H2020-SC6-GOVERNANCE-2018-2019-2020

DT-GOVERNANCE-05-2018-2019-2020

ACROSS

Towards user journeys
for the delivery of cross-border services
ensuring data sovereignty

D3.4 Implementation of the ACROSS Data Governance framework for data sovereignty - Intermediate

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	D3.4: Implementation of the ACROSS Data Governance framework for data sovereignty - Intermediate
Work package	WP3: ACROSS Data Governance framework
Nature	Other
Dissemination Level	Public
Date	01/03/2023
Status	Final version
Editor(s)	Valentín Sánchez (TEC)
Contributor(s)	Idoia Murua (TEC), Urtza Iturraspe (TEC)
Reviewer(s)	Vincenzo Savarino (ENG), David Britnell (DATAPORT), Enrique Areizaga (TEC)
Document description	This report includes the description of the intermediate version of the ACROSS Personal Data Management Framework covering the complete set of functionalities. The final version will reflect the changes requested by the use cases regarding usability and the solution to the issues arising during the validation phase.

About

The project is co-funded by the European Commission's Horizon 2020 research and innovation framework programme. Spanning through three years, ACROSS consists of a consortium of 10 partners from 7 countries: Athens Technology Center (coordinator), Tecnalia, Dataport, Engineering, Fraunhofer, GRNET, TimeLex, The Lisbon Council, Waag and VARAM.

DISCLAIMER

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use, which may be made of the information contained therein.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	17/02/2023	First draft for revision	TECNALIA
V0.2	28/02/2023	Formal revision process	ENGINEERING, DATAPORT
Final	01/03/2023	Added conclusion section	TECNALIA

Executive Summary

The main objective of the ACROSS project is to provide the means (tools, methods and techniques) to enable user-centric design and implementation of interoperable cross-border (digital) public services compliant with the current European regulations (e.g. the Single Digital Gateway (SDG) and Once -Only principle (OOP), European Interoperability Framework (EIF)) where the private sector can also interconnect their services **while ensuring the data sovereignty of the citizens, who can set the privacy level that will allow the public and private sector to access to their data based on their requirements**.

In order to ensure the protection of personal data (and documents) and its compliance with GDPR and other relevant regulations, especially when shared between organizations, ACROSS will design and implement with **a data governance framework** where data subjects can control the use of their personal data empowering them**.**

The **data governance framework will** allow users to:

1) monitor which data are available and how they are used or how it has been accessed,
2) control: add, delete or change data, provide or block access to public bodies (where permitted or enforced by the law), businesses or data brokers, giving individuals the power to determine how their data can be used.

From a technical point of view the Data governance framework includes:

1) A "private/personal data" governance platform including a Personal data management site which provides a user interface to define manage and control the use of personal data. (Data portal)
2) A set of APIs/libraries to interact with the ACROSS platform

A previous deliverable [1] gathered the ACROSS data governance framework requirements, including the data governance, security and privacy requirements from the use cases, considering both the technical and operational perspectives, the final user expectations regarding data privacy and the ACROSS platform integration strategy. Furthermore, an initial design of the framework was included. Then, a first prototype of the data governance framework [2], the so-called minimum viable product was developed to check the initial design and based on the validation results, the final framework architecture [3] was designed. Next, an intermediate version of the Data Governance Framework including all the expected functionality has been implemented and deployed.

This report contains the documentation needed to use the intermediate version of the Data Governance Framework including the user manual, the integration guide and the installation guide.

Table of Contents

List of Figures

List of Tables

List of Terms and Abbreviations

Abbreviation	Definition
DPO	Data Protection Officer
CPSV-AP	Core Public Service Vocabulary Application Profile
ABC	Attribute Based Credentials
GDPR	General Data Protection Regulation
DGA	Data Governance Act
PIMS	Personal Information Management System
SDGR	Single Digital Gateway Regulation
OOP	Once-only principle
CRUD	Create, Read, Update and Delete
DPV	Data Privacy Vocabulary
Transparency Dashboard	The name of the Data Governance Framework graphical user interface application

1 Introduction

1.1 Context

One of the ACROSS objectives is **to ensure the protection of personal data (**and documents**) and its compliance with GDPR and other relevant regulations, especially when shared between organizations.** This objective has been fulfilled by designing and implementing a private/personal data governance framework where data subjects can control the use of their personal data empowering them.

ACROSS offers the citizen the possibility of defining which public and private organization will be allowed to *access which data and for what purpose* through the **ACROSS Data Governance Framework.** The main aim is to give the citizen the chance of **govern the access to** their data, profiting from a set of usage policies that implement levels of access and they can be the **sovereign owner** of such data.

The **data governance framework,** that allows users to

1) monitor which data are available and how they are used or how it has been accessed,
2) to control: add, delete or change data, provide or block access to public bodies (where permitted or enforced by the law) businesses or data brokers, giving individuals the power to determine how their data can be used.

From a technical point of view the Data governance framework includes:

3) A "private/personal data" governance platform including a Personal data management site which provides a user interface to define manage and control the use of personal data. (Data portal)
4) A set of APIs/libraries to interact with the ACROSS platform

The governance framework has been based on existing initiatives and techniques.

1. **MyData**[1] model for human-centered personal data management and processing and MyData operator concept[2]
2. Built on the approach adopted in CaPe solution[3] for personal data management,
3. Include generic ***data usage policies***[4] when the private data needs to be transferred among several stakeholders (IDSA Data Sovereignty)

[1] https://mydata.org/
[2] https://mydata.org/mydata-operators/
[3] https://github.com/OPSILab/Cape
[4] https://internationaldataspaces.org/data-sovereignty-updated-position-paper-on-data-usage-control-in-the-ids/

D3.1 (Design of the ACROSS Data Governance framework for data sovereignty – Initial) provided an accurate description of the ACROSS data governance framework requirements, along with a first draft of technical architecture, modules, and APIs. Besides, a set of relevant baseline technologies that will be used for the implementation of the data governance framework were described and their applicability to ACROSS was analysed.

These following conclusions from D3.1 have driven the evolution of the data governance framework design and its implementation.

- The ACROSS Personal Data Governance Framework is part of the so-called ACROSS platform, useful in the context of cross-border public/private services for the citizens. However, it has been designed to be an independent framework useful also for the individuals to manage their personal data according to the GDPR in any other context.
- ACROSS data governance framework does not cover the following functionalities included in other initiatives:
  - Secure Data Storage and data minimization techniques: These will be provided by personal wallet technologies being developed by other projects.
  - Secure Data transfer among services
- ACROSS extends the MyData operator with data usage control based on data usage policies

Then, a first prototype of the data governance framework [2], the so-called minimum viable product was developed to check the initial design and based on the validation results, the final framework architecture [3] was designed. Based on the final design, an intermediate version of the Data Governance Framework including all the expected functionality has been implemented and deployed.

1.2 Purpose and Scope

This deliverable includes the implementation of the intermediate version of the ACROSS Personal Data Management Framework covering the complete set of functionalities included in D3.2 "Design of the ACROSS Data Governance framework for data sovereignty – Final". This intermediate version will be evaluated by the use cases to produce D3.5: Implementation of the ACROSS Data Governance framework for data sovereignty – Final.

The deliverable includes the information needed to use this intermediate version including:

- The user manual
- The integration manual
- The installation guide

Finally, some conclusions are presented along with a set of next steps.

1.3 Approach for Work Package and Relation to other Work Packages and Deliverables

The goal of WP3 is to design, implement and deploy a “private/personal data” governance framework that allows the citizens to control how their data and their activities are created or used by businesses, governments, or data brokers, giving individuals the power to determine how their data can be used. The governance framework has been based on existing solutions such as MyData model for human-centred personal data management and processing, but it will also include generic data usage policies when the private data needs to be transferred among several stakeholders.

The services from this WP will be integrated into the platform created in WP5 and will demonstrate the functionality of the use cases in WP6.

WP5 aims at providing the architectural and implementation aspects for the delivery of the ACROSS tools taking into account the full range of requirements for such service. The design of the ACROSS platform has driven the design and implementation of the various components produced in the context of WP3, WP4 & WP5.

The ACROSS Personal Data Governance Framework is part of the so-called ACROSS platform (defined in WP5), useful in the context of cross-border public/private services for the citizens. However, it has been designed to be an independent framework which can be used also for individuals to manage their personal data according to the GDPR in any other context. Furthermore, it extends the MyData operator concept with Data usage policies enforcement.

WP2 and WP6 together defined the so-called user journeys based on the results several interviews with people from the three pilot countries. The aim of the interview process is to form potential user journeys, building on initial ideas. User journeys can include actions, touch points, emotions, pain points, and phases. Eventually to result in concrete (socio-technical) requirements for the ACROSS platform modules. A specific section about Data privacy issues was included in the questionnaire in order to gather requirements for the Data Governance Framework.

The final design was based on the results of the usability test findings for the first version of the platform (D3.3) that have been gathered in D6.2 Use case evaluation and impact assessment – Initial. **User tests** via structured interviews and a **co-creation workshop** have helped in collecting valuable feedback about the initial version of the ACROSS platform from real users, as well as stakeholders from pilot countries and EU institutes who are involved in relevant national or European projects. **A set of recommendations for**

the evolution of ACROSS solution have been reported, mostly focus on optimizing already implemented features as well as making previous requirements more specific.

Furthermore, some new functionalities have been included in the final design and have been implemented in the intermediate version or the Data Governance Framework:

1. Data usage policies enforcement for Data access control
    a. Data usage policy editor
        i. Create, modify and delete policies associated to services
    b. Rest interface for policy enforcement (Usage control)
2. Rest interface for data consent definition from the User Journey Service Engine (UJSE)
3. My Personal Data view

The following previous results of the project have been taken into account:

- D3.1 Design of the ACROSS Data Governance framework for data sovereignty – Initial [1]
- D3.3 Implementation of the ACROSS Data Governance framework for data sovereignty – Initial [2]
- D3.2 Design of the ACROSS Data Governance framework for data sovereignty – Final [3]
- D2.4 Report for cross-border service gap analysis – Final [4]
- D6.2 Use case evaluation and impact assessment – Initial [5]
- D5.2 System Architecture & Implementation Plan – Final [6]

1.4 Structure of the Deliverable

This deliverable has been structured in the following sections:

Section 2 contains the User Manual. The first objective of this section is helping the end user to understand the rationale behind the Personal Data Framework, the main concepts and functionalities of the framework. Next, a complete user manual of the Transparency dashboard is included.

Section 3 contains the integration guide i.e., the APIs exposed by the ACROSS data governance framework back-end that will be used by external applications to interact with the framework.

Section 4 includes the installation guide of the current version of the Data Governance Framework.

Finally, some conclusions are drawn together with recommendations for future work.

2 ACROSS Data governance framework user manual

The ACROSS Data governance framework defines a completely new way to manage personal data. Nowadays, the common way of dealing with personal data that we share with companies is to give the necessary permissions to each of the companies/services that use the data in a one-by-one basis using the applications provided by them.

