Project: 101094364 — ITHACA — HORIZON-CL2-2022-DEMOCRACY-01
EUROPEAN RESEARCH EXECUTIVE AGENCY (REA)
REA.C – Future Society
C.1 – Inclusive Society

ITHACA
AI To Enhance Civic Participation

ITHACA

artificial Intelligence To enHAnce Civic pArticipation

Deliverable D1.2: Overview of Personal Information Management Systems

Work Package:	WP1 – State of the art and conceptualization
Authors:	Alexander Nussbaumer, Gunnar Binda, Erich Weichselgartner, Michael Bedek, Maria Zangl, Dietrich Albert (UniGraz), Georgia Papaioannou (KT)
Contributors:	UniGraz, KT, SnP
Status:	Final
Due Date:	30/9/2023
Version:	1.0
Submission Date:	29/9/2023
Dissemination Level:	PU - Public*

Disclaimer:

This document is issued within the frame and for the purpose of the ITHACA project. This project has received funding from the European Union's Horizon Europe Framework Programme under Grant Agreement No. 101094364. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

This document and its content are the property of the ITHACA Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or licence on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the ITHACA Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the ITHACA Partners. Each ITHACA Partner may use this document in conformity with the ITHACA Consortium Grant Agreement provisions.

(*) Dissemination level: Public — fully open (automatically posted online); Sensitive — limited under the conditions of the Grant Agreement; EU classified — RESTREINT-UE/EU-RESTRICTED; CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444

ITHACA Project Profile

Grant Agreement No:	101094364
Acronym::	ITHACA
Title::	artificial Intelligence To enHAnce Civic pArticipation
URL:	www.ithaca-project.eu
Start Date	01/01/2023
Duration:	36 months

Partners

Short Name	Legal Name	Country
KT	KONNEKT ABLE TECHNOLOGIES LIMITED	IE
CERTH	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	EL
UPAT	PANEPISTIMIO PATRON	EL
RtF	RAISING THE FLOOR	BE
SnP	STAMADIANOS KAI SYNETAIROI DIKIGORIKI ETAIREIA	EL
UniGraz	UNIVERSITAET GRAZ	AT
MNLT	MNLT INNOVATIONS IKE	EL
SIMAVI	SOFTWARE IMAGINATION & VISION SRL	RO
PEDAL	PEDAL CONSULTING SRO	SK
BMA	AGENTIA METROPOLITANA PENTRU DEZVOLTARE DURABILA BRASOV ASOCIATIA	RO
MARTIN	MESTO MARTIN	SK

Document History

Version	Date	Author (Partner)	Remark/Changes
0.1	07/03/2023	Alexander Nussbaumer, Gunnar Binda (UniGraz)	Initial structure
0.2	15/06/2023	Gunnar Binda (UniGraz)	Initial content of PIMS
0.3	04/07/2023	Alexander Nussbaumer, Gunnar Binda (UniGraz)	PIMS Overview
0.4	29/07/2023	Alexander Nussbaumer, Gunnar Binda, Erich Weichselgartner (UniGraz)	Relation for ITHACA
0.5	08/09/2023	Alexander Nussbaumer, Gunnar Binda, Erich Weichselgartner, Michael Bedek, Maria Zangl (UniGraz)	Refinements
0.6	15/09/2023	Alexander Nussbaumer, Erich Weichselgartner (UniGraz)	Draft version
0.7	24/09/2023	Georgia Papaioannou (KT), Team SnP	GDPR updates and refinements
1.0	28/09/2023	Alexander Nussbaumer (UniGraz)	Final version

Table of Contents

Executive Summary

This deliverable provides an overview of Personal Information Management Systems (PIMS). This type of system aims to allow individuals to manage their personal data in secure storage systems and share them when and with whom they choose. Storage and sharing needs to adhere to legal and ethical standards, such as the General Data Protection Regulation (GDPR) and all applicable privacy and transparency principles. According to the description of Task 1.6, this overview includes (a) existing initiatives and projects claiming PIMS features, (b) elements of architecture, records, and checklists required for the implementation, (c) safeguards for compliance with the GDPR, and (d) user interfaces of such systems. This elaboration and overview should serve as a guideline for the design and implementation of the ITHACA platform. Task 3.10 will take up these considerations along with user requirements elaborated in Work package 2, in order to design and develop a PIMS for ITHACA.

Following the task description, this document presents an overview to PIMS, lists several current systems and projects, and outlines requirements of the PIMS design in ITHACA. First, a general introduction to PIMS and requirements is given that includes a definition of PIMS, a schematic architecture, and basic requirements. Then, existing systems, projects, and initiatives are presented that implement PIMS features. This list consists of NextCloud, Solid, MyDex, Mydata, PIMCity, CONSUL DEMOCRACY, and the Better Reykjavik platform. Based on these systems and the general requirements, key PIMS concepts are extracted and technical and human-centred requirements for the design of the PIMS component in ITHACA are presented, such as data security, interoperability, transparency, consent management, and accessibility. Furthermore, an overview of personal information is given that might be relevant in the context of ITHACA, and a co-creation concept is advocated on how to integrate user requirements in future work. Finally, conclusions for the design of the ITHACA platform are derived from these considerations.

List of Figures

List of Tables

List of Abbreviations

Abbreviation / Acronym	Description
AI	Artificial Intelligence
API	Application Programming Interface
EEA	European Economic Area
GDPR	General Data Protection Regulation
ITHACA	artificial Intelligence To enHAnce Civic pArticipation
PDK	PIMS Development Kit
PIMS	Personal Information Management Systems
PSK	PIMCity Stakeholders
SaaS	Software as a Service
Solid	Social Linked Data

1. Introduction

1.1 Purpose and scope

This deliverable provides an overview of Personal Information Management Systems (PIMS). This type of system aims to allow individuals to manage their personal data in secure storage systems and share them when and with whom they choose. According to the description of Task 1.6, this overview includes (a) existing initiatives and projects claiming PIMS features, (b) elements of architecture, records, and checklists required for the implementation, (c) safeguards for compliance with the General Data Protection Regulation (GDPR), and (d) user interfaces of such systems. This elaboration and overview should serve as a guideline for the design and implementation of the ITHACA platform.

The main purpose of this deliverable is to provide information of existing PIMS for the development of PIMS in Work package 3. According to the task description Task 3.10 will make use of best practices of PIMS identified in T6.1 as well as user requirements gathered in WP2. The development of a PIMS in T3.10 (a) will support data protection principles, (b) will enable users to define how their personal information should be used and for what purpose, and (c) will enable users to keep track of the way this information is used so as to be sure that it is not processed in a way not permitted by them. This will ensure comprehensive consent management functionality enabling users to also withdraw their consent when desired and a user-friendly control dashboard to be provided for this purpose.

Following these task descriptions, this deliverable will provide a general introduction to PIMS including their system architecture concepts and key features related to personal data and data protection. Furthermore, existing PIMS are listed and shortly described, in order to provide a reference for the development. Finally, considerations for the PIMS development in the context of ITHACA are given at the end of the deliverable taking into account the requirements for ITHACA and existing PIMS.

1.2. Intended audience

The main goal of this deliverable is to guide the design and development of the ITHACA platform and specifically the PIMS development conducted in T3.10. Thus, the primary audience consists of the researchers, designers and developers of the ITHACA platform. They are provided with general information of PIMS, a list and short description of existing tools, building blocks of the software architecture, key concepts and features related to legal and ethical aspects, and examples of user interfaces.

The second type of audience are the end users with a focus on vulnerable groups and their needs. This indirect audience will benefit from the elaboration of this deliverable, as it provides information on how to secure personal data, make personal data transparent, and provide support for informed decisions, all in alignment with the 'Privacy by Design' and 'Privacy by Default' principles outlined in Article 25 of the GDPR.

.

1.3 Structure of the document

The document is structured in the following way. First, a general overview of PIMS is given in the next section, which includes a definition, the general approach, and basic requirements of general PIMS. Section 3 provides a list of existing systems, projects, and initiatives that deal with PIMS. Conclusions and requirements derived from existing systems and PIMS concepts that are relevant for the development of the ITHACA platform are presented in Section 4. Finally, a summary and future work is given in the last section.

2. PIMS definition and concept

This section gives a general overview of PIM systems, which consists of recent definitions of PIMS, a description of the overall concept, and requirements derived from the definitions and concepts.

