Issue 3 | 2020

TECH DISPATCH

# Personal Information Management Systems

Personal Information Management Systems (PIMS) are new products and services that help individuals to have more control over their personal data. PIMS enable individuals themselves to manage and control their online identity.

## I. What are Personal Information Management Systems?

The PIMS concept offers a new approach in which individuals are the 'holders' of their own personal information. PIMS allow individuals to manage their personal data in secure, local or online storage systems and share them when and with whom they choose. Individuals would be able to decide what services can use their data, and what third parties can share them. This allows for a **human centric approach to personal data** and to **new business models**, protecting against unlawful tracking and profiling techniques that aim at circumventing key data protection principles.

There is a growing interest in our 'digital societies' in how individuals can better control their personal data. A Eurobarometer survey from March 2019 revealed that half of the respondents (51%) felt only in partial control over the information they provided online, while 30% believed that they had no control at all. Only 14% of the respondents thought they were in complete control. A US survey from 2019 even showed 80% of respondents feeling they were not in control of their personal data.

In the European Union, Article 8 of the EU Charter enshrines the **protection of personal data as a fundamental right for every** person and the EU General Data Protection Regulation (GDPR) aims to empower individuals to be in control of their data. For this purpose, practical and effective tools and services are needed.

Personal data is constantly collected in the digital environment, leading to individuals leaving **digital footprints.** The GDPR provides for several data subject rights, such as the right to access and rectification of personal data. The current architecture of information society services makes it however challenging for individuals to have full control of how their data are used, who should have access to them and how to provide effective restrictions and objections to data processing.

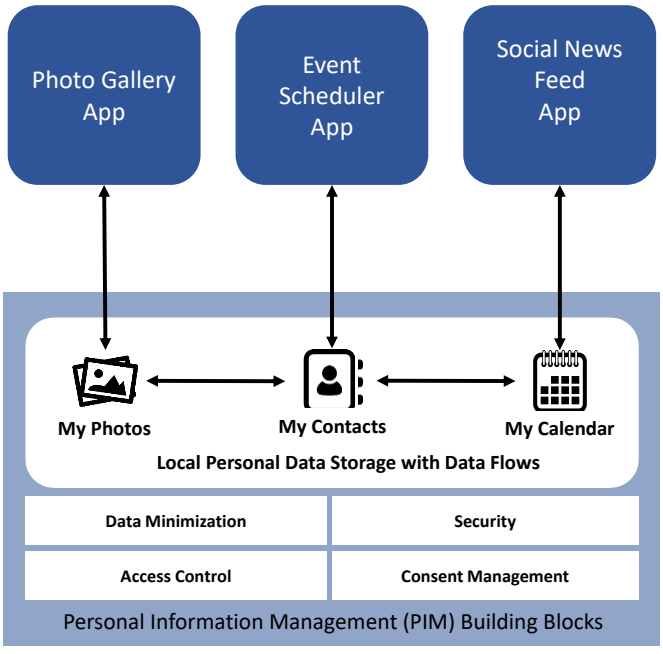


Figure 1: A simple schema for a Personal Information Management System with a local personal data storage.

A basic feature of a common concept of PIMS (see Figure 1) is providing **access control and an access trail**. Individuals, service providers and applications would need to authenticate to access a personal storage centre. This enables individuals to track back who has had access to their digital behaviour. Individuals are able to customize what categories of data they want to share and with whom. Other usually common elements of PIMS are secure data storage, secure data transfers (transporting data safely between systems and applications) and data-level interoperability and data portability.

There are several examples of initiatives and projects claiming PIMS features. They include: **Nextcloud** enables individuals and organisations to use their own cloud services for file sharing and collaboration services, as well as sharing files across different Nextcloud servers. People can install the free and open source software themselves or receive the software as a service (SaaS) from professional providers. Many universities, governments and companies already employ Nextcloud.

**Solid** is a 'proposed set of conventions and tools for building decentralised social applications'. Data such as contacts, calendars and photos may be stored in a so-called *personal online datastore* (POD). These data can be accessed by compatible apps. Users are allowed a continuous experience across apps within the ecosystem, keeping the data within their pods without unnecessarily replicating them.

**MyDex** is a UK-based Community Interest Company providing a portable, interoperable online identifier. Users can access a particular service online through a secure personal store, where all personal 'verified' records are managed. They can be securely accessed by other applications using Application Programming Interfaces (APIs). It provides the ability to grant and revoke access permissions on a general or ad-hoc basis.

**MyData** is a non-profit association teaming up initiatives around the world to 'empower individuals by improving their right to self-determination regarding their personal data'. MyData claims to combine industry needs for data access with digital human rights, through promoting open standards and sharing the same set of principles, for a 'shift from data protection to data empowerment'.

# II. What are the data protection issues?

## II.1. Individual empowerment plus Data protection by design and by default

When correctly designed, PIMS could help data controllers to implement the obligations of **privacy and data protection by design and by default** and to support them to demonstrate compliance with the GDPR. If however these tools or systems fail to be properly designed, for example, there is a **risk** that data subjects will not be empowered to manage their own digital identity, but will instead unwittingly find themselves on a **path of being determined by others** or **which result in data subjects taking decisions contrary to their own interests under the influence of these tools/system.**

## II.2. Consent management

PIMS deliver their full potential when they rely on users' consent. **Individuals would keep full control** and would be free to share their personal data according to their own preference and delete them whenever they want. In some circumstances however, the law decides how data should be processed (e.g. storing tax declarations for some years). Control in such cases would achieve transparency in the way personal data are processed, and being able to verify their accuracy, retention time etc.