This approach has several drawbacks from the final user perspective. To manage the personal data related permissions, it is necessary to use many different web sites and find the way to exercise the personal data rights. Furthermore, it is almost impossible to remember the whole set of applications/services holding and using our personal data.

The ACROSS Data Governance Framework offers the citizens a centralized way to manage all the personal data they share, defining which public and private organization will be allowed to access which data and for what purpose. Furthermore, the citizens will be able to see what services/applications and companies are using each specific personal data concept, e.g., their address or their age.

In summary, the data governance framework allows users to:

1) monitor which data are available and how they are used or how it has been accessed,
2) to control: add, delete or change data, provide or block access to public bodies (where permitted or enforced by the law) businesses or data brokers, giving individuals the power to determine how their data can be used.

Next section provides an overview of the main concepts related to the personal data management.

2.1 Personal data management related concepts

Next, some important concepts regarding personal data management are defined. To have a clear understanding of this concepts is paramount to use the Data governance framework.

2.1.1 Personal data

The European Commission[5] defines personal data as "any information about an identified or identifiable personal, also known as the **data subject"**. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. Even personal data that has

[5] https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data and falls within the scope of the General Data Protection Regulation (GDPR).

Personal data includes information such as their:

- name
- address
- ID card/passport number
- income
- cultural profile
- Internet Protocol (IP) address
- data held by a hospital or doctor (which uniquely identifies a person for health purpose s).

Certain types of sensitive personal data are subject to additional protection under the GDPR. These are listed under Article 9 of the GDPR as "**special categories**" of personal data. The special categories are:

1. Personal data revealing racial or ethnic origin.
2. Political opinions.
3. Religious or philosophical beliefs.
4. Trade union membership.
5. Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.
6. Data concerning health.
7. Data concerning a natural person's sex life or sexual orientation.
8. Personal data related to criminal convictions and offences unless this is authorised by EU or national law

Processing of these special categories is prohibited, except in limited circumstances.

In order to homogenise the personal data models, the ACROSS Personal Data Framework will use the personal data model defined on DPV-PD: Extended Personal Data categories for DPV [6] taxonomy and classes.

DPV provides broad top-level personal data categories adapted from the taxonomy contributed by EnterPrivacy[7]. The top-level concepts in this taxonomy refer to the nature of information (financial, social,

[6] DPV-PD: Extended Personal Data categories for DPV (w3c.github.io)

[7] https://enterprivacy.com/wp-content/uploads/2018/09/Categories-of-Personal-Information.pdf

tracking) and to its inherent source (internal, external). Each top-level concept is represented in the DPV vocabulary as a Class and is further elaborated by subclasses for referring to specific categories of information - such as preferences or demographics.

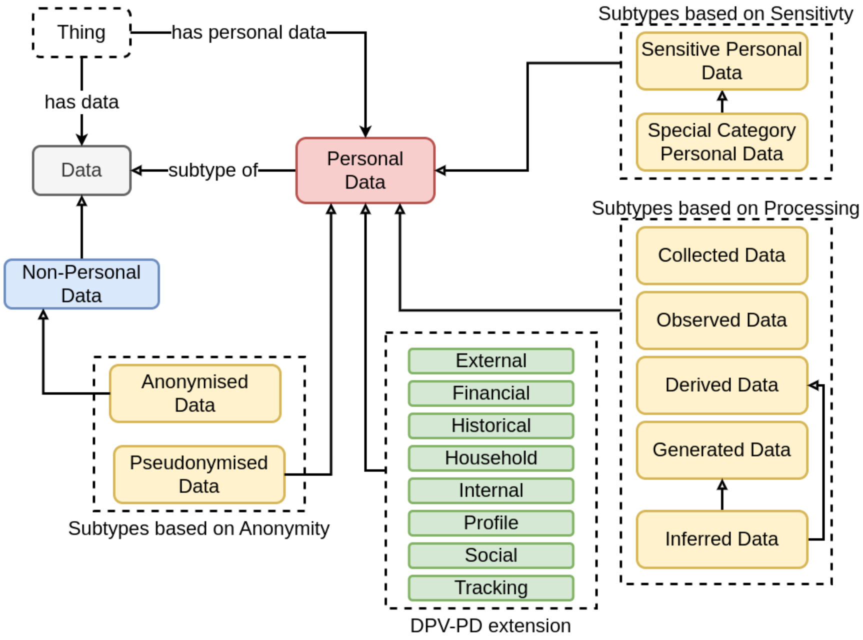


Figure 1 DPV taxonomy for personal data[8]

DPV's list of concepts is not universal nor exhaustive and includes 206 personal data concepts[9]. The ACROSS Data Governance Framework uses these concepts to describe the personal data used by the Services.

2.1.2 GDPR: General Data Protection Regulation

The GDPR is an EU data privacy law that went into effect May 25, 2018. It is designed to give individuals more control over how their data is collected, used, and protected online. It also binds organizations to strict new rules about using and securing the personal data they collect from people, including the mandatory use of technical safeguards like encryption and higher legal thresholds to justify data collection.

There are two main features of the GDPR the final user of the ACROSS data management framework must understand.

[8] https://enterprivacy.com/wp-content/uploads/2018/09/Categories-of-Personal-Information.pdf

[9] DPV-PD: Extended Personal Data categories for DPV (w3c.github.io)

- Explicit consent
- GDPR User rights

2.1.2.1 Explicit consent

According to de GDPR, a company using personal data need to have a “legal base”. DPV[10] provides the following categories of legal bases based on GDPR Article 6: **consent of the data subject**, contract, compliance with legal obligation, protecting vital interests of individuals, legitimate interests, public interest, and official authorities.

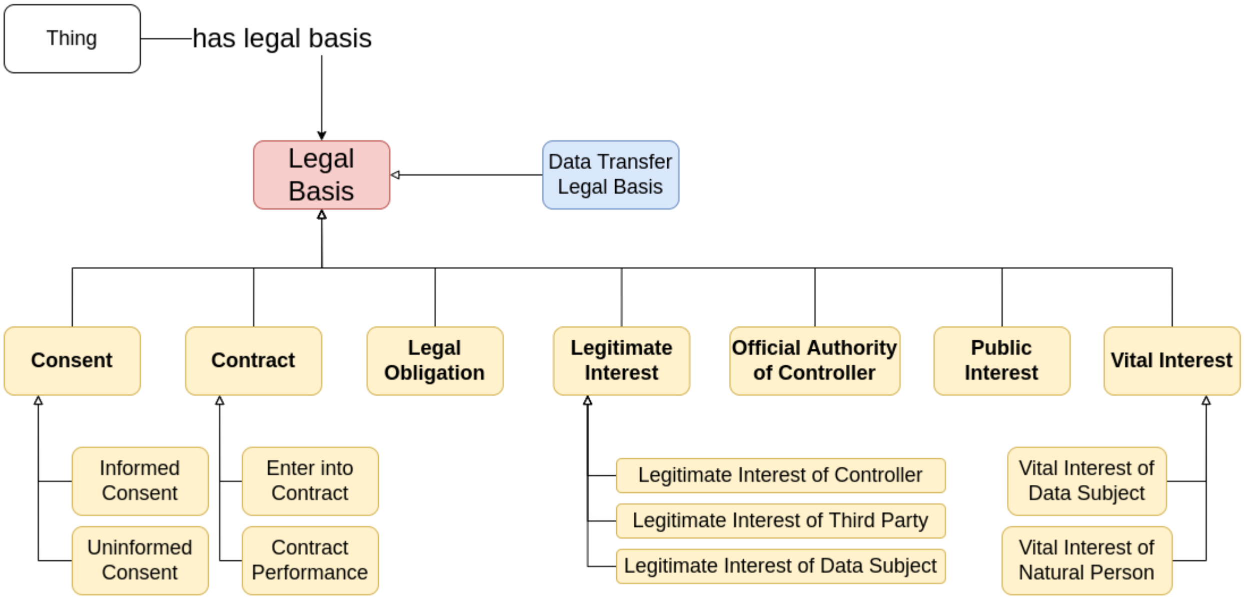

Thing
has legal basis
Legal Basis
Data Transfer Legal Basis
Consent
Contract
Legal Obligation
Legitimate Interest
Official Authority of Controller
Public Interest
Vital Interest
Informed Consent
Uninformed Consent
Enter into Contract
Contract Performance
Legitimate Interest of Controller
Legitimate Interest of Third Party
Legitimate Interest of Data Subject
Vital Interest of Data Subject
Vital Interest of Natural Person

Figure 2 Overview of Legal Basis concepts in DPV

The ACROSS Personal Data Framework provide the individual the means to manage Consents, so that public bodies, businesses or data brokers are able to get explicit consent to use the personal data of an individual. Section 2.1.4 elaborates more on the concept of consent and how it is used by the ACROSS data governance framework.

2.1.2.2 GDPR User rights

GDPR provides several rights to the data subject, whose applicability depends on the context and nature of processing taking place. DPV lists these rights at an abstract level as concepts along with their origin in specific clauses of the GDPR. The following list provides information about the user rights along with the way in which the Personal Data Framework facilitates the exercise of the rights by the individual.

[10] Primer (w3c.github.io)

- **information** about the processing of your personal data
  This information is included in the description of the service, although by now only one category of processing is included.
- **obtain access to** the personal data held about you.
  This right is not provided by the framework, but the email of the DPO is included in the service description so the user can write requesting the personal data the service provider holds.
- ask for incorrect, inaccurate or incomplete personal data to be **corrected**
  This right is not provided by the framework, but the email of the DPO is included in the service description so the user can request to exercise this right.
- request that personal **data be erased** when it's no longer needed or if processing it is unlawful
  This right is not provided by the framework, but the email of the DPO is included in the service description so the user can write requesting the personal data the service provider holds.
- **object** to the processing of your personal data for marketing purposes or on grounds relating to your particular situation
  The user can reject the consent if the processing of the personal data includes some specific purpose. Another way is by writing an email to the DPO.
- request the **restriction** of the processing of your personal data in specific cases.
  This right is not provided by the framework, but the email of the DPO is included in the service description so the user can request to exercise this right.
- receive your personal data in a machine-readable format and send it to another controller ('**data portability**')
  This right is not provided by the framework, but the email of the DPO is included in the service description so the user can request to exercise this right.
- request that decisions based on **automated processing** concerning you or significantly affecting you and based on your personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision.
  This right is not provided by the framework, but the email of the DPO is included in the service description so the user can request to exercise this right.

2.1.3 Services

The ACROSS Data Governance Framework uses the concept of service in a broad sense to refer to the services offered by a company to the user. Therefore, the user is able to give the consent to use personal data to each specific service.

The whole list of services available are managed by an external application, the Service Catalogue. In order to register a service in the Service Catalogue the service provider has to introduce the information described in the CPSV-AP[11] standard with some extensions.

CPSV-AP captures fundamental characteristics of a service, such as the name, description, organisation, output, etc. Public administrations and service providers can therefore use this approach to describe their services and guarantee a level of cross-domain and cross-border interoperability at European, national and local level.