2.1 Introduction

Traditionally, two decades ago PIMS research addressed the efficiency and productivity of the workflow in private and professional context. Concepts, approaches, and software tools have been created that aimed to support individuals to manage their data. Approaches have been elaborated that help people to find previously stored information again, recall it when needed, and use it effectively in the next interaction with the item (e.g. Bergman, Beyth-Marom, & Nachmias, 2003).

More recently, PIMS research deals with storing and sharing of personal data and focuses on legal and ethical aspects, such as privacy and transparency (e.g. Jansen & Singh, 2022). A key question is how to assure the control and sovereignty of the users concerning their personal data. The work and PIMS overview provided in this deliverable refer to the concepts and approaches of the recent PIMS research, and do not take into account workflow efficiency that has been the research topic in older PIMS research.

2.2 Definition

The European Data Protection Supervisor appointed by the European Parliament and the Council provides a definition that focuses on the secure management and sharing of personal data (European Data Protection Supervisor, 2023a):

> "Personal Information Management Systems (or PIMS) are systems that help give individuals more control over their personal data. PIMS allow individuals to manage their personal data in secure, local or online storage systems and share them when and with whom they choose. Providers of online services and advertisers will need to interact with the PIMS if they plan to process individuals' data. This can enable a human centric approach to personal information and new business models."

Another event short definition is given by Jansen & Singh (2022):

> "Personal Information Management Systems (PIMS) seek to empower users by equipping them with mechanisms for mediating, monitoring and controlling how their data is accessed, used, or shared."

These definitions address the management of personal information of individuals and includes the following characteristics:

- the data can be stored in data storages in a secure way
- the data can be shared with other applications and provide interoperability for these applications
- the management of the data follows a human-centric approach

2.3 Overall concept

A TechDispatch report of the European Data Protection Supervisor (2020) provides further information on the overall concept of PIMS. It highlights that the PIMS concept offers a new approach in which individuals are the owners and managers of their personal information. The end users should be enabled to manage their personal data in a secure way in 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 which third parties can use 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.

Thus, this concept consists of two parts, a technical concept and a human-centric concept. The technical concept describes how the data is managed technically, including the storage of the data, the interoperability features to share data with third party applications, and the implementation of user-centric concepts. An overview of the technical concept is depicted in Figure 1. This diagram gives an example where photo, contacts, and calendar data in the same storage are used by different applications. Moreover, the storage (a PIMS) enables security features, consent management, access control, and data minimisation principle.

The human-centric part of the concept refers to how the user perceives key features of PIMS, such as security and access control. Access to own data must be provided in an understandable way, so that the user can understand with reasonable cognitive effort what the data are about, how they are used, by whom they are used, and how they can control the third party usage of their data.

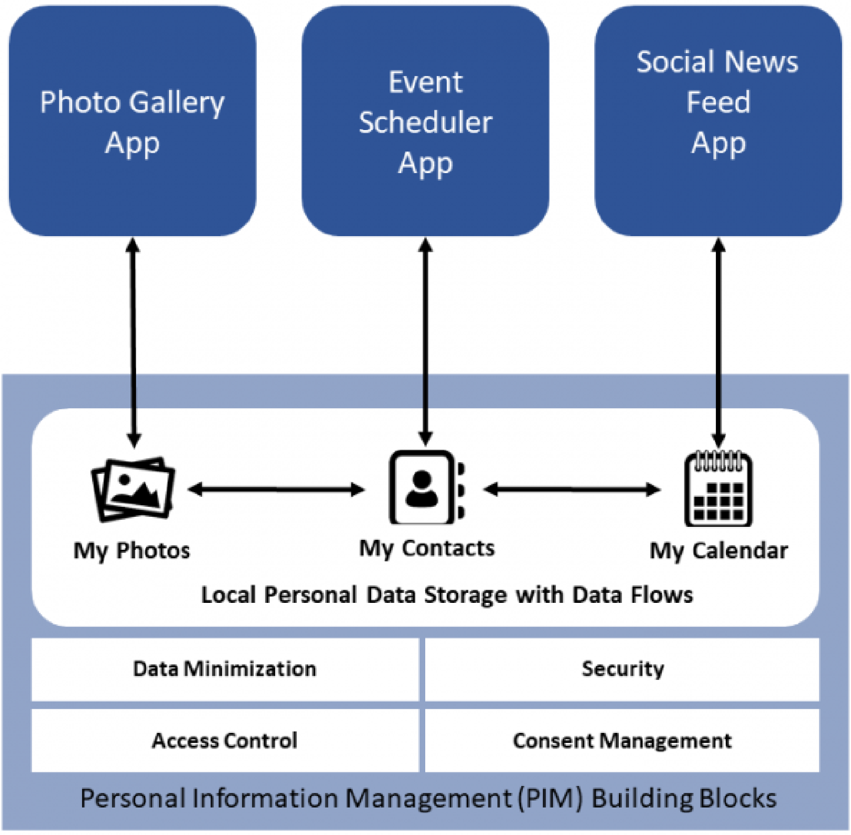


Figure 1: A simple schema for a Personal Information Management System with personal data storage. Image taken from European Data Protection Supervisor (2020).

2.4 General requirements

The main objective of PIMS is to put users in control of their personal information. In addition to serving as an effective and user-friendly mechanism to provide or withdraw consent, well-designed PIMS would also facilitate the users' rights of access to their data and their right to keep it up-to-date and accurate, thus enhancing the quality of data. From a legal point of view, this also refers to the General Data Protection Regulation (GDPR) of the European Commission (Regulation, 2016), as it enhances compliance with the requirements of informed consent (art. 7 of GDPR).

Following these considerations the following requirements of PIMS can be derived (European Data Protection Supervisor, 2020). Most of these concepts have both technical and human-centric aspects. Technical aspects relate to the implementation of the respective concept. Human-centric aspects relate to ethical, legal, and societal aspects.

2.4.1 Consent management

In the context of PIMS is consent and consent management a key concept as it involves users in the collection, storage, and processing of their personal data. Users become aware of which data is processed and for which purpose this is done, and they are empowered to understand and revoke the storage of their data. Bernemann, J., & Kneuper, R (2023) describe an approach of how the issue of granting relevant consent to the storage and use of cookies is solved with the use of PIMS. They propose to store the consent in the storage of a PIMS, where users can manage their consent. This includes, the ex-ante settings of consents, the editing and revoking of consents, the automatic creation of a report in which consent has been given.

Furthermore, Bernemann, J., & Kneuper, R (2023) also list general requirements on consents. Providing consent must be voluntary, users must be informed about the purpose of the consent, the consent must be for a specific case, and the consent must be provided explicitly and without ambiguity. Moreover, the PIMS must record all details about the consent, the duration of the consent must be provided, and the user must have the possibility to revoke the consent.

More importantly, consent management ensures compliance with GDPR by specifically addressing the following critical elements:

- Demonstration of Consent: The controller (the controlling person or organisation) is required to substantiate that the data subject has willingly consented to the processing of their personal data.
- Written Declaration: When consent is embedded within a broader written agreement, the clause seeking consent must stand out clearly from other sections. The language should be straightforward, unambiguous, and easily comprehensible. Any part of the declaration conflicting with GDPR standards will be deemed invalid.
- Right to Withdraw Consent: Individuals have the prerogative to rescind their consent at any moment. Revoking consent does not retroactively affect the legality of data processing activities conducted before the withdrawal. Individuals must be made aware of this right before offering their consent, and the withdrawal process should be as uncomplicated as the initial consent procedure.
- Assessment of Freely Given Consent: In determining the legitimacy of consent, particular attention must be paid to whether the fulfilment of a contract or the delivery of a service hinges on consent for processing non-essential personal data.

2.4.2 Transparency and traceability

Commercial online platforms often collect personal information of users as part of their business model. In their general *terms of usage* statements they require the consent of the users. Though they are subject to the GDPR and have to provide information about which data is stored, they mostly do not provide this information in a user-friendly way.

PIMS, however, should provide information about stored personal data in an understandable and comprehensive way. Comprehensiveness refers to the fact that all data should be visible to the user, including the purpose why they are stored ,which function or tool makes use of them and what is the flow of processing. Understandability refers to the method of how the information is presented. Instead of texts or lists, a graphical dashboard could be provided that can help individuals to follow their data and their processing.

Adhering to these guidelines is not merely a matter of enhancing user experience but is crucial for compliance with the transparency and liability principles outlined in GDPR. Specifically, this aligns with Article 5(1)(a) which mandates lawful, fair, and transparent processing, and Article 24 which requires controllers to implement appropriate measures to ensure compliance. Providing clear, comprehensive, and easily accessible information about personal data storage and processing is essential for meeting GDPR's stringent requirements for transparency and accountability as stipulated in Articles 12, 13, and 14 concerning the provision of information to data subjects.

