Privacy, security and Trust for Digital living

City x City Festival

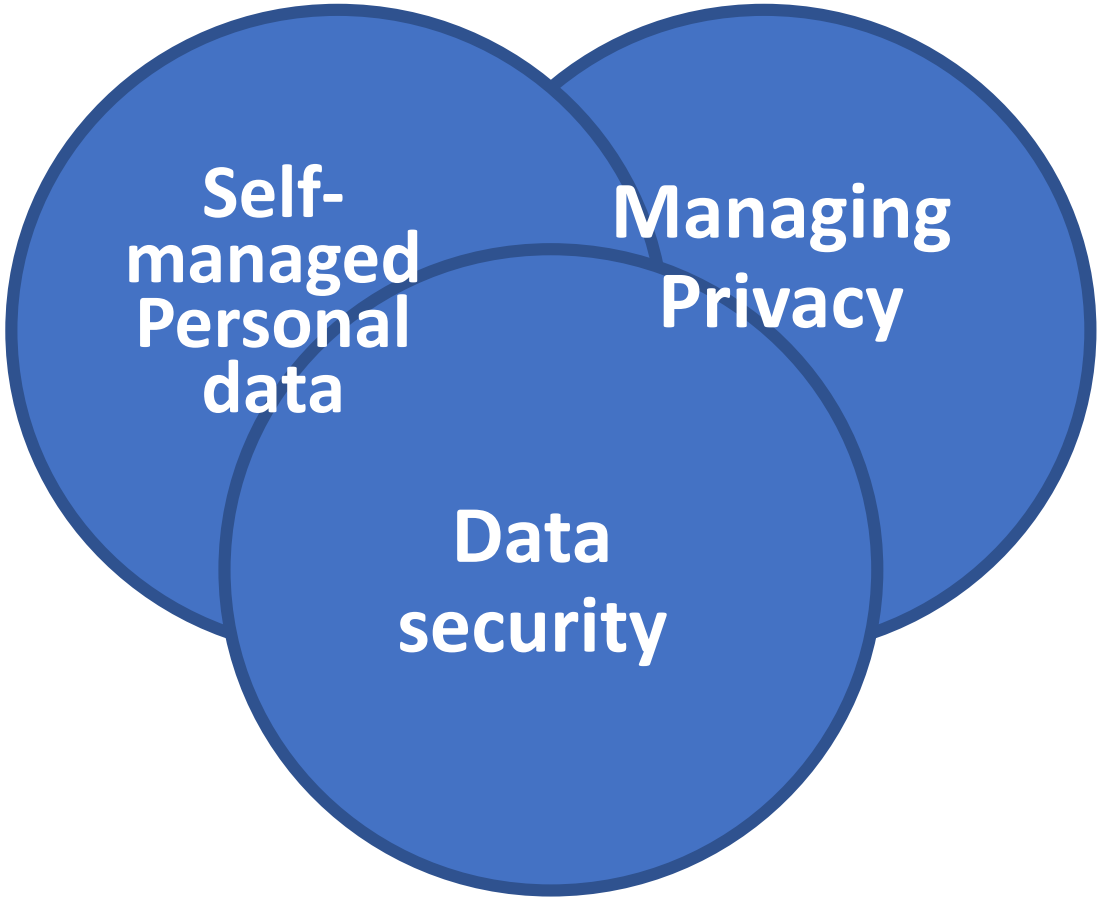
Michael Mulquin OASC

Privacy and Trust

There are two aspects to Privacy, both of which are important.

1. One is how organizations (whether public or private) can manage personal data in a way that protects individual privacy and is compliant with regulations such as GDPR.
2. The second aspect, which is the focus of MIM4, is about personal data management - putting citizens in control of their personal data. By enabling citizens to manage their own data they are able to trust that their privacy is being maintained

Three key interlocking issues



Managing Personal data - MIM4

How can individuals give permission for who has access to their data, so that they always remain in control?

How can they enable applications to access the relevant attributes about them to make the right decisions about their eligibility for benefits or the most appropriate treatment for any health conditions, while avoiding the need to link that data with their personal identity?

There are many initiatives

Two major networks:

- MyData https://mydata.org/
- SOLID https://solidproject.org/

Many other initiatives:

- RUDI – Rennes Urban Data Interface https://uia-initiative.eu/en/uia-cities/rennes-metropole
- IRMA and Privacy by Design Foundation https://privacybydesign.foundation/en/
- DataVaults Horizon Project https://www.datavaults.eu/
- Kraken Project https://www.krakenh2020.eu/the_project/overview
- Japanese Information banks

Also relevant are Citizen Cards and national and European ID cards as well as the coming European Digital Identity Framework

The key barrier for Personal data management – business model

Our personal data is already owned by Google, Facebook, Amazon, Baidu, …

This cannot be easily challenged, especially within a fragmented marketplace

Local community managed data ecosystems are a good place to start, by enabling management of data held by local service providers

And helping to align the existing initiatives so that they together form a viable offering – MIM4

Managing privacy - MIM?

How can datasets that include personal data be anonymised to provide useful information about service effectiveness, without enabling an unauthorised person to access personal sensitive information, particularly when the linking of several anonymised datasets might allow personal data to be inferred?

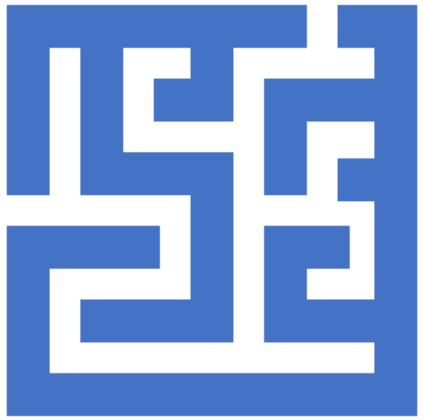
One of the main standards bodies working in this area is ISO/IEC JTC1 Sub Committee 27 *Information security, cybersecurity and privacy protection*

This is a key issue for data ecosystems

- It is challenging enough for an organisation to ensure that it manages personal data to ensure privacy within its own data store
- It is a much greater concern to provide personal data within a local data ecosystem or data space if we cannot know who else might use our data and what other data sets they might combine it with – what are our legal liabilities?
- It is vital to have appropriate terms and conditions, including covering legal liability/effective penalties, for use of data in general and personal data in particular for a local data space and to make sure that compliance is managed effectively

Open energy (UK)

Description	Example Datasets	Personal Sensitivity	Commercial Sensitivity	Security Sensitivity
Datasets which include personal data, requiring appropriate consent to share, or other legal bases to data processing, as defined by the EU GDPR and brought into UK law via the DPA 2018. Currently not suitable to share within the OE ecosystem, with future extensibility subject to consultation.	Smart meter data, home temperature preferences, protected characteristics or special category data (e.g. dependence on power due to health conditions), individual EV charging records, transaction data.	Very High	Medium/ High	Medium/ High



- For data to be used in the data ecosystem, it may often need to go through a complex path between where it is generated and where it is finally used.
- At every stage in that process, it is vulnerable to attack and proper systems need to be put in place to address this.

One of the main standards bodies working in this area is ISO/IEC JTC1 Sub Committee 27 *Information security, cybersecurity and privacy protection*

Data security – MIM6

Tackling these issues will have wider benefits

Getting terms and conditions right in the local data ecosystem

Managing business sensitive information

Building trust in the local administration and its partners