In the context of the Personal Data Management Framework the main information provided to the final user to support the process of definition of the consent is:

- **Personal data** requested by the services in two categories:
  - **Mandatory**: Information necessary to offer the service.
  - **Optional**: Additional information that can be used to improve the service, for example offering a greater degree of personalization
- **Organization** which provides the service.
- **Purpose**: represent the *reason* or *justification* for processing of personal data. Purposes are organised within DPV[12] based on how they relate to the processing of personal data in terms of several factors, such as: management functions related to information (e.g., records, account, finance), fulfilment of objectives (e.g., delivery of goods), providing goods and services (e.g. service provision), intended benefits (e.g. optimisations for service provider or consume r), and legal compliance. However, according to the DPV purposes do not have a strict structure as used in real-world use-cases, it is important to note the following for real-world implications of Purpose:
  - There is no universal definition for what constitutes a ’purpose’ or what attributes are associated with it.
  - There are several distinct ways to model purposes, e.g., as a ‘goal’ such as ‘Delivery of Ordered Goods’; or as a statement explaining the processing of personal data, e.g., ‘Sending newsletters to email’.
  - DPV does not define requirements for what is a ‘valid purpose’ as these are defined externally, e.g. in laws such as [GDPR] Article.5-1b where purposes are required to be ‘explicit and legitimate’.

[11] About Core Public Service Vocabulary Application Profile | Joinup (europa.eu)
[12] Primer (w3c.github.io)

  - Purposes have contextual interpretations within their application and domains i.e., depending on how they are used in an use-case). For example, ServiceProvision is interpreted distinctly across the use-cases of an online website, a goods delivery outlet, and a medical centre - even if they use the same term or wording.

  Following from the above, most use-cases would need to extend one of the concepts within DPV's purpose taxonomy to ensure its purpose descriptions are specific and understandable within the context of that use-case. Therefore, DVP suggest, where possible and appropriate, to create a customised purpose as required within the use-cases by extending or subtyping one or several purposes from the DPV taxonomy and to provide a human readable description to assist in its accurate interpretation. Following this recommendation, ACROSS have defined a restricted set of purposes, closer to the real-world use of terms.

- **Processing**: DPV's taxonomy of processing concepts reflects the variety of terms used to denote processing activities or operations involving personal data, such as those from GDPR Article.4-2 definition of processing. Real-world use of terms associated with processing rarely uses this same wording or terms, except in cases of specific domains and in legal documentation. On the other hand, common terms associated with processing are generally restricted to: collect, use, store, share, and delete. DPV provides a taxonomy that aligns both the legal terminologies such as those defined by GDPR with those commonly used. In ACROSS, only the common terms are use d, so that it facilitates the usability from the final user point of view.

2.1.4 Consent

Consent is an important legal basis given its emphasis on individual empowerment and control, as well as the attention and relevance it receives from being part of direct interactions with individuals. In order to facilitate the definition of consents, the consent model used includes only the following information:

- **User Id**: The identifier of the user in the personal data framework
- **Service Id**: The identifier of the service in the service catalogue
- **Personal data permissions** for each personal data category needed by the service, both required and optional
- **Status of the service**: It can be Granted, Denied or Withdrawn (See more information in section 2.2)

2.1.5 Data usage policies

ACROSS data governance framework focuses on permission management, providing a way for people to define the specific data that can be shared (or disclosed) between parties, for which purposes, and for how long. Furthermore, it will go beyond basic permission management including the possibility to define data usage policies for more fine-grained usage control. In general, the overall goal is to enforce usage restrictions for data after access has been granted.

A data usage policy could be used to constraint the location in which data is used, to enforce the deletion of the personal data after a specific period or to modify the personal during the data transfer process.

In fact, some of the defined data usage policies can be used to enforce the some GDPR rights and principles. For example, the rule that allows to modify the data in transit could be used to ensure the data minimization principle.

The complete data usage policy enforcement functionality is performed by a specific software (the IDS connectors) and some of the rules can only be applied by the consumer connector, so it can be used only if the services (both public and private services) deploy the IDS connectors technology for data transfer.

However, the ACROSS personal data government framework strategy is to minimize the service providers adaptation needed to use the framework and it will assume the responsibility of performing data usage policies management and enforcement. Therefore, not real “data usage control” can be applied, only a restricted set of data usage policies providing data access rules. Each service is associated with a data usage policy that can be composed by one or several policy rules.

The following rules can be used:

- **N times usage**: This policy rule restricts the numeric count of using your data by a specified data consumer (provider side). The number of times used is updated and consulted via an external end point.
- **Duration usage**: allows data usage for a specified time period. For example, an instantiated policy from this policy class may allow a Data Consumer to use the data for a duration of three months. The permitted period may start from a given date and time.
- **Usage during interval:** This policy rule provides data usage within a specified time interval (start + end date)

Other rules that can only be enforced by the service provider receiving the pe rsonal data have not been implemented, specifically the Role-restricted Data Usage and Purpose-restricted Data Usage rules.

The following management functionalities are provided for the end user:

- Data usage policies browsing and filtering
- Data usage policy create/modify/delete functionalities

2.2 End users workflow

2.2.1 Data governance framework scenario description

This section describes the workflow the users must follow to use final implementation of the ACROSS Data Governance framework for data sovereignty. Three types of users are envisaged: Administrator, End User (Citizen) and Service provider.

1. **Administrator:** Users management. Register and manage new users including end users and services providers. This functionality is provided by the external security package.
2. **Service provider:** Service description and registration. Each service provider has to register the services using the CSPV-AP extended model.
3. **End User:** The ACROSS Personal data framework facilitates the individual to perform the end-to-end process of consent management. In order to use all the functionalities, a workflow has been designed and consists of the following steps:
    a. Select services→ Select the services the user is going to use.
    b. Consent Management→ Define the personal data to be used by each selected service.
    c. Data Usage policies management→ Define the data usage policies applicable the data to be used by each service. This is an optional step.
    d. Monitor the data usage for each service
    e. Monitor the services using a specific personal data category

Next table summarizes the functionalities covered by each step.

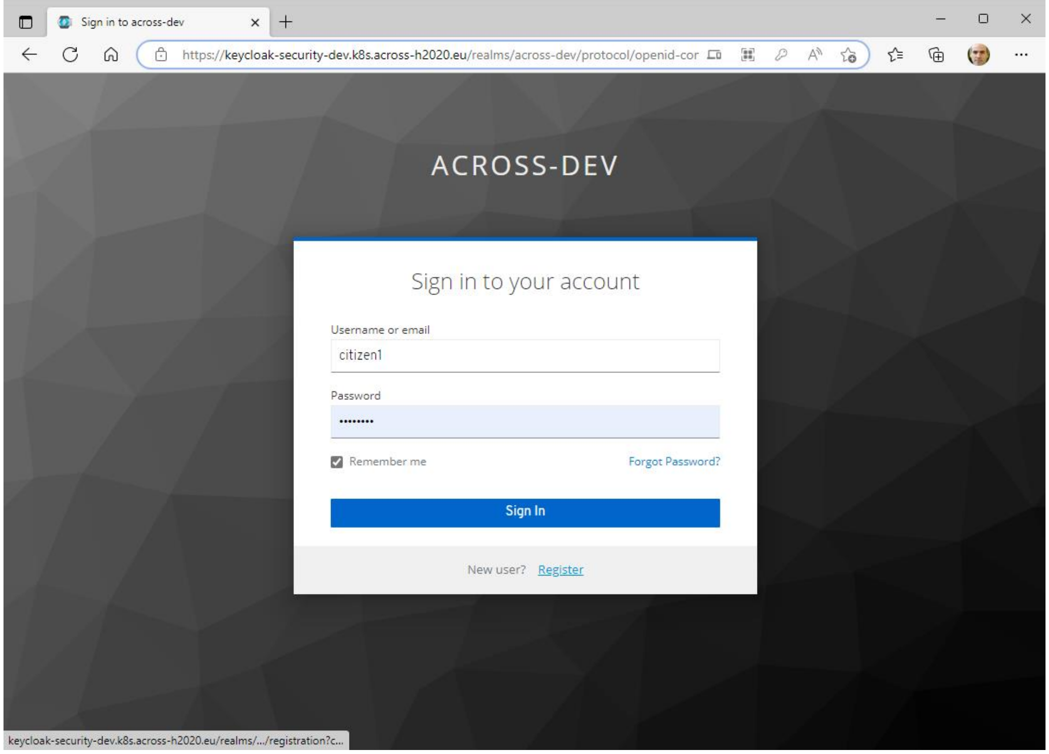
Table 1 ACROSS workflow

Step	Functionality
Service description and registration	This is an initial step covered by the services catalogue and it is the responsibility of the service providers. The service model is the CPSV-AP extended with: • personal data related data model: Purpose and processing • Information about Personal data needed by the service, including optional data. • Information about the REST service channel if available.
Login	End User logged in the ACROSS Personal data governance framework. The registration process is made in the KeyCloak external system by the data

	governance framework administrator. Self-registration has not been implemented.
Service Selection	Using the Services window, the user selects the services to be used among the whole list of services registered in the catalogue. Consents and data usage policies can be defined and assigned only to previously selected services.
Consent management	For each selected service the user can create a consent that define the personal data categories that can be shared. All the mandatory personal data categories must be allowed to use the service. For each Consent the end User can change the **Status** of the relative Consent: - **Grant**: Enables a new consent or a previously denied Consent - **Deny**: disable the Consent - **Withdraw**: revoke the Consent, a new one must be given by the Consenting phase.
Data Usage policies management	For each selected service the user can define a data usage policy composed by one or more policy rules that restricts the access to personal in a more fine-grained way.
Monitor data usage notifications and Activity Logs	Once the user has defined the applicable consents and data usage policies (optional), all the data transfers among services are tracked by the ACROSS data governance framework as Event Logs that can be viewed both by the Data Subject (via the Transparency dashboard) and by the Service Provider (via the Service Catalogue user interface). Furthermore, all the interactions of the user with the Transparency dashboard are logged, so that the user is able to consult them.

2.3 Transparency dashboard user guide

The Transparency dashboard is the Web portal for End Users (acting as Data Subjects) to manage the Services they use and their related consents and get an overview of what is happening with their Personal Data. Next figure shows the main login window. The user registration is done previously by the Data Governance Framework administrator.