2.4.3 Data portability and interoperability

It is a common feature of PIMS that they provide access to personal data of individuals to other applications and tools. This requires standardised or at least well established formats of data representation and application programmable interfaces (API). Furthermore, documentation of the applied formats and standards is necessary to provide interoperability and share data with other applications.

2.4.4 Data security

Data security is a highly important requirement as it concerns personal data of individuals. In PIMS personal data of individuals is accessed by external applications through an API, which exposes the data to the outside. This requires strong security measures, such as encryption and data minimisation. Encryption can be used to verify the authenticity of data and to implement privacy and data protect features, as the access is only granted to authorised agents. Encryption can be applied in both processes, data storage and data transfer. Data minimisation relates to the amount of data that is stored. Only necessary data should be stored and no data should be stored without purpose. So in case of unwanted access, a smaller amount of data can be affected.

Implementing these security measures is not just best practice but is also critical for proving compliance with specific GDPR provisions. Specifically, this aligns with Article 32, which mandates the implementation of appropriate security measures to ensure a level of security appropriate to the risk. By employing encryption and data minimization strategies, organisations can demonstrate their commitment to safeguarding personal data, thereby fulfilling GDPR's stringent requirements for data protection and accountability.

2.4.5 Accountability and liability

When it comes to processing personal data also questions of responsibility, liability, and accountability have to be clarified before setting up such a system. It has to be specified which organisation and persons are in charge of ensuring the privacy and who takes action if a data breach occurs. Furthermore, a process has to be set up on how to deal with data problems and user complaints. This information needs to be accessible and displayed for all users.

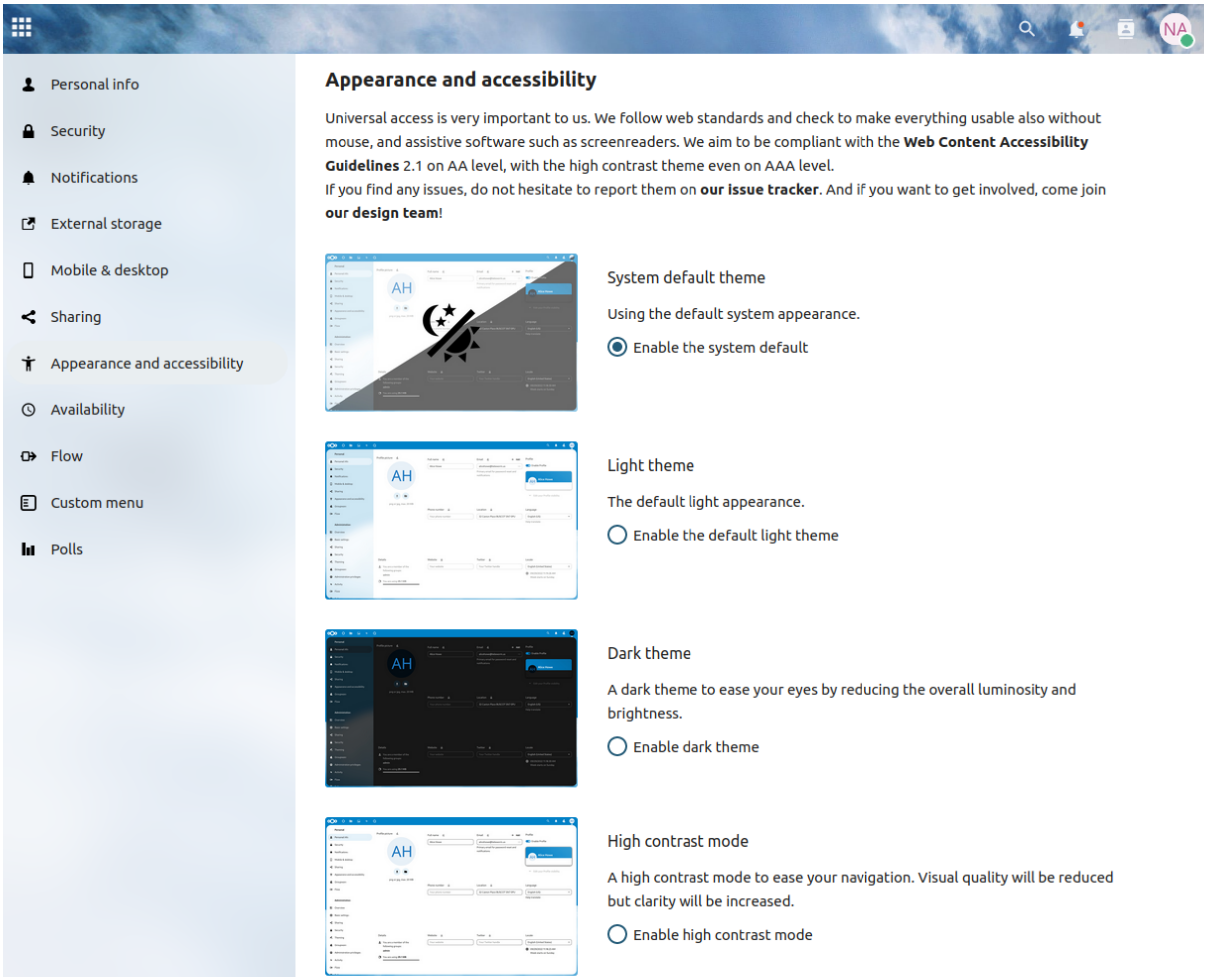
3. Existing PIMS solutions and best practices

This section lists and describes a selection of current systems, projects, and initiatives in the context of PIMS. The listed tools serve as best practices of existing PIMS software and should give hints for the development of the ITHACA PIMS solutions.

3.1 Nextcloud

Nextcloud (2023) is an open source Software as a Service (SaaS) solution that offers cloud services for individuals and groups. Users are provided with a safe environment where they can store and share their data of any file type in a hierarchical file system. Furthermore, Nextcloud embraces modules calendar, event schedules, project boards, text processors (Only Office), chat, and video conference tools (Big Blue Button).

Nextcloud is not primarily a PIMS with main focus on sharing data with other applications. However, it shares some relevant features with PIMS. Users can set the appearance by selecting a theme (Figure 2). This dialog also allows users to choose a theme with high contrast, which helps people with visibility problems or impairment. Furthermore, Nextcloud enables users to share their stored files with others by providing a URL to the file. Sharing permissions can be configured, so that the users can control which data is accessible by others. The sharing can be restricted to specific users or allowed to anybody who has the URL. A screenshot of the sharing settings dialog is given in Figure 3. Profile visibility can be configured on a fine granular level (Figure 4). For each profile item (e.g. full name or email addresses) it can be configured if this information is shown to anybody, to users logged in to the system, or to none.



Appearance and accessibility

Universal access is very important to us. We follow web standards and check to make everything usable also without mouse, and assistive software such as screenreaders. We aim to be compliant with the **Web Content Accessibility Guidelines** 2.1 on AA level, with the high contrast theme even on AAA level.
If you find any issues, do not hesitate to report them on **our issue tracker**. And if you want to get involved, come join **our design team**!

System default theme

Using the default system appearance.

● Enable the system default

Light theme

The default light appearance.

○ Enable the default light theme

Dark theme

A dark theme to ease your eyes by reducing the overall luminosity and brightness.

