.

The provisional sets of capabilities identified so far are listed below.

For individual citizens:

1. Citizens need to be able to choose the operator they wish to manage their data and to move from operator to operator.
2. Citizens should be able to access their data through many different channels.
3. Citizens should be able to use the identity of their choosing, in best cases a keychain of identities can be defined, so that users can choose the identity per service.

4. Citizens should have insight into what personal data is available, stored, shared, etc., by the providers of the applications and/or services they use.
5. Citizens should be able to request changes to or deletion of part or all personal data available, stored, shared, etc., by the provider of the applications and/or services in use. The providers would need to comply with these requests unless there were legally justifiable reasons not to do so.[7]
6. Citizens should be able to indicate in which circumstances what personal data is "free" to use for which parties through a "permission arrangement".
7. Citizens should be able to grant consent to providers of the applications and/or services, be it governmental or businesses, that attribute-based, decentralised storage, and "revealing" of personal data attributes provides full service and access to these applications and/or services.
8. Citizens should be able to roam with their data between cities and internationally.

For cities and data using services:

1. Cities need to enable users to handle consent, allow and revoke access, and have full transparency on their personal data.
2. Permission management needs to be handled preferably on the attribute level. Personal data processing should be described in a fine-grained manner, by covering all aspects (purposes, processing, types of data, etc.) in a standardised manner (see, for example, W3C Data Privacy Vocabulary[8]).
3. Personal data management needs to have an open API in line with MIM1 to broker data and standard data models MIM2. Data sources need to be open and documented, and discoverable via MIM1, listing their data via MIM2. Operators may benefit from being groupable at joint initiative of cities with close ties.

[7] For instance, the citizen cannot expect information regarding their age or any other key factual piece of information to be changed so as to be incorrect, specifically in a way that will affect their eligibility for services.

[8] https://dpvcg.github.io/dpv/

4. PDM systems need to manage the personal data to a high level of security (the detail of how to do this will be dealt with by MIM6).
5. PDM systems need to be flexible enough to handle methodologies that require personal data pods to store the data as well as those that utilise personal data spaces or that allow the data to continue to be stored by the relevant organisation, but where the subject of the data is able to exercise rights as to its use.

This list of capabilities will be tested with the various projects and initiatives working in the field to develop a consensus-based set that can be used to review and compare different initiatives that aim to enable personal data management.

9.2.2 Requirements

A detailed proposal for interoperability between personal data management operators has been reviewed in detail by MyData Global, Vastuu Group, Forum Virium Helsinki, RUDI (the Urban Data Initiative of the city of Rennes), the DataVaults, DataPorts and KRAKEN European Projects focusing on personal data management, and the CAPE personal data management solution developed by the engineering group.

This proposal has two pillars:

- Pillar 1: One connector for all personal data management operators.
- Pillar 2: Legal framework governance.

The proposal is described in the paper "Towards Interoperable Personal Data Management within Smart Cities: Minimum Interoperability Mechanism 4" that can be accessed at: https://mims.oascities.org/mims/oasc-mim4-trust/references

Effectively, this defines a connector that enables any personal data management provider that complies with the legal agreement to be able to access data from any data source that is MIM4 compliant. In this way, each personal data management provider can innovate freely around their technical solution, provided that it enables the capabilities defined in MIM4, while data providers only need to provide a single method for them to access the data.

This review indicated that the proposed interoperability mechanism is a feasible way of enabling a level of interoperability between all of these and is likely to be relevant to all personal data management solutions. All the above initiatives have also agreed to work together over to develop demos to test the

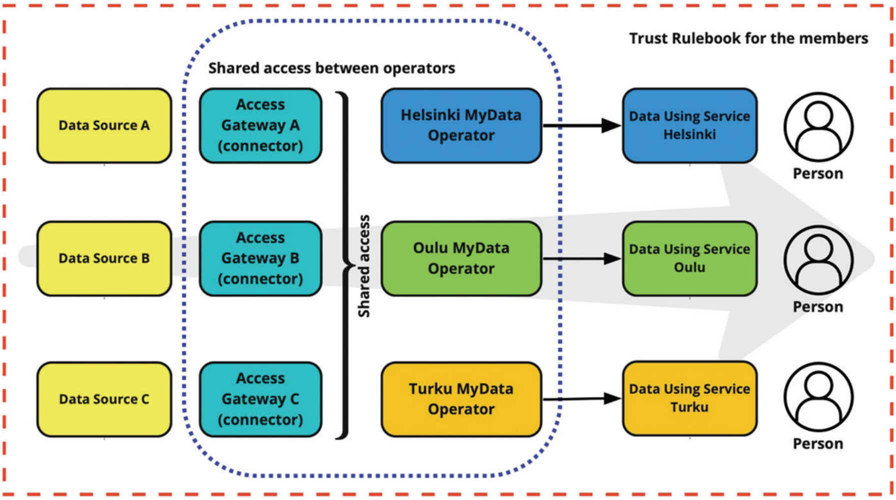

Figure 9.1 Shared access.

technical suitability of this solution in practice. In addition, the Flanders Data Utility Company[9] that is implementing a Solid-based approach to enabling the citizens of Flanders to manage their personal data has agreed to join the testing programme.

The organisations taking part will also review the proposed legal agreement to ensure that it is practical and covers all the key issues.

9.3 The Link with National ID/Citizen Cards

Within Europe, the planned European Digital Identity Framework being developed under eIDAS will make it possible for every person eligible for a Member State national ID card to have a digital identity that is recognised anywhere in the EU. It will provide a simple and safe way to control how much information an individual wants to share with services that require sharing of information. It will operate via the use of digital wallets available on mobile phone apps and other devices to:

- identify the citizen both online and offline;
- store and exchange information provided by governments, e.g., name, surname, date of birth, and nationality;

[9] https://www.vlaanderen.be/digitaal-vlaanderen/het-vlaams-datanutsbedrijf/the-flemish-data-utility-company

- store and exchange any other information provided by trusted private sources;
- use that information to demonstrate the right of the individual to access services.

Specifically, for Europe, the development of the European Digital Identify Framework and Digital Wallet will have a significant impact when it is launched in the next two to three years and the MIMs Plus version of MIM4 will need to take that into consideration.

More widely, the European Digital Identity Framework not only builds on multi-purpose National Identity Cards within member states, for instance Estonia, but on the work many cities around the world are doing to develop citizen cards to help citizens access local services. It is also worth noting the White Label citizen card solution being developed by Eurocities. These citizen cards may be provided using a dedicated smart card or via a smartphone app.

MIM4 will be developed in a way that will align with these initiatives.