Sign in to across-dev

https://keycloak-security-dev.k8s.across-h2020.eu/realms/across-dev/protocol/openid-cor

Username or email: citizen1

Password: ••••••••

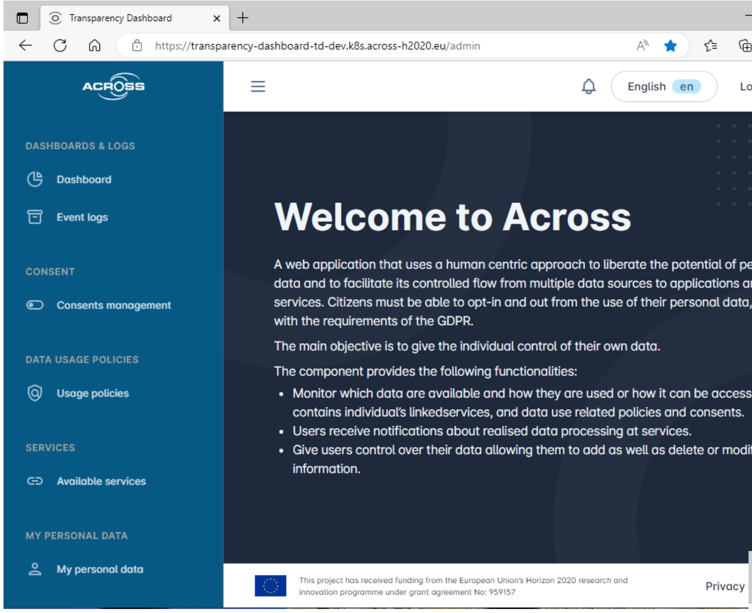
☑ Remember me

keycloak-security-dev.k8s.across-h2020.eu/realms/.../registration?c...

Figure 3 Login window

Next figure shows the Data Governance framework main window. The main page structure is common for all pages:

- Left frame with the vertical menu to access the framework functions
- The page header providing access to notifications, language selection and logout.
- A central frame which provides the interface for each functionality. In all the windows a new “information” icon has been included with detailed information about the interface.
- The page footer allows the user to access the Privacy policy of the Data Governance Framework



Welcome to Across

A web application that uses a human centric approach to liberate the potential of personal data and to facilitate its controlled flow from multiple data sources to applications and services. Citizens must be able to opt-in and out from the use of their personal data, in line with the requirements of the GDPR.

The main objective is to give the individual control of their own data.

The component provides the following functionalities:

- Monitor which data are available and how they are used or how it can be accessed. It contains individual's linkedservices, and data use related policies and consents.
- Users receive notifications about realised data processing at services.
- Give users control over their data allowing them to add as well as delete or modify information.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: 959157

Figure 4 Transparency dashboard main window

The end user by interacting with the Transparency Dashboard, will be able to:

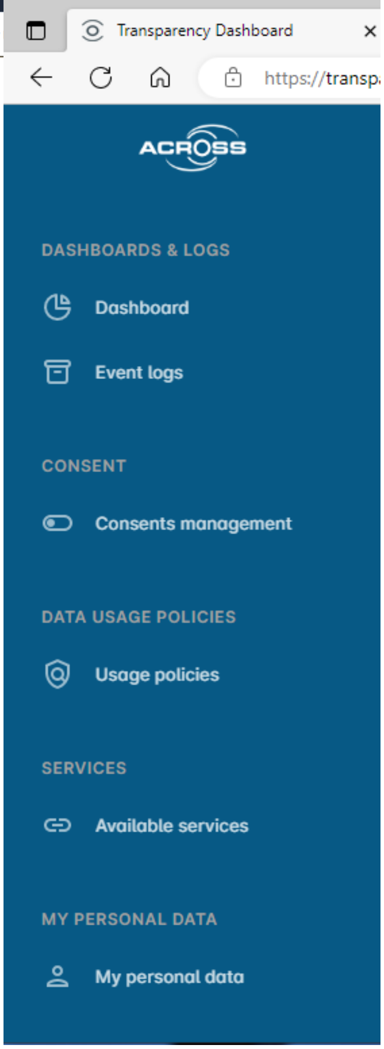
Monitor the personal data being processed

Get an overview and manage the lifecycle of consents

Get an overview and manage the lifecycle of data usage policies

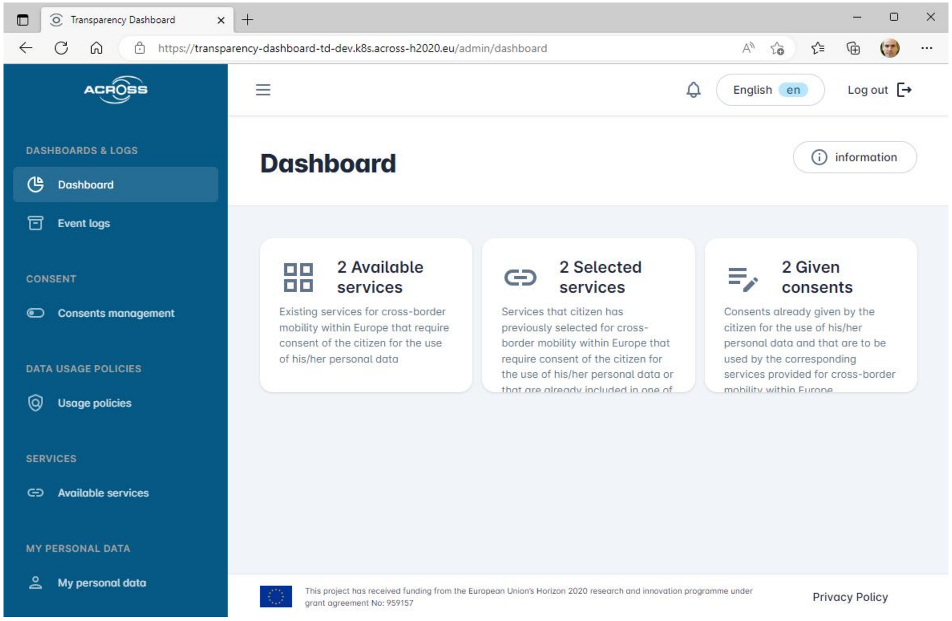
Get an overview and manage the selected services

Get an overview of where each category of personal data is processed



2.3.1 Dashboard

In the Dashboard section (image below), the Transparency dashboard provides to the Data Subject an overview of the available, the selected services and given consents.



Dashboard

2 Available services
Existing services for cross-border mobility within Europe that require consent of the citizen for the use of his/her personal data

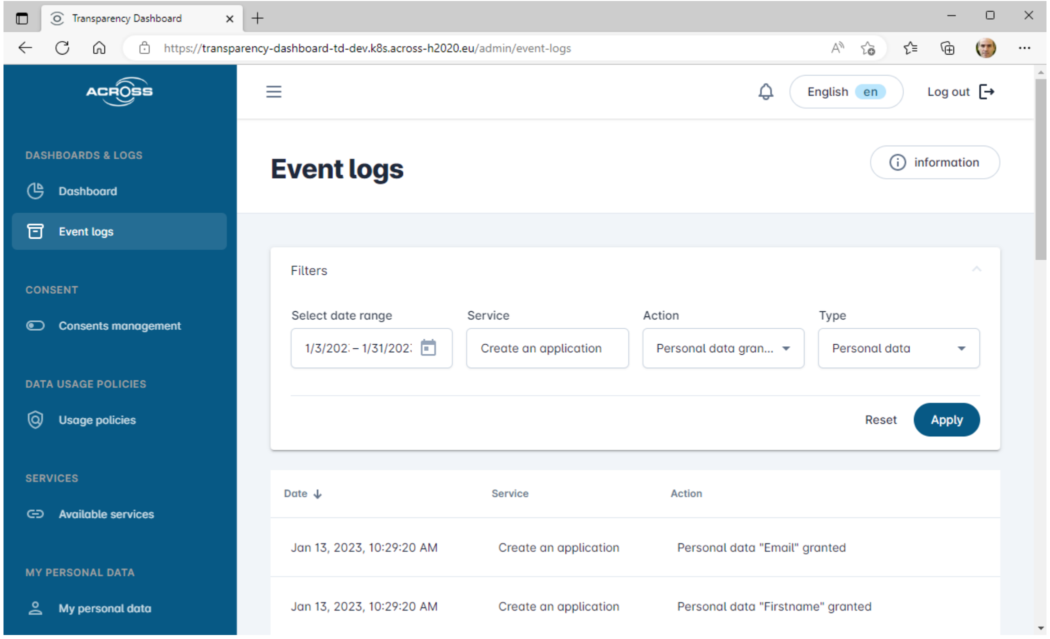
2 Selected services
Services that citizen has previously selected for cross-border mobility within Europe that require consent of the citizen for the use of his/her personal data or that are already included in one of

2 Given consents
Consents already given by the citizen for the use of his/her personal data and that are to be used by the corresponding services provided for cross-border mobility within Europe

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: 959157

2.3.2 Event logs

The event log window



Event logs

Filters

Select date range: 1/3/202: – 1/31/202:

Service: Create an application

Action: Personal data gran...

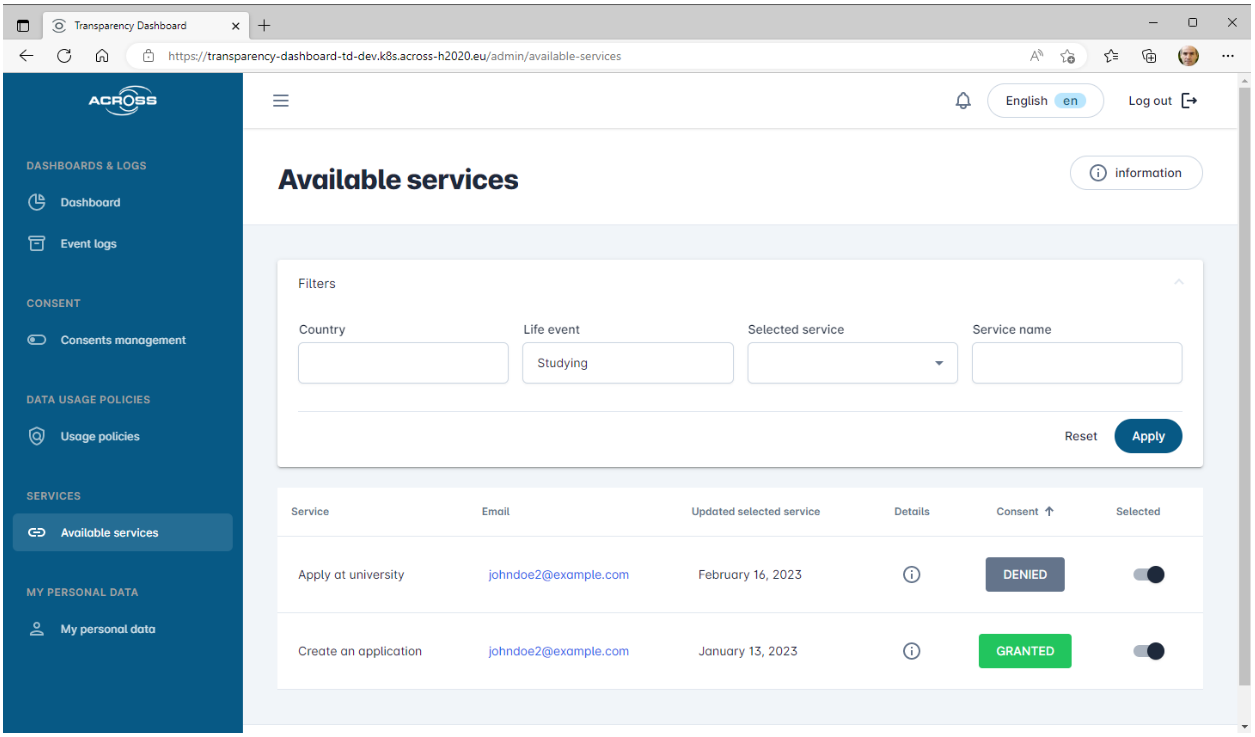
Type: Personal data

Date ↓	Service	Action
Jan 13, 2023, 10:29:20 AM	Create an application	Personal data "Email" granted
Jan 13, 2023, 10:29:20 AM	Create an application	Personal data "Firstname" granted