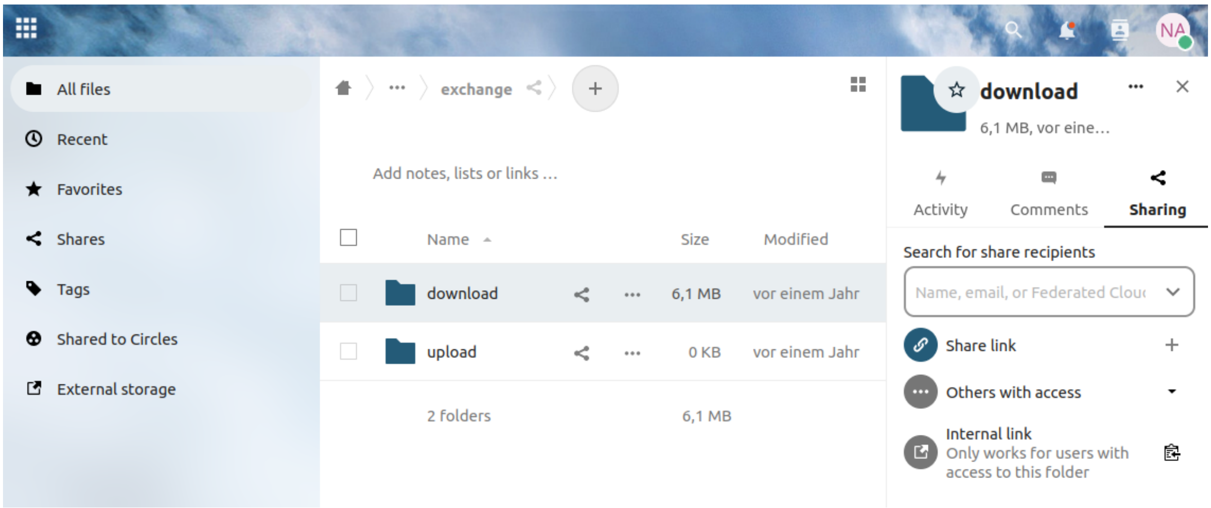
○ Enable dark theme

High contrast mode

A high contrast mode to ease your navigation. Visual quality will be reduced but clarity will be increased.

○ Enable high contrast mode

Figure 2: The Nextcloud accessibility settings dialog. Screenshot of the Nextcloud web application.



Add notes, lists or links ...

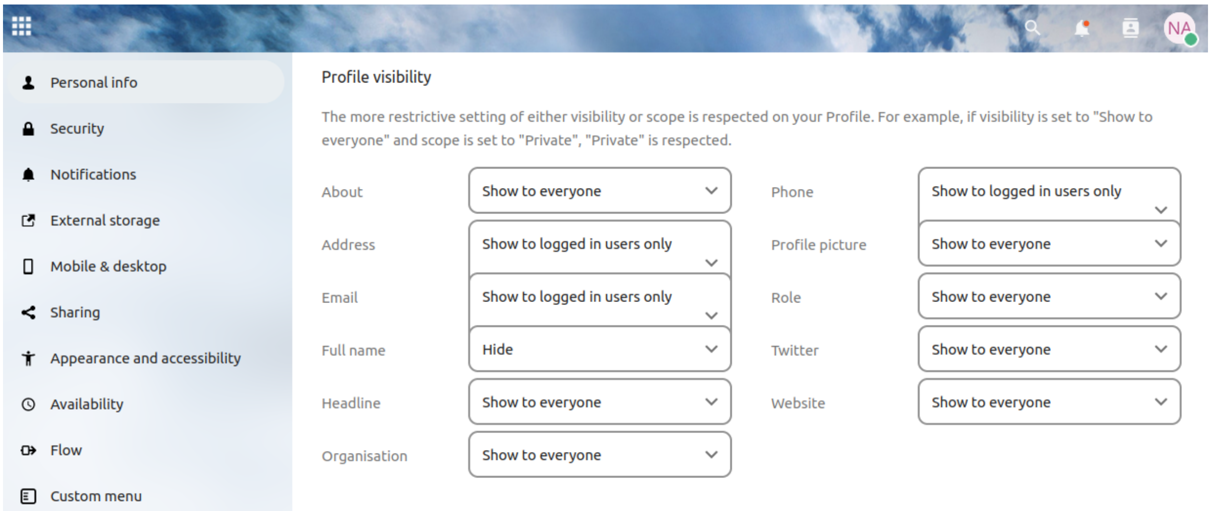
Name	Size	Modified
download	6,1 MB	vor einem Jahr
upload	0 KB	vor einem Jahr
2 folders	6,1 MB	

download
6,1 MB, vor eine...

Search for share recipients
Name, email, or Federated Clou

Internal link
Only works for users with access to this folder

Figure 3: The Nextcloud file sharing settings dialog. Screenshot of the Nextcloud web application.



Profile visibility

The more restrictive setting of either visibility or scope is respected on your Profile. For example, if visibility is set to "Show to everyone" and scope is set to "Private", "Private" is respected.

About	Show to everyone	Phone	Show to logged in users only
Address	Show to logged in users only	Profile picture	Show to everyone
Email	Show to logged in users only	Role	Show to everyone
Full name	Hide	Twitter	Show to everyone
Headline	Show to everyone	Website	Show to everyone
Organisation	Show to everyone		

Figure 4: The Nextcloud profile visibility settings dialog. Screenshot of the Nextcloud web application.

3.2 Solid

Solid (2023) is a specification that lets people store their data securely in decentralised data. Solid is an acronym for Social Linked Data and its development is led by Tim Berners Lee. Users can store their data in the so-called Pods that are like secure personal web servers for user data, where any kind of information can be stored. Pods are hosted on Solid servers where users can have multiple Pods.

Users can control access to their data and decide what data to share and with whom (see Figure 5). With Solid's Authentication and Authorization systems, users determine which people and applications can access their data. They grant or revoke access to any slice of their data as needed.

The same sharing and access control features are available for Solid applications. Within the interoperable Solid ecosystem, different applications can access the same data instead of requiring separate data silos specifically for the applications. For example, instead of inputting email with a bank statement notification service and with the phone's billing service, this information can be stored in a Pod only once and access is granted to read the email information to these disparate applications.

Figure 5: Solid pods of individual users. Image taken from Solid (2023).

3.3 MyDex

MyDex (2023) is a platform that provides any citizen with a Personal Data Store hosted safely and securely in the cloud. The Personal Data Store enables citizens to collect, receive, and store personal data about them and their life. Organisations can deliver personal data into them as part of normal service delivery or collect data from the Personal Data Store with the consent of the citizen (see Figure 6).

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. Thus, It does this by putting citizens in control. They can choose what data is used and how. This way, it's easy for citizens to exercise their rights under GDPR and the Data Protection Act, and for organisations to meet their obligations for transparency, data portability, and informed consent.

MyDex provides a secure identity service supporting registration, authentication, and ongoing management of privacy-protecting digital identity credentials. This puts citizens in control of their own online identities and enables accessing services where and when they need to, without endlessly creating usernames and passwords.

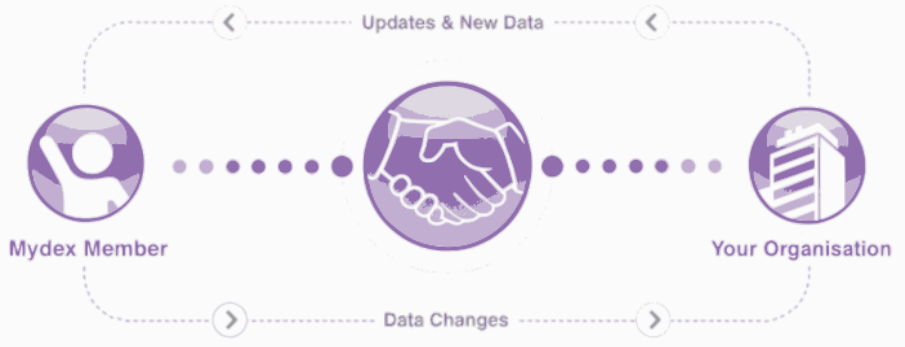


Figure 6: MyDex model for interchange of data with organisations. Image taken from MyDex (2023).

3.4 MyData

MyData (2023) is an initiative to empower individuals by improving their right to self-determination regarding their personal data. It provides a human-centric approach to personal data management, which combines industry need for data with digital human rights. The core idea is to offer an easier way to see where personal data goes, specify who can use it, and alter these decisions over time. The MyData approach aims to strengthen digital human rights whilst opening new opportunities for businesses to develop innovative, personal data-based services built on mutual trust. The initiative offers a set of principles to combine industry-needs for data access with digital human-rights.

The MyData model seeks to give people access to their information and control over their data (Poikolam et. al, 2020). The General Data Protection Regulation (GDPR) provides a good basis for this, but MyData claims that systems under the GDPR lack easy-to-use tools for people to access and transfer information about themselves from one system to another. Thus MyData proposes a human-centric model that puts the user in control of their data.

The MyData operator reference model (Poikolam et. al, 2020) 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 nine core functional elements are:

- ***Identity management.*** Identity management handles authentication and authorisation of individuals and organisations in different, linked identity domains and links identities to permissions.
- ***Permission management***. Permission management enables people to manage and have an overview of data transactions and connections and to execute their legal rights.
- ***Personal Data Storage.*** Personal data storage allows data to be integrated from multiple sources (including data created by a person) in storage under the individual's control.