A basic feature for PIMS is managing the use and sharing preferences of an individual's personal data such as photos, videos, contact lists, and even geolocation. For each category of personal data, individuals should be able to decide what services can use them, for what purposes and with whom they can share them. When consent is withdrawn, advanced PIMS might provide reliable evidence that a service no longer uses one's data.

## II.3. Transparency and traceability

Online service providers often collect users' personal data in exchange for allegedly 'free' services. The data subject is often faced with a 'take it or leave it' approach, with little or no transparency for the individuals on how his or her personal data is handled. PIMS would allow for transparency both at the level of shared policies and by technical design, disclosing what services are processing which data for what

specific purposes. Information can be given in real time. **Personal data dashboards** can help individuals to follow their data and their processing.

The use of PIMS can also support eGovernment services providing advantages such as greater traceability and transparency on which public administration has access to what personal data.

### II.4. Exercise of individual's rights of access, to rectification and erasure or 'right to be forgotten'

PIMS provide features for individuals to be able to access their personal data, as well as to rectify or erase them, as provided for by the GDPR, either because the data are in repositories under their direct control or because all shared data are linked to a source, which is again in the control of the individual.

**Data accuracy** In PIMS, individuals are responsible for the data they provide. At the same time, when other organisations are accountable for personal data (e.g. banks, utility providers), certain PIMS can provide proof of origin/validity from those organisations, thus granting the necessary level of reliability. Greater data accuracy is a benefit also to those third parties that have an interest in accessing the data, thus enabling synergies between individuals and organisations.

**Data portability and interoperability** PIMS can usually offer personal data and other metadata describing their properties in **machine readable formats**, as well as programming interfaces (APIs) for data access and processing. This last feature implies the use of **standard policies and system protocols.** This is an essential element, the lack thereof currently also represents a limit for PIMS adoption.

**Data security** PIMS must also ensure the security of personal data at rest and in transit from unauthorised or accidental access or modification. In order to be fully implemented, PIMS should be able to rely on **Privacy Enhancing Technologies (PETs)**, a wide range of techniques that include trusted execution environments, homomorphic encryption, secure multi-party computation and differential privacy. Data minimisation and anonymisation services should also be provided. One feature of many PETs is the use of cryptography.

Cryptographic features may be used to verify the authenticity of data and to implement users' privacy preferences such as authorised purposes and permitted retention periods against service providers and third parties. A common use of cryptography is **data encryption**, which supports confidentiality and integrity of communications, databases and other repositories. Current cryptographic researches are developing ways to allow for calculations without decrypting the data. This would mitigate risks of unauthorised access or disclosure. Cryptography also provides mathematical evidence that data and communications come from a certain source as well as proof that an entity (for example a service, an organisation, or an individual) is authorised to access categories of (personal) data for certain purposes or perform any other actions on those data, even on a granular basis. Data would then be disclosed only to those services bearing that cryptographic evidence.

Finally, it supports **data minimisation** techniques (e.g. attribute-based credentials), to ensure that third parties can access only necessary pieces of information, thus avoiding the disclosure of the full identity of the individual.

Currently, a big challenge for PIMS is the low market application of these technologies, in a digital world dominated by a few big tech companies that are making use of the current online tracking models. This situation so far prevents the growth of PIMS and consequently their adoption. If adopted, the EU Commission's **Data Governance Act** would provide conditions for intermediation services between data subjects that seek to make their personal data available and potential data users, including making available the technical or other means to enable such services, in the exercise of the rights provided in the GDPR.

## III. Recommended Reading


ENISA (2017). *Privacy and Security in Personal Data Clouds*.

Eurobarometer (2019a). *Survey 487a. General Data Protection Regulation*.

– (2019b). *Survey 487b. Charter of Fundamental Rights*.

European Commission (2019). *Take control of your virtual identity*.

European Data Protection Supervisor (2016). *Opinion on Personal Information Management*.
– (2018). *Preliminary Opinion on privacy by design*.
German Federal Government's Data Ethics Commission ('Datenethikkommission') (2019). *Opinion of the Data Ethics Commission*.
International Association of Privacy Professionals (2019). *Personal information management systems: A new era for individual privacy?*
Linked Data (2020). *Linked Data - Connect Distributed Data across the Web*.
Royal Society (2019). *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*.
Verborgh, Ruben (2017). *Paradigm shifts for the decentralized web*.
Verbraucherzentrale Bundesverband (2020). *Neue Datenintermediäre – Anforderungen des vzbv an 'Personal Information Management Systems' (PIMS) und Datentreuhänder*. German.

This publication is a brief report produced by the Technology and Privacy Unit of the European Data Protection Supervisor (EDPS). It aims to provide a factual description of an emerging technology and discuss its possible impacts on privacy and the protection of personal data. The contents of this publication do not imply a policy position of the EDPS.

Issue Author: Massimo ATTORESI, Thiago MORAES
Editor: Thomas ZERDICK
Contact: techdispatch@edps.europa.eu

To subscribe or unsubscribe to the EDPS TechDispatch publications, please send a mail to techdispatch@edps.europa.eu. The data protection notice is online on the EDPS website.



ISSN 2599-932X
HTML: ISBN 978-92-9242-433-6
QT-AD-20-003-EN-Q
https://data.europa.eu/doi/10.2804/096824
PDF: ISBN 978-92-9242-434-3
QT-AD-20-003-EN-N
https://data.europa.eu/doi/10.2804/11274