2.3.3 Managing services

The available services window provides the list of services registered in the Service catalogue. The following management functionalities are provided:

- Services browsing and filtering
- View services detailed information
- Select/Unselect services



https://transparency-dashboard-td-dev.k8s.across-h2020.eu/admin/available-services

Available services

Country:
Life event: Studying
Selected service:
Service name:

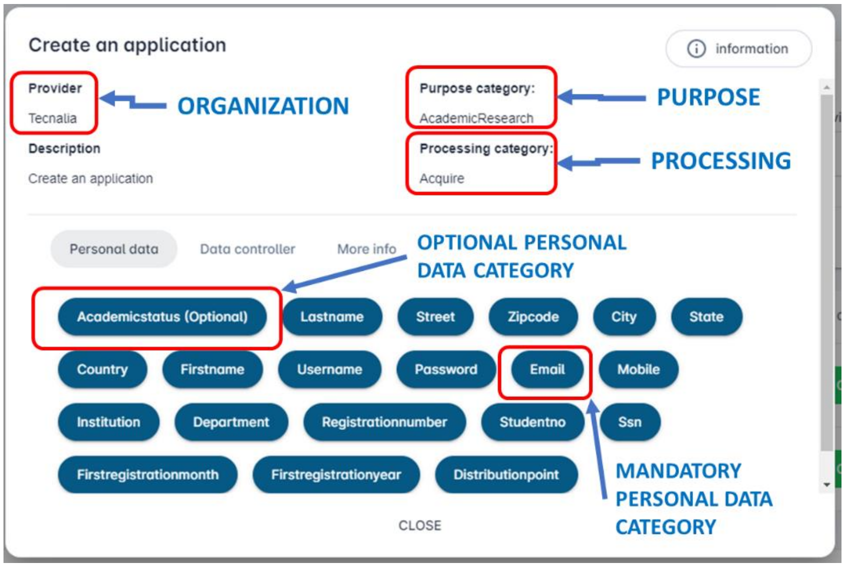
Service	Email	Updated selected service	Details	Consent ↑	Selected
Apply at university	johndoe2@example.com	February 16, 2023	ⓘ	DENIED	●
Create an application	johndoe2@example.com	January 13, 2023	ⓘ	GRANTED	●

This window allows the user to browse all the available services using a list format. For each service the following information is presented to the user: The service name, the email of the DPO of the service provider, date of the last service update, and the related consent status.

Service list can be filtered out by:

- Country
- Life event
- Selected services
- Service name

The user can also access more detailed information about the service and select/unselect services. Next figure provides an example of the window providing information about one specific service:



Create an application

Provider
Tecnalia

Description
Create an application

Purpose category:
AcademicResearch

Processing category:
Acquire

Figure 5 Service information window

This window also provides more detailed information about the service provider and the service characteristics via the “Data controller” and “More info” buttons.

2.3.4 Managing consents

The Consent management window provides access and management functionalities for the consents. The following management functionalities are provided:

- Consents browsing and filtering
- Consents create/delete functionalities
- Consents status management

This window allows the user to browse all the defined consents using a list format. For each service the following information is presented to the user:

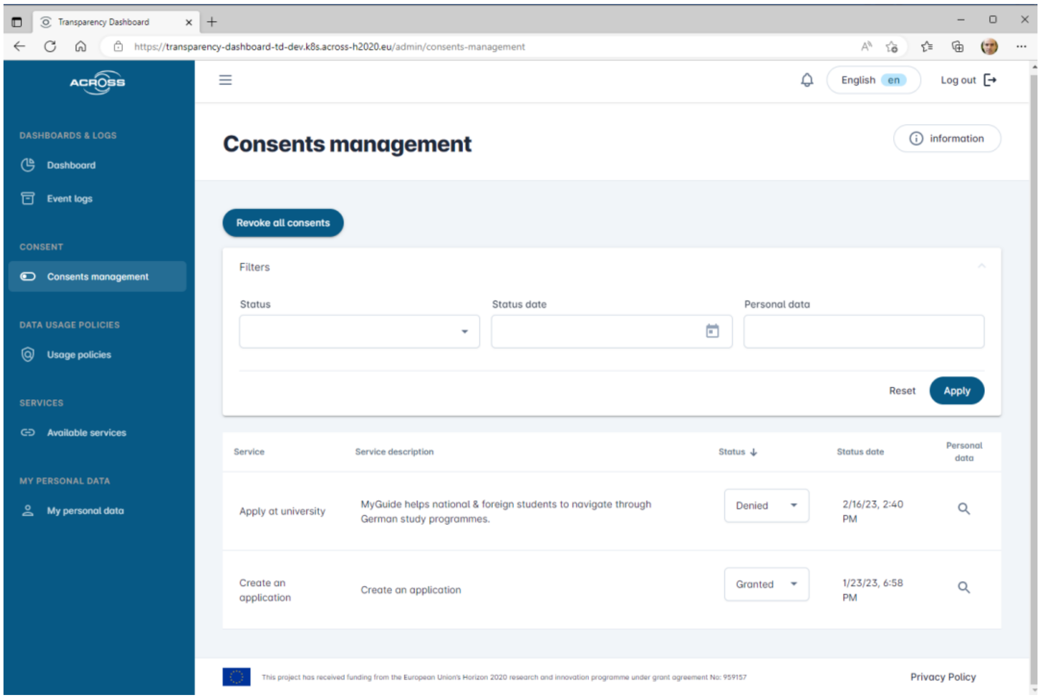
- The service name and description
- The status of the Consent and. The status of the consent can be changed
- The date of the last update of the consent
- A button to define the permissions for each personal data category requested by the service.

Consent list can be filtered out by:

- Status
- Status date

- Personal data category

Finally, a special button “Revoke all consents” is available to revoke all the consents.



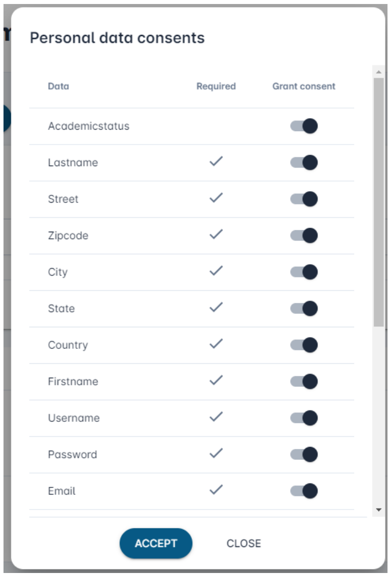
Consents management

Service	Service description	Status	Status date	Personal data
Apply at university	MyGuide helps national & foreign students to navigate through German study programmes.	Denied	2/16/23, 2:40 PM	🔍
Create an application	Create an application	Granted	1/23/23, 6:58 PM	🔍

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: 959157

Figure 6 Consent management window

Next figure shows the window to define the specific permissions for each personal data category requested by the service.



Personal data consents

Data	Required	Grant consent
Academicstatus		●
Lastname	✓	●
Street	✓	●
Zipcode	✓	●
City	✓	●
State	✓	●
Country	✓	●
Firstname	✓	●
Username	✓	●
Password	✓	●
Email	✓	●

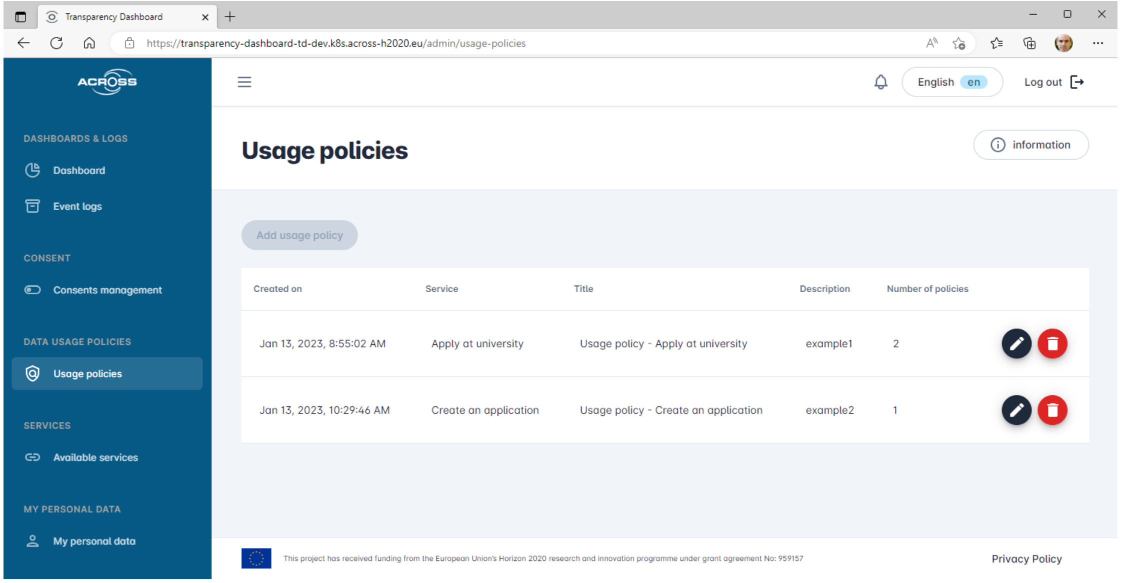
Figure 7 Personal data categories permissions associated to the consent

2.3.5 Managing data usage policies

The Policy templates window provides access and management functionalities for the data usage policies. The following management functionalities are provided:

- Data usage policies browsing
- Data usage policy create/modify/delete functionalities

Each service is associated with a data usage policy that can be composed by one or several policy rules.