- ***Service management.*** Service management uses connection and relationship management tools to link operators, data sources, and data using services
- ***Value exchange.*** Value exchange facilitates accounting and capturing value (monetary or other forms of credits or reputation) created in the exchange of data.
- ***Data model management.*** Data model management is about managing the semantics (meaning) of data, including conversion from one data model to another.
- ***Personal data transfer.*** Personal data transfer implements the interfaces (e.g. APIs) to enable data exchange between the ecosystem participants in a standardised and secure manner.
- ***Governance support.*** Governance support enables compliance with the underlying governance frameworks to establish trustworthy relationships between individuals and organisations.
- ***Accountability and logging.*** Logging and accountability entails keeping track of all information exchanges taking place and creating transparency about who accessed what and when.

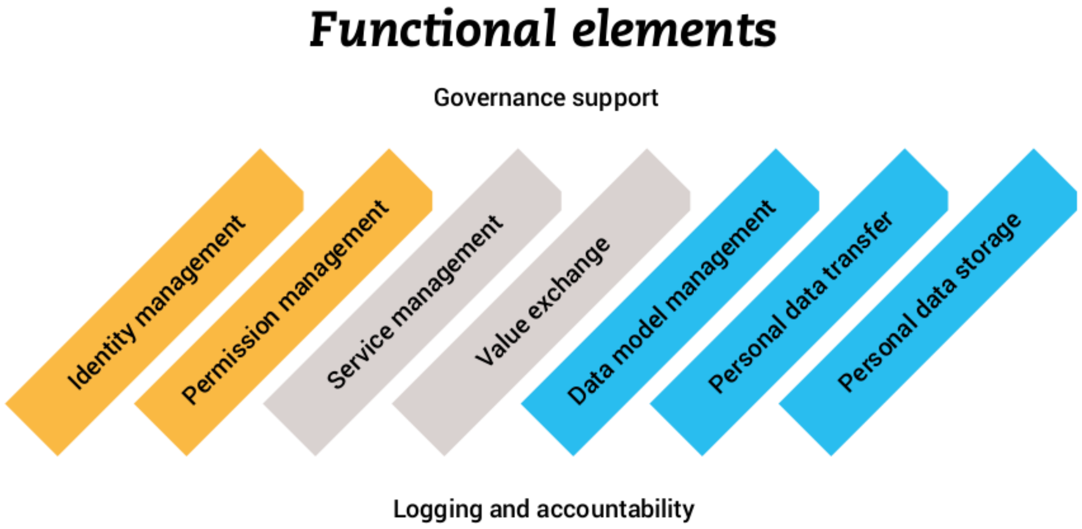


Figure 7: MyData operator reference model. Image taken from Poikolam et. al (2020).

3.5 PIMCity

PIMCity (2023) is a Horizon Europe Project that elaborates a holistic approach to PIMS creation by defining a comprehensive set of required tools and functions. The core part of the project is the development of the PIMS Development Kit (PDK) that aims to reduce the complexity of PIMS and lower the barriers for companies to enter the web data market. Furthermore, PIMCity designs new mechanisms to increase the awareness of users and stakeholders. In order to demonstrate the effectiveness of this concept and the tools of the PDK, EasyPIMS has been developed which is a fully-fledged PIMS. An overview of these components is outlined in Figure 5.