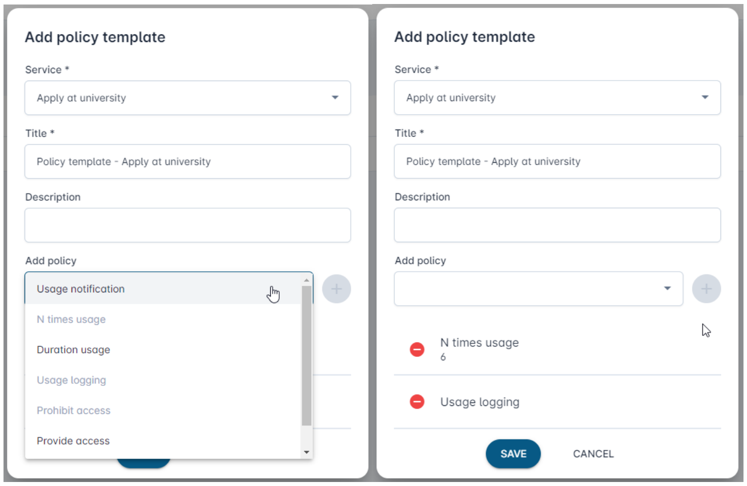


Usage policies

Created on	Service	Title	Description	Number of policies
Jan 13, 2023, 8:55:02 AM	Apply at university	Usage policy - Apply at university	example1	2
Jan 13, 2023, 10:29:46 AM	Create an application	Usage policy - Create an application	example2	1

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: 959157

Figure 8 Data usage policy browse window



Add policy template

Service *: Apply at university

Title *: Policy template - Apply at university

Description

Add policy: Usage notification

Add policy template

Service *: Apply at university

Title *: Policy template - Apply at university

Description

Add policy

N times usage
6

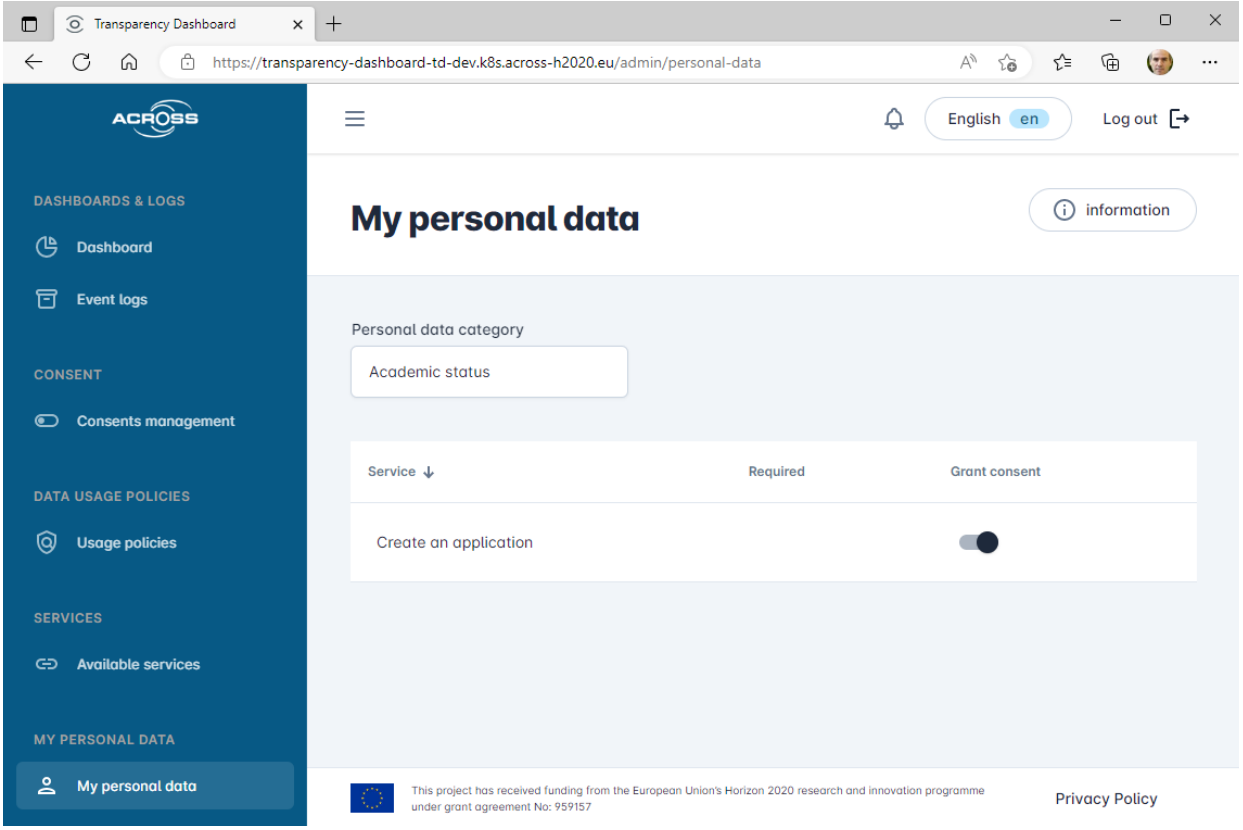
Usage logging

Figure 9 Add policy window examples: one policy composed by several policy rules

2.3.6 Managing personal data: My personal data view

This new functionality allows the user to view the list of services that are using a specific personal data concept. The framework will give the service provider a way to map its specific data model with the DPV Personal Data Categories data model. In this way, it would be possible to have a vision of where each type of data is being used in different services.

Next figures show the user interface of My Personal Data view. From this interface is possible to revoke or grant the consent to use a specific data category by a service.



https://transparency-dashboard-td-dev.k8s.across-h2020.eu/admin/personal-data

My personal data

Personal data category: Academic status

Service ↓	Required	Grant consent
Create an application		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: 959157

Figure 10 Personal data view interface: list of services using the "Academic status" personal data category

In this example the "Academic Status" personal data category is requested by "Create an application" service but it is not mandatory, and the user has not granted its use in the consent.

Next window shows the interface to select a specific personal data category.

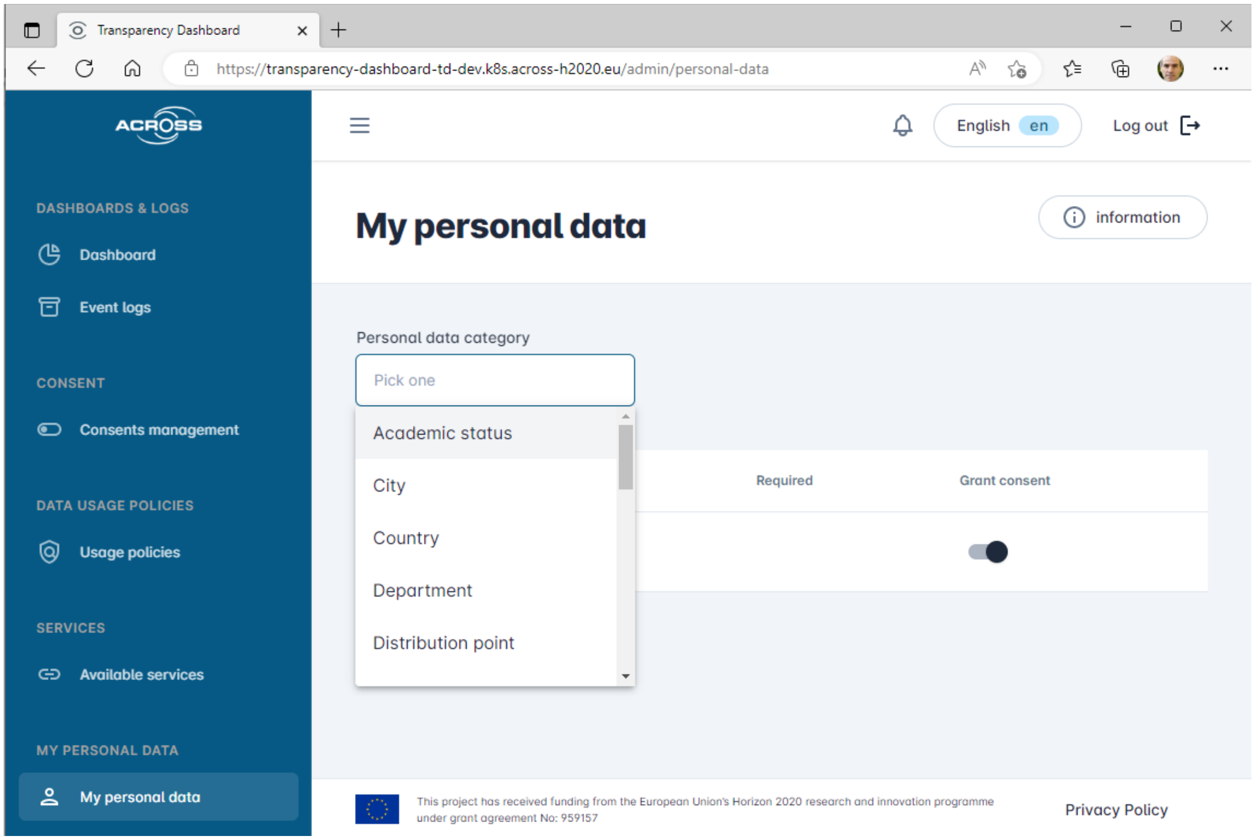


Figure 11 Personal data view interface: selecting a personal data category

3 ACROSS Data governance framework integration guide

The ACROSS Personal Data Governance Framework is part of the so-called ACROSS platform, useful in the context of cross-border public/private services for the citizens. However, it has been designed to be an independent framework useful also for the individuals to manage their personal data according to the GDPR in any other context.

Any application or service can interact with the Personal Data Governance Framework to ensure that it is using personal data in accordance with the permissions and restrictions set by the end user.

Next figure shows the whole ACROSS scenario with the main actors, components and interactions.

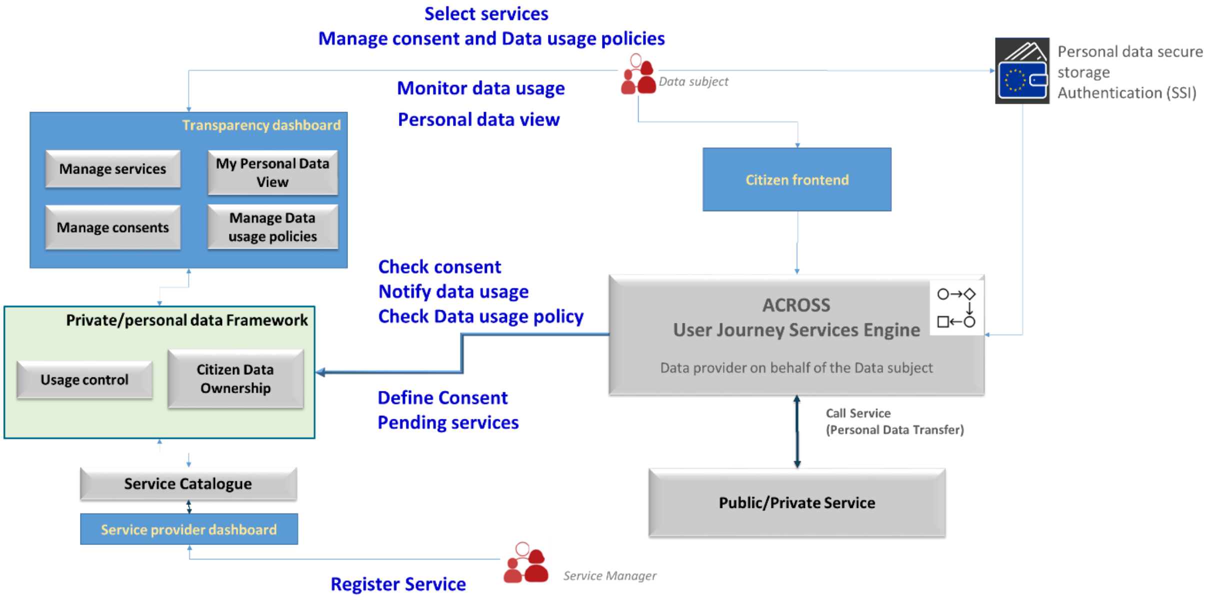


Figure 12 ACROSS Personal data governance framework scenario

The following logical interfaces have been defined:

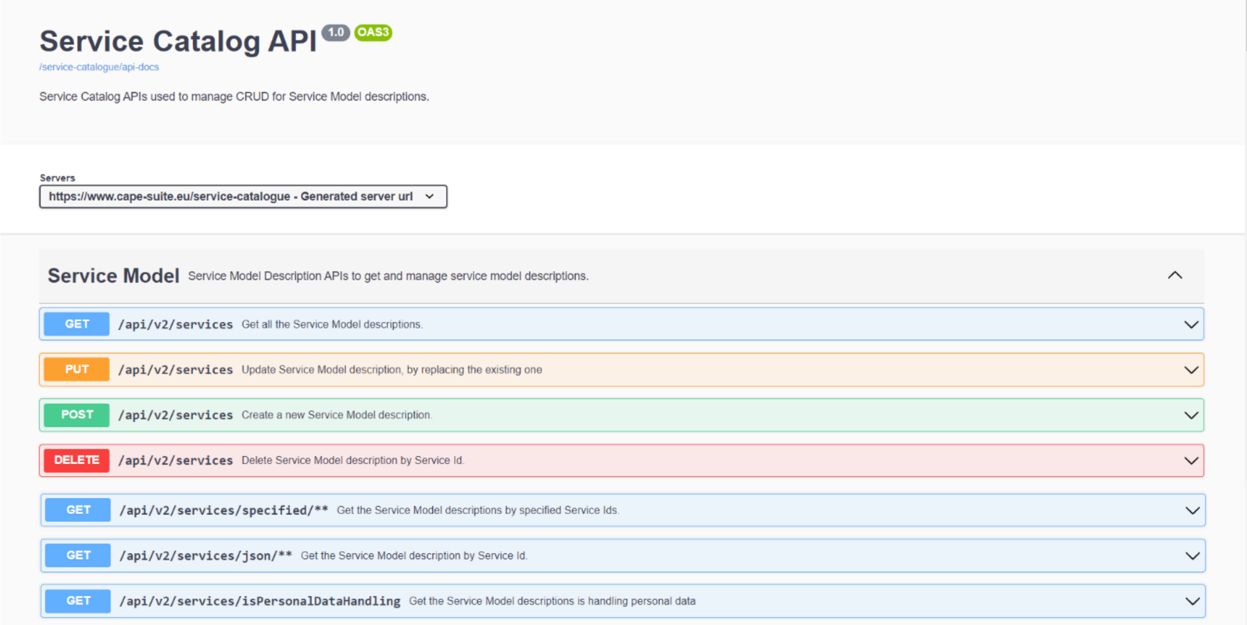
- **Register Service:** First, each service provider must register the services using the CSPV-AP extended model. This API is provided by the Service Catalogue, which is an independent module not included in the Data Governance Framework.
- **Check consent**: The UJSE request to check the permissions to use personal data of a specific user by a service.
- **Check Data usage policy**: The UJSE request to enforce the data usage policies defined by a user for a service.
- **Pending services**: The UJSE inform the framework about the services included in a new workflow.

- **Notify data usage**: Each time a service is used the UJSE notifies the Data Governance framework about the personal data usage for logging and audit functions.
- **Define consent**: If a service called by the UJSE doesn't have the consent to use the personal data, this interface gives the user the possibility of creating the consent directly from the USJE.

Keycloak will be used for Identity and Access Management instead of the SSI Authentication included in the figure.

3.1.1 Service Catalogue API used by the framework

The Service Catalogue API provides several REST services to register a new service and to get information about the service, e.g.: if it makes use of personal data, and which personal data it uses. Next figure shows the API used by the Data Governance framework to interact with the Service Catalogue. The complete Service Catalogue API is described in Swagger UI (cape-suite.eu)



Service Catalog API 1.0 OAS3

/service-catalogue/api-docs

Service Catalog APIs used to manage CRUD for Service Model descriptions.

Servers

https://www.cape-suite.eu/service-catalogue - Generated server url

Service Model Service Model Description APIs to get and manage service model descriptions.

GET /api/v2/services Get all the Service Model descriptions.

PUT /api/v2/services Update Service Model description, by replacing the existing one

POST /api/v2/services Create a new Service Model description.

DELETE /api/v2/services Delete Service Model description by Service Id.

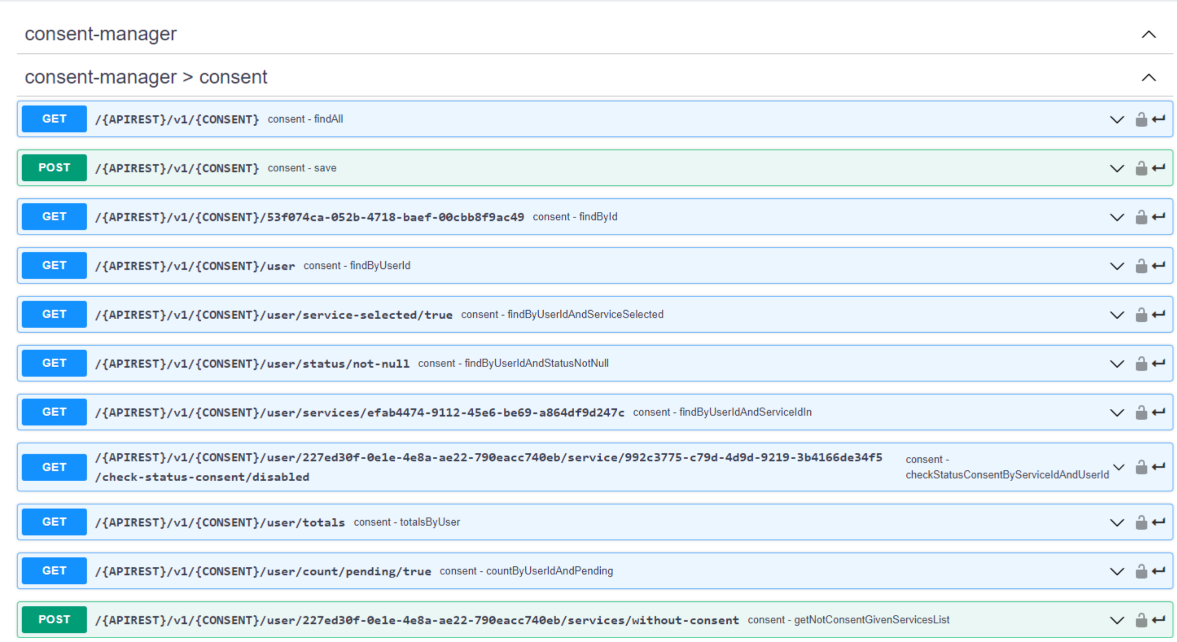
GET /api/v2/services/specified/** Get the Service Model descriptions by specified Service Ids.

GET /api/v2/services/json/** Get the Service Model description by Service Id.

GET /api/v2/services/isPersonalDataHandling Get the Service Model descriptions is handling personal data

3.1.2 Consent-manager > Consent: API to manage consents

The Consent Manager provides the following API to manage the consents, that is, to give, deny or withdraw consents and to get information about the consents already given, by different criteria.



consent-manager

consent-manager > consent

GET /{APIREST}/v1/{CONSENT} consent - findAll

POST /{APIREST}/v1/{CONSENT} consent - save

GET /{APIREST}/v1/{CONSENT}/53f074ca-052b-4718-baef-00cbb8f9ac49 consent - findById

GET /{APIREST}/v1/{CONSENT}/user consent - findByUserId

GET /{APIREST}/v1/{CONSENT}/user/service-selected/true consent - findByUserIdAndServiceSelected

GET /{APIREST}/v1/{CONSENT}/user/status/not-null consent - findByUserIdAndStatusNotNull

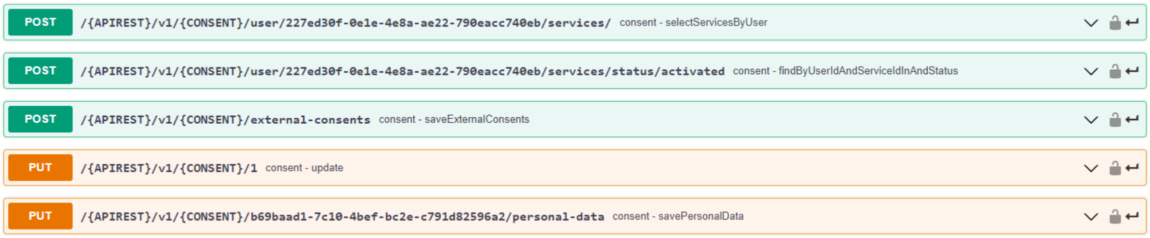
GET /{APIREST}/v1/{CONSENT}/user/services/efab4474-9112-45e6-be69-a864df9d247c consent - findByUserIdAndServiceIdIn

GET /{APIREST}/v1/{CONSENT}/user/227ed30f-0e1e-4e8a-ae22-790eacc740eb/service/992c3775-c79d-4d9d-9219-3b4166de34f5/check-status-consent/disabled consent - checkStatusConsentByServiceIdAndUserId

GET /{APIREST}/v1/{CONSENT}/user/totals consent - totalsByUser

GET /{APIREST}/v1/{CONSENT}/user/count/pending/true consent - countByUserIdAndPending

POST /{APIREST}/v1/{CONSENT}/user/227ed30f-0e1e-4e8a-ae22-790eacc740eb/services/without-consent consent - getNotConsentGivenServicesList



POST /{APIREST}/v1/{CONSENT}/user/227ed30f-0e1e-4e8a-ae22-790eacc740eb/services/ consent - selectServicesByUser

POST /{APIREST}/v1/{CONSENT}/user/227ed30f-0e1e-4e8a-ae22-790eacc740eb/services/status/activated consent - findByUserIdAndServiceIdInAndStatus

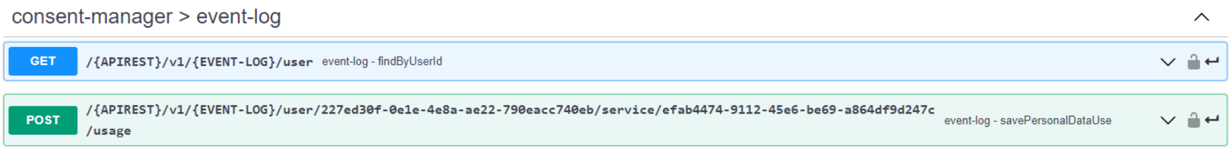
POST /{APIREST}/v1/{CONSENT}/external-consents consent - saveExternalConsents

PUT /{APIREST}/v1/{CONSENT}/1 consent - update

PUT /{APIREST}/v1/{CONSENT}/b69baad1-7c10-4bef-bc2e-c791d82596a2/personal-data consent - savePersonalData

3.1.3 Consent Manager > Event-log: API to manage event logs

The Consent Manager provides the following API to log events (applied actions on consents), and to retrieve those logs.