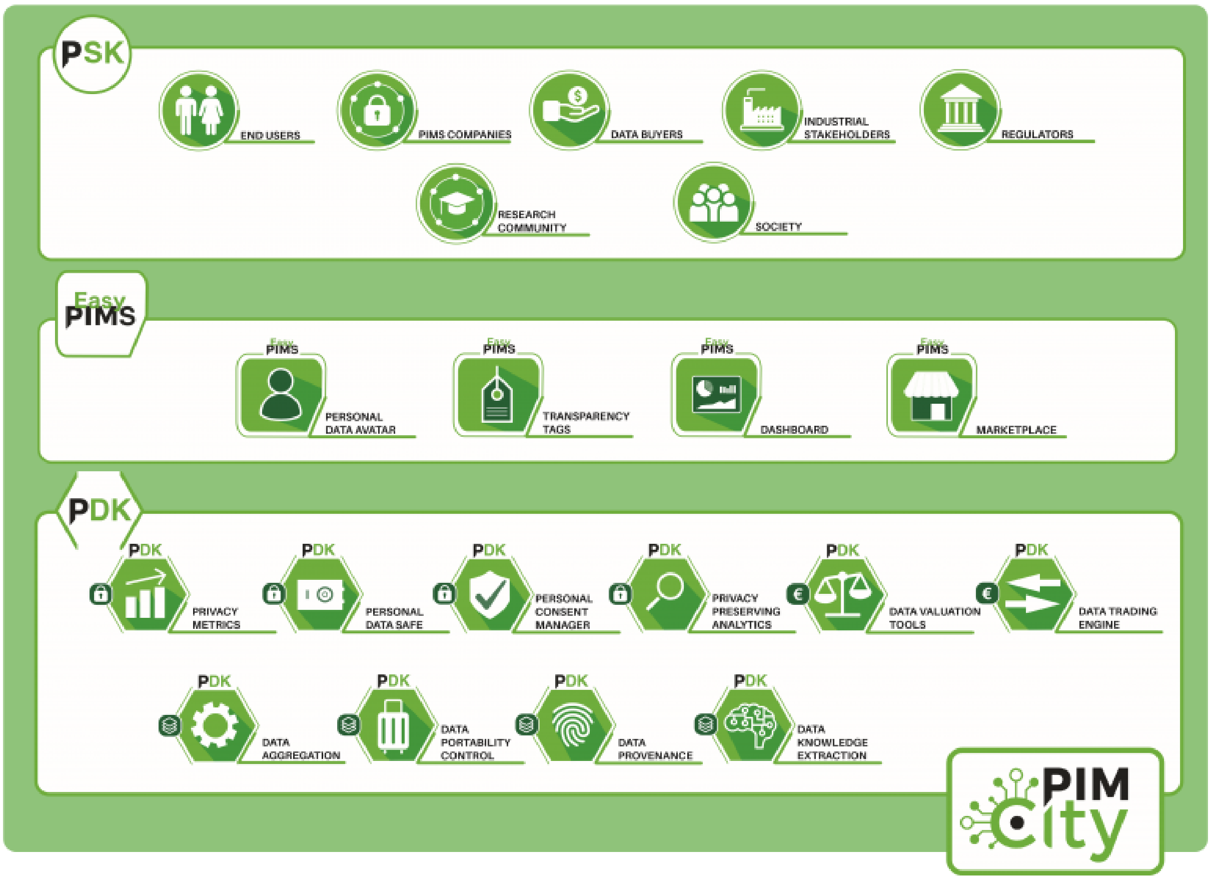


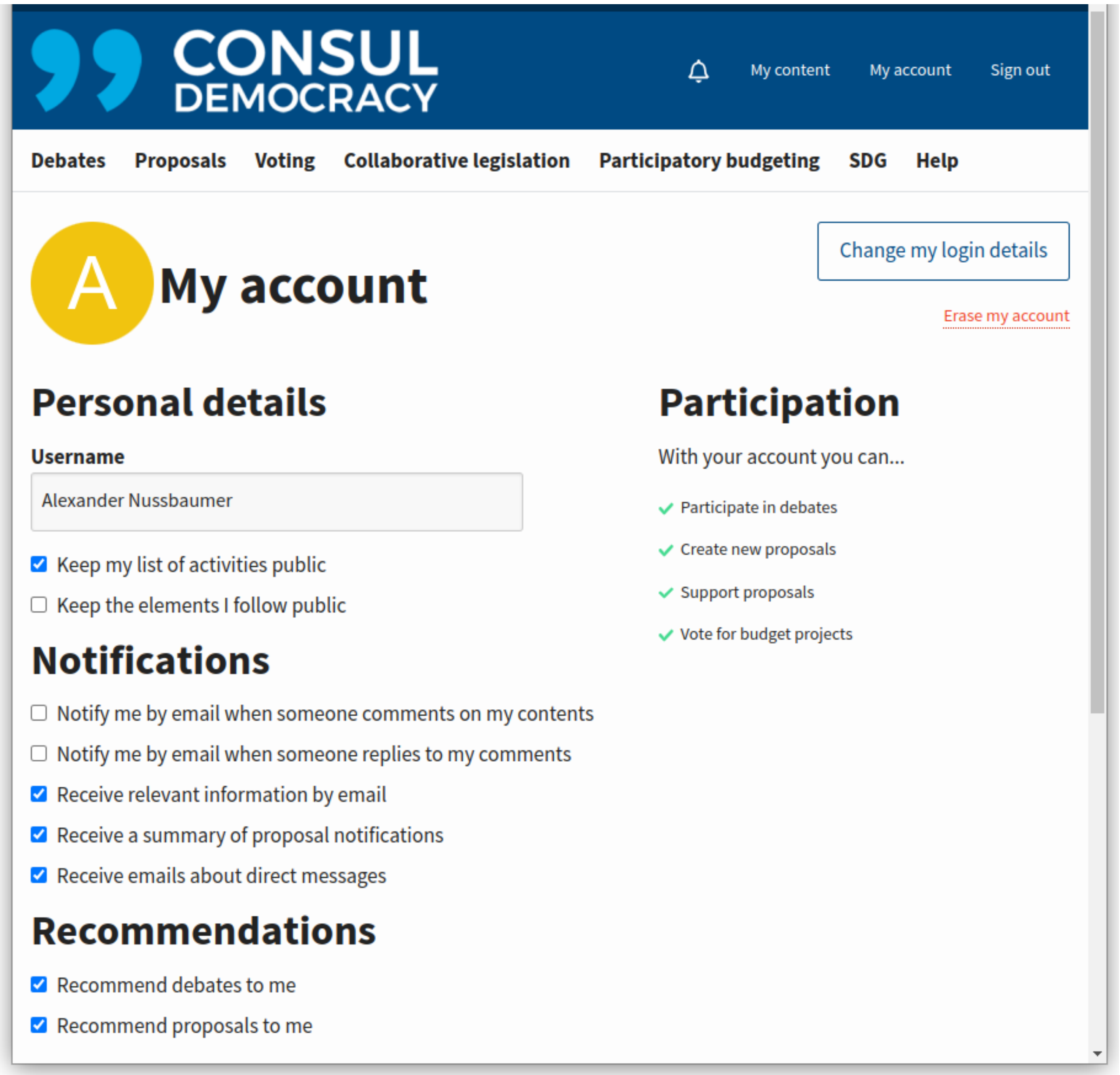
Figure 8: Overall representation of PIMCity's outputs, PDK components and EasyPIMS platform, together with stakeholders which will benefit from them. Image taken from PIMS (2023).

The tools of the PDK include tools to improve users' privacy, tools for new data economy, and tools for novel data management (Jha, 2022). The following list shortly presents the tools for privacy management:

- The Personal Data Safe (P-DS) enables the storage of personal data in a controlled form. It implements a secure repository for the user's personal information like navigation history, contacts, preferences, personal information, etc.
- The Personal Privacy Metrics (P-PM) represent the means to increase the user's awareness. This component collects, computes and shares easy-to-understand metrics to allow users to know how a service stores and manages the data.
- The Personal Privacy Preserving Analytics (P-PPA) allows extracting useful information from data while preserving users' privacy.
- The Personal Consent Manager (P-CM) is the means to define all the user's preferences when dealing with personal data. It defines which data a service is allowed to collect, process, or which can be shared with third parties.

3.6 CONSUL DEMOCRACY

CONSUL DEMOCRACY (2023) is an open source web-based platform that enables citizen participation for an open, transparent and democratic government. CONSUL aims to support decision making processes of citizens with useful features. Briefly, users will register on the platform with an email account and name. They can initiate discussions and surveys on interesting topics. Related surveys or discussions can be structured or unstructured, which also enables group discussions. Furthermore, resources like documents or photos and videos can be integrated into the platform taken from other platforms, such as Facebook. A screenshot of the user settings is shown in Figure 9.



My account

Personal details

Username

Alexander Nussbaumer

☑ Keep my list of activities public

☐ Keep the elements I follow public

Notifications

☐ Notify me by email when someone comments on my contents

☐ Notify me by email when someone replies to my comments

☑ Receive relevant information by email

☑ Receive a summary of proposal notifications

☑ Receive emails about direct messages

Recommendations

☑ Recommend debates to me

☑ Recommend proposals to me

Participation

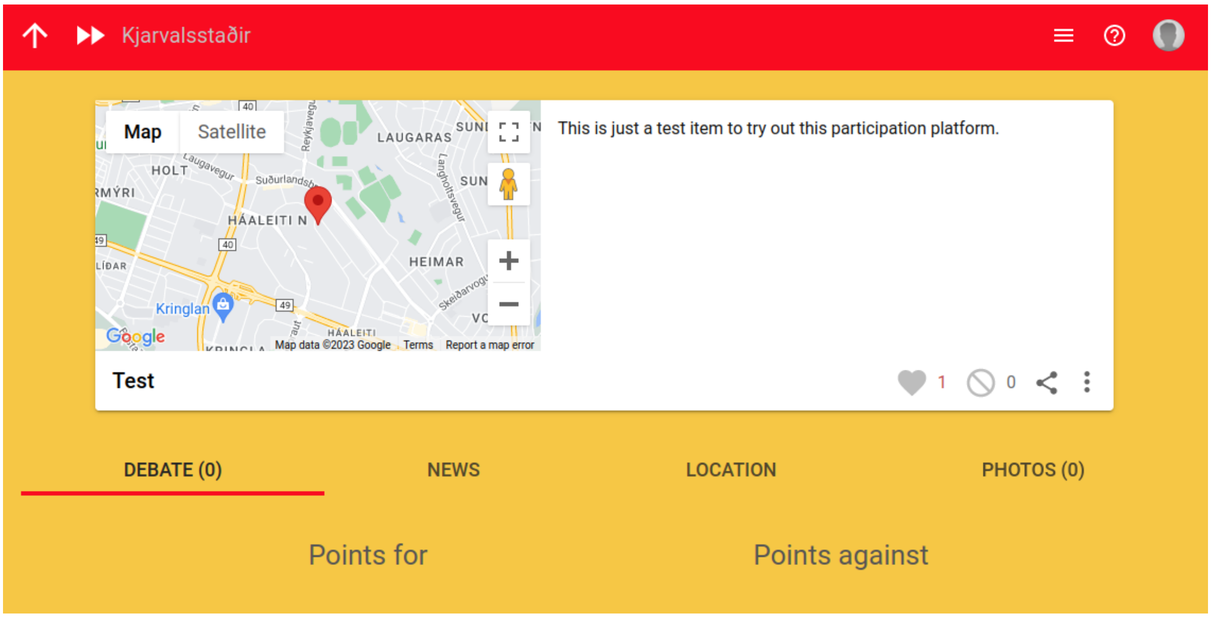
With your account you can...

- ✓ Participate in debates
- ✓ Create new proposals
- ✓ Support proposals
- ✓ Vote for budget projects

Figure 9: User settings page of the CONSUL DEMOCRACY platform. Screenshot of the CONSUL DEMOCRACY web application.

3.7 Better Reykjavik

The second example of a citizen participation project with PIMS features is the Better Reykjavik (2023) project. This project allows citizens of Iceland to participate in the democratic process. Users can add new ideas or topics in relation to certain topics, as well as comment, discuss, and like other ideas. A screenshot with a new idea (a test item) is shown in Figure 10. Other users can debate this idea by adding arguments for or against this idea. Each user can get an overview of their own ideas or discussion items added to this platform (Figure 11). This view provides a graphical overview of the content that uses have added. If there is a discussion of others on a user's contributed content, the user will be notified. In a settings dialog the user can configure how (e.g. email or on the website) to be notified on which action (e.g. comment on own idea). This dialog is shown in Figure 12.



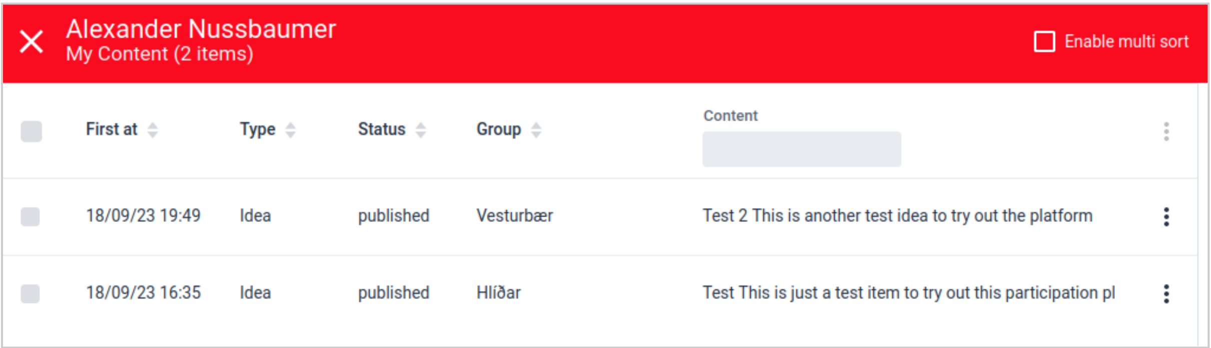
This is just a test item to try out this participation platform.

Test

Points for

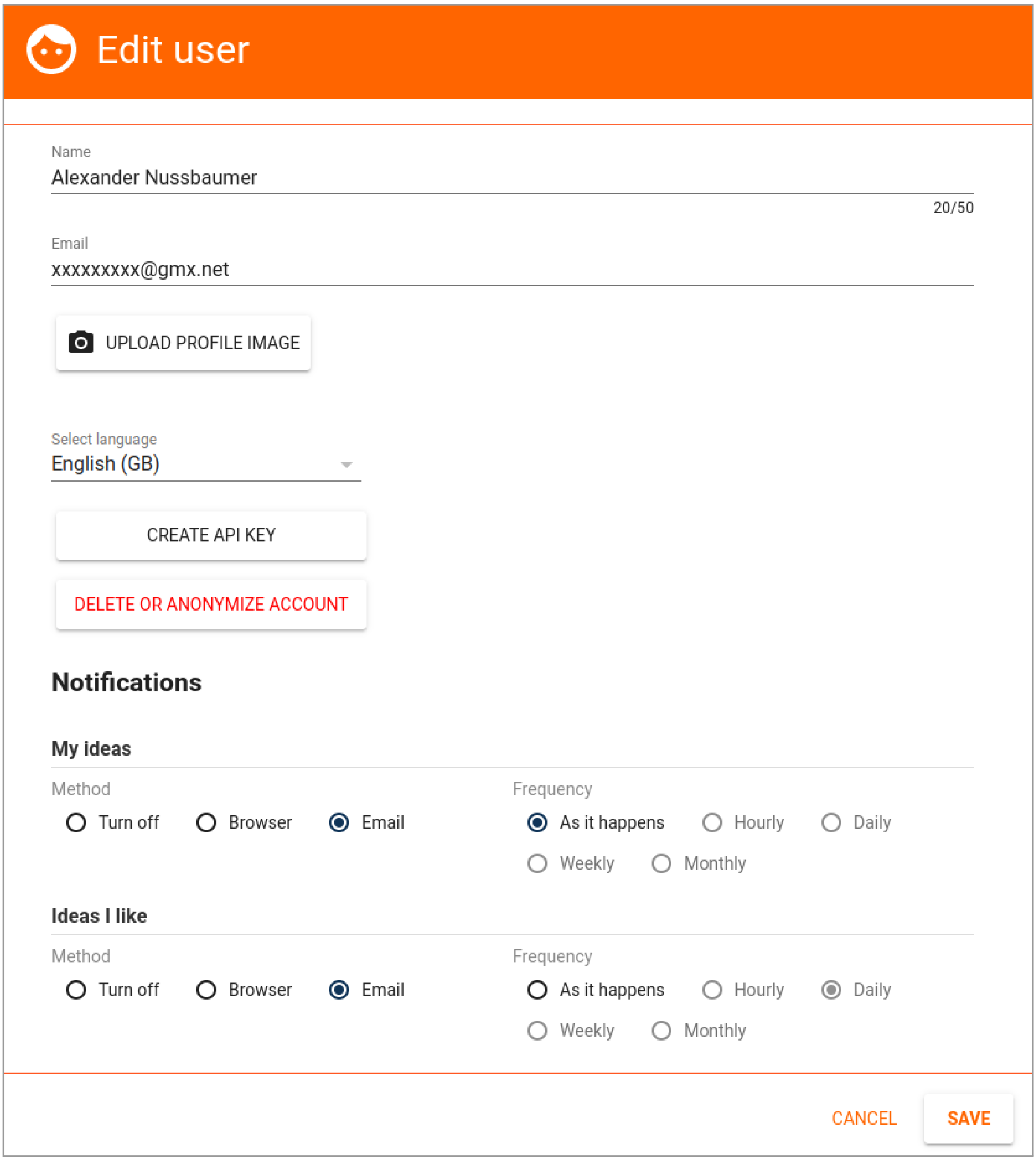
Points against

Figure 10: A test item (an idea) added to the Better Reykjavik platform. The item includes an item, a description, and a location shown on the map. Screenshot of the Better Reykjavik web application.



First at	Type	Status	Group	Content
18/09/23 19:49	Idea	published	Vesturbær	Test 2 This is another test idea to try out the platform
18/09/23 16:35	Idea	published	Hlíðar	Test This is just a test item to try out this participation pl

Figure 11: The test item is shown in the content overview page of the Better Reykjavik platform. Screenshot of the Better Reykjavik web application.



Edit user

Name
Alexander Nussbaumer
20/50

Email
xxxxxxxxx@gmx.net

Select language
English (GB)

Notifications

My ideas

Method
○ Turn off ○ Browser ● Email

Frequency
● As it happens ○ Hourly ○ Daily
○ Weekly ○ Monthly

Ideas I like

Method
○ Turn off ○ Browser ● Email

Frequency
○ As it happens ○ Hourly ● Daily
○ Weekly ○ Monthly

Figure 12: User settings page of the Better Reykjavik platform. Screenshot of the Better Reykjavik web application.

4. Relevance for citizen participation

This section provides guidelines for the development of the ITHACA platform from the PIMS perspective. Since the concrete use cases and functionalities of ITHACA have not been specified yet, this guideline is kept rather general and provides requirements, ideas and safeguards that should be taken into account.

4.1 Requirements for ITHACA

Following the discussion in Sections 2 and 3, there are several requirements that arise from dealing with this personal data in a citizen participation platform. Furthermore, ITHACA has a focus on vulnerable groups which imposes additional requirements. The following list summarises these requirements. This list at the current stage of the project is not a final set of requirements, but a proposal or a frame to define the detailed requirements in the design phase of the ITHACA platform (T3.10). It consists of both technical and human-centric aspects, whereby some requirements are mainly technical, some are mainly human-centric, and some overlap and include both types. Furthermore, most requirements are interrelated, meaning that there are interdependencies and mutual exclusions. Thus, a final detailed requirements set must balance this initial set.

Topic	Description
Personal data storage	A record or storage of personal user data needs to hold all personal user data, such as own contributions in form of various media, reactions on contributions of others, personal settings, as well as permissions and consents.
Data security	The storage and transfer of personal data must adhere to the highest security standards. Specifically, it is imperative to guarantee the implementation of appropriate technical and organisational measures, such as encryption and access management systems. Additionally, the transfer of personal data outside the European Economic Area (EEA) should either be avoided or be conducted in compliance with the guarantees described in Articles 44-50 of the GDPR.
Interoperability	Personal data saved in a data storage needs to be accessible by the various modules of the ITHACA platform, which requires a well defined and documented API, as well as a documented data model with sufficient semantics.
Privacy	It is essential to uphold the principles of 'Privacy by Design' and 'Privacy by Default' in the handling of personal data. This entails implementing robust technical and organisational measures to ensure data security, in alignment with the 'Privacy by Design' principle. Concurrently, 'Privacy by Default' measures must be in place to safeguard user privacy. These measures include collecting only the data that is strictly necessary (data minimization), restricting any further use of the data, and

	employing techniques such as anonymization and pseudonymization to protect the collected data.
Data analytics	Personal data should be anonymously analysed, in order to draw conclusions that can be used by an application to support the user. If data analytics is not performed anonymously, then additional consent is needed.
Data management	Only necessary user data should be stored needed for the system's functions and no data should be stored without purpose (data minimisation). Furthermore, users need to be able to access and delete their own data.,
Data integrity	Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (data integrity principle). This can be achieved by appropriate backup mechanisms, which ensures that data remains intact.
Permission management	The users should be enabled to perform fine grained settings about which application or function is allowed to access which data.
Consent management	Consent management is needed that puts people in control of which data are used for which purposes. This includes that users can deny or revoke the use of personal data.
Transparency	It must be shown to the user, which personal data is collected, stored, and how it is processed. This includes a complete list of data and the purposes of use thereof along with, where, and why the data is used. This requirement is strongly related to understandability and explainability of the presented information.
Sharing visibility	It should be shown which data is shown to other users, user groups, or the public.
Traceability	Actions and processes should be recorded and presented in a way that users can understand past activities and the development of a process.
Understandability	All information presented to the end-user (e.g. transparent presentation of stored data, stored permissions and consents, and explanations) should be understandable by end-users. This includes the use of simple language, easy to understand explanations of technical concepts, and understandable presentation of graphical data.
Explainability	The processing and presentation of data, consent, and permissions has to be explained in a way that is understandable by the end users. Within the scope of the ITHACA Project, which incorporates advanced artificial