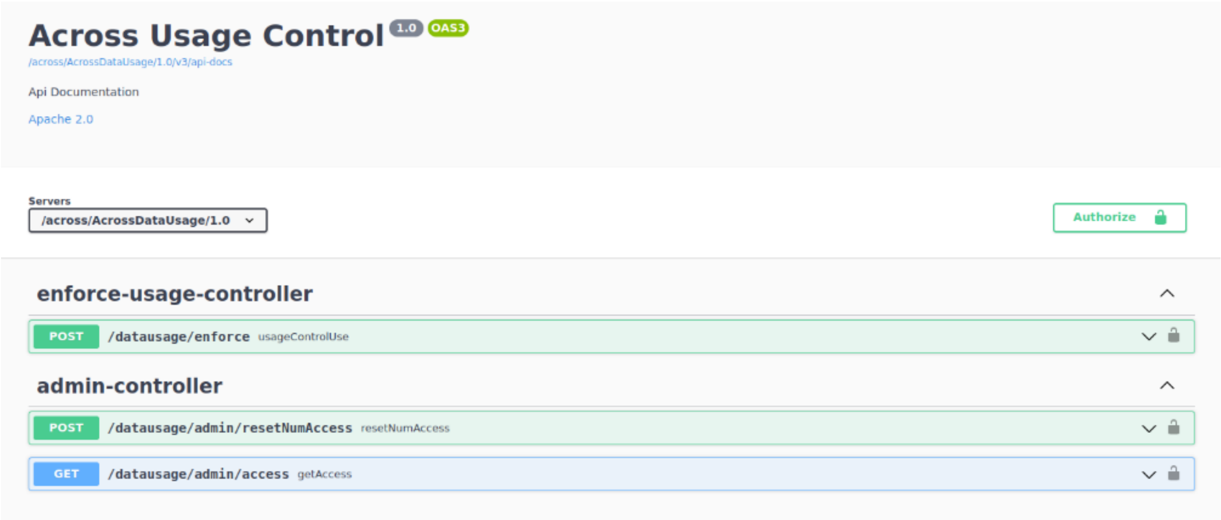
consent-manager > event-log

GET /{APIREST}/v1/{EVENT-LOG}/user event-log - findByUserId

POST /{APIREST}/v1/{EVENT-LOG}/user/227ed30f-0e1e-4e8a-ae22-790eacc740eb/service/efab4474-9112-45e6-be69-a864df9d247c/usage event-log - savePersonalDataUse

3.1.4 Usage Control > Enforcement API

The Usage Control component provides the enforcement mechanism to apply usage policies according to previously defined data usage policies. This enforcement can be invoked by the following API.



Across Usage Control 1.0 OAS3
/across/AcrossDataUsage/1.0/v3/api-docs

Api Documentation

Apache 2.0

Servers
/across/AcrossDataUsage/1.0

enforce-usage-controller

POST /datausage/enforce usageControlUse

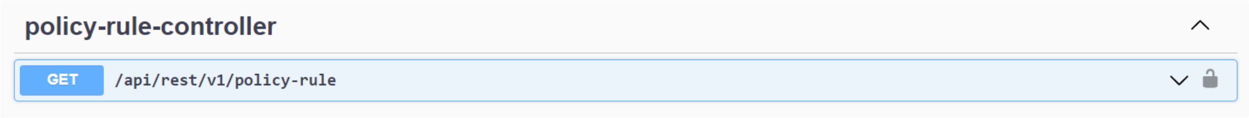
admin-controller

POST /datausage/admin/resetNumAccess resetNumAccess

GET /datausage/admin/access getAccess

3.1.5 Usage Control > Policy rules: API to retrieve supported policy rules

The Usage Control component provides the following API to retrieve the policy rules supported by the framework.

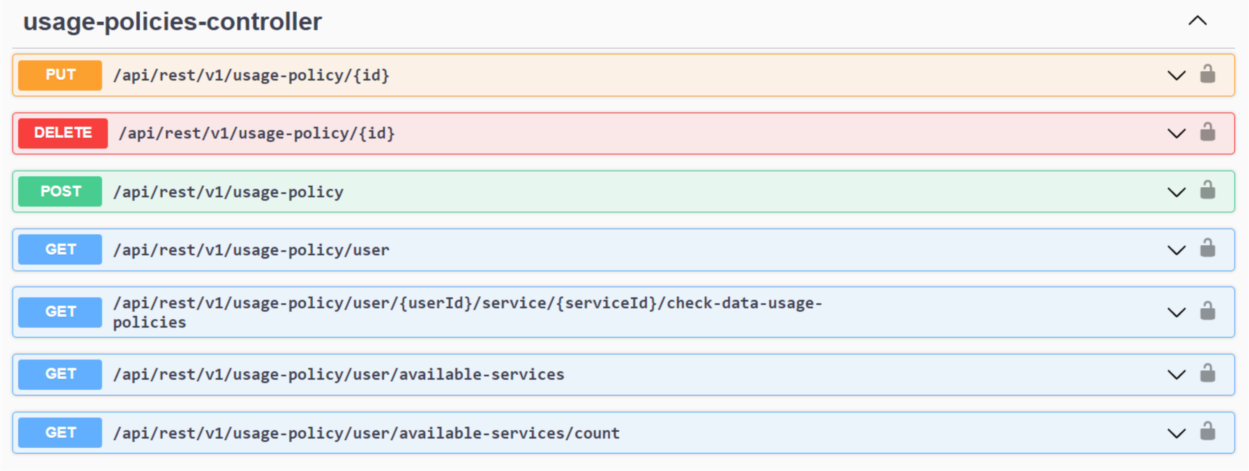


policy-rule-controller

GET /api/rest/v1/policy-rule

3.1.6 Usage Control > Policies: API for policies management

The Usage Control component provides the following API to manage the usage policies defined by the end user.



usage-policies-controller

PUT /api/rest/v1/usage-policy/{id}

DELETE /api/rest/v1/usage-policy/{id}

POST /api/rest/v1/usage-policy

GET /api/rest/v1/usage-policy/user

GET /api/rest/v1/usage-policy/user/{userId}/service/{serviceId}/check-data-usage-policies

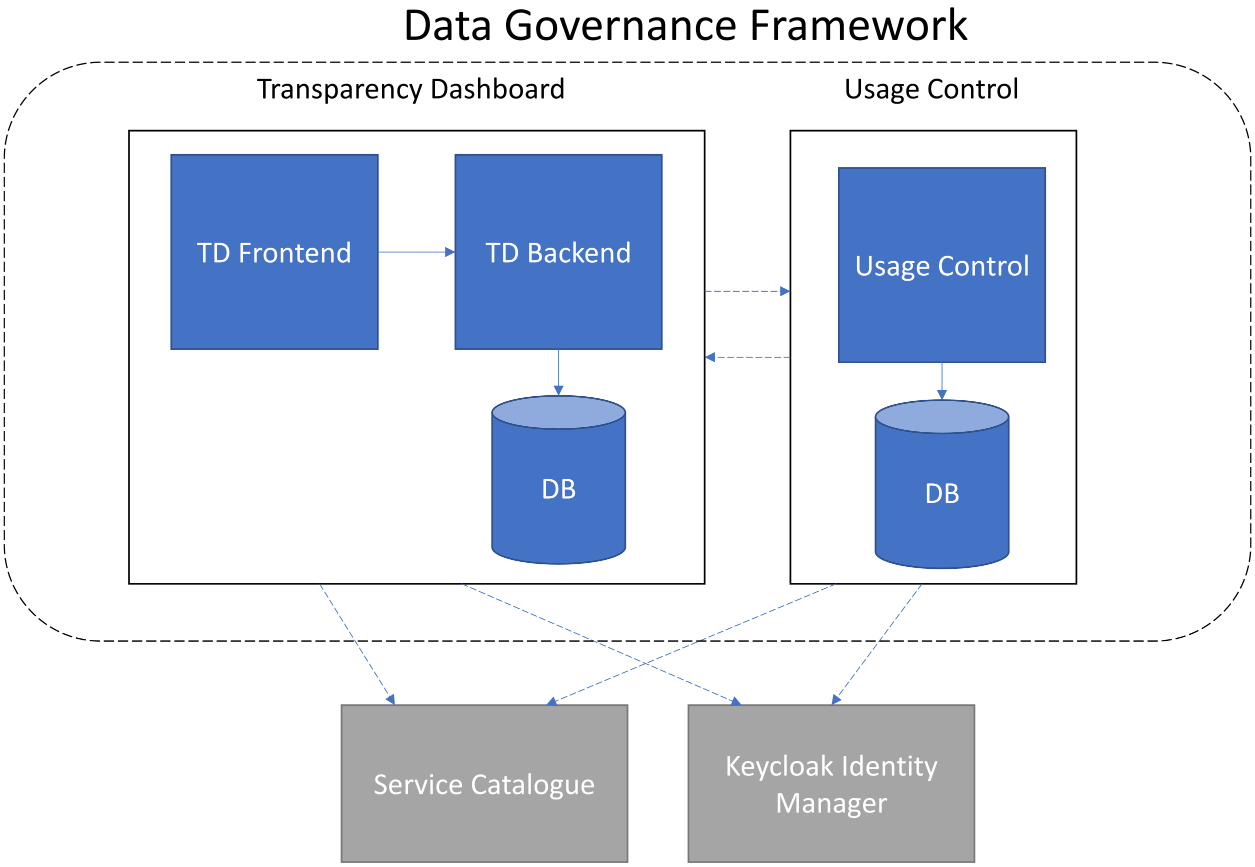
GET /api/rest/v1/usage-policy/user/available-services

GET /api/rest/v1/usage-policy/user/available-services/count

4 Installation manual

This section provides the description of the installation of the Data Governance framework.

The installation involves the deployment of several components that make up the Data Governance framework. The interaction among these components is shown in the following figure:



Moreover, these components communicate with the following external modules:

- Keycloak Identity Manager: used for end-user and software clients' authentication.
- Service Catalogue: to get information about the services.

Each of the components in the Data Governance Framework correspond to a docker container. These docker containers are the following:

- Transparency Dashboard component:
  - transparency_dashboard_frontend docker container

    - transparency_dashboard_backend docker container
    - MySQL database docker container
- Usage Control component:
    - Datausage docker container
    - PostgreSQL database docker container

The deployment process is explained in the following sections.