	intelligence (AI) techniques for data processing, the principle of explainability is of paramount importance. Given that AI methods can often function as black boxes, it becomes crucial to elucidate how data is processed and how specific outcomes are derived. This is not just a matter of ethical transparency but also a legal requirement for compliance with GDPR provisions on automated decision-making, including profiling, as outlined in Article 22. Ensuring explainability in the processing of personal data is therefore essential for both user trust and regulatory compliance
End-user needs	A great part of ITHACA end-users are intended to be vulnerable groups with various special needs that have to be taken into account. The design of data access and interfaces need to be guided by the end-user needs and limitations. This includes accessibility features of the user interface that lowers the barrier to use the ITHACA platform and thus enables the participation of vulnerable groups.
Issue reporting	Users should have the possibility to report and give feedback if there are any issues or problems with the data management

Table 1: General and non-functional requirements for the ITHACA platform.

4.2 Concept for data management

Following the requirements listed above, this subsection presents a general concept for data management that takes into account the user data, the tools and functions, and related human aspects. The data presented in this section are examples that are used to outline the concept. The concrete data for the ITHACA platform will be elaborated later in a different work package.

User data that might be collected and used by participation tools are listed in Table 1. This table categorises user information into three types of data. First, personal data is information that describes the user, such as name or age. Second, participation data addresses data that the user or citizen has provided as part of a participation process, such as discussion items, comments, or surveys data. Third, external data relates to data of the user stored and provided by other applications, such as social media platforms.

Category	**Data**	**Description**
Personal data	person name	The full name of a person; can be the real name or a nickname or any name the user prefers; visible to others
	username, password	The username and password needed to login; not visible to others; password encrypted

	age	The age or age range of the person
	gender	The gender of the person; careful use of options needed
	email, mobile number	for contacting the person and for securing the account
	place of residence	The place where the person (mainly) lives; this relates to the participation in specific topics (or exclusion from topics)
	language	the language of the user interface and the language(s) the person communicates with others
	accessibility	accessibility relates to special needs regarding the user interface and presentation of information, such as easy language, colour blindness, or visual impairment; this also relates to support tools, such as text-to-speech functions.
	vulnerability characteristics	information about the nature of vulnerability, if applicable, for example if a person is a member of a minority group. This might have an effect on the participation process.
	current location	the current (and past) location of a person; can be derived from GPS data
	role	the type of access and system rights, such as administrator or moderator
	trust level	information if a user is trusted or if there were unwanted behaviour in the past, such as insults
	settings	general technical settings and configurations
	activity	usage of the system and functions, log data
Participation data	discussion items and comments	contributions in a discussion including media data
	feedback and evaluation	feedback and evaluation on community contributions, such as likes or ratings
	survey and voting	data provided in a survey or voting
External data	social media profiles	profile information of social media, such as @username@mastodon.social
	social media data	data provided at social media, such as postings, images, or likes
	social relation	relation data in social media, such as Facebook

		friends or Mastodon followers

Table 2: Potential user data related to participation platforms and description why they are relevant.

4.3 Bias mitigation

A key focus of the ITHACA project is the mitigation of social biases related to vulnerable people and groups. This goal is also important when it comes to the management of personal information. Different social and vulnerable groups have different needs which have to be taken into account. Thus these needs should be transformed in functional requirements and integrated in the system and tool design.

Examples of requirements for vulnerable groups are understandability and accessibility. Understandability refers to the provision of information in a way that it is understandable for all addressed types of end users and social groups. This might include the use of clear and easy-writing style, choosing the right language, avoiding technical information that is not needed, and meaningful explanation of the provided information and tool functions.

Accessibility refers to the designing the user interface so that it does not provide any barrier for the target group. This mainly refers to disabilities, such as visual disabilities, but also to the digital device that users have available.

Hence, the design of the user interface with the presented information needs a careful analysis of the addressed end user groups, their needs and constraints.

4.4 Co-design approach

The design and development of the PIMS component in ITHACA is dedicated to Task 3.10. According to the task description this task will take into account the architectural elements and best practices elaborated in this deliverable, as well as the user requirements elicited in work package 2. Consequently, end-users should be included in the user requirement and design process. A co-design approach that includes end-users in the conceptual design of the software would balance the requirements formulated in this deliverable and the end-user needs elicited in work package 2. Workshops and focus groups with end-users are a suitable method to design the PIMS concept of ITHACA.

5. Conclusion and outlook

This deliverable provides an overview of Personal Information Management Systems (PIMS) and specifies optional requirements of the ITHACA PIMS. According to the task description (T1.6), this overview includes (a) an elaboration of existing initiatives and projects claiming PIMS features (Section 3), (b) elements of architecture, records, and checklists required for the implementation (Section 2.3 and 4.2), (c) safeguards for compliance with the General

Data Protection Regulation (GDPR) (Section 4.1), and (d) user interfaces of such systems (Section 4.2). Furthermore, a general introduction to PIMS is given in Section 2.

This elaboration and overview is intended to serve as a guideline for the design and implementation of the ITHACA platform. Future work will include a user-centred design process of the ITHACA platform. Apart from findings and considerations presented in this deliverable, user studies and requirements elicitation with end uses are being conducted in WP2. In these studies, system design and functions are discussed with end users (vulnerable groups) and their feedback will be taken into account. The system can be implemented based on the guidelines in this deliverable, the results from the user studies, and the project goals.

References

Bergman, O., Beyth-Marom, R. and Nachmias, R. (2003), The user-subjective approach to personal information management systems. J. Am. Soc. Inf. Sci., 54: 872-878. https://doi.org/10.1002/asi.10283

Bergman, O., Beyth-Marom, R., & Nachmias, R. (2008), The user-subjective approach to personal information management systems design: Evidence and implementations. J. Am. Soc. Inf. Sci., 59: 235-246. https://doi.org/10.1002/asi.20738

Bernemann, J., & Kneuper, R (2023). Personal Information Management Systems nach TTDSG. HMD Praxis der Wirtschaftsinformatik, 60, 308–321. https://doi.org/10.1365/s40702-023-00946-4

Better Reykjavik (2023). Website of the Better Reykjavik project. https://betrireykjavik.is

Consul (2023). Consul website. https://consuldemocracy.org/en/

European Data Protection Supervisor (2016). EDPS Opinion on Personal Information Management Systems. https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

European Data Protection Supervisor (2020). Personal Information Management Systems. TechDispatch 2020(3). https://edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf

European Data Protection Supervisor (2023). Personal Information Management System. https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en

Janssen, H. & Singh, J. (2022). Personal Information Management Systems, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 11, Iss. 2, pp. 1-6, https://doi.org/10.14763/2022.2.1659

Jha, N., Trevisan, M., Vassio, L., Traverso, S., Garcia-Recuero, A. & et al. (2022). A PIMS Development Kit for New Personal Data Platforms. IEEE Internet Computing, 26(03), pp. 79-84. http://doi.org/10.1109/MIC.2022.3157356

MyData (2023). MyData website. https://www.mydata.org/

MyDex (2023). MyDex website. https://mydex.org/

Nasar, M. R. A., Mohd, M., & Ali, N. M. (2011). Personal information management systems and interfaces: An overview. In Proceedings of the International Conference on Semantic Technology and Information Retrieval, pp. 197-202. http://doi.org/10.1109/STAIR.2011.5995788.

Nextcloud (2023). Nextcloud website. https://nextcloud.com/

PIMCity (2023). PIMCity website. https://www.pimcity-h2020.eu/

Poikolam, A., Kuikkaniemi, K., Kuittinen, O., Honko, H., Knuutila, A., & Lähteenoja, V. (2020). MyData - An introduction to human-centric use of personal data.

https://www.mydata.org/wp-content/uploads/2022/07/mydata-white-paper-english-2020-2.pdf

Regulation (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016: General Data Protection Regulation (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Solid (2023). Solid website. https://solidproject.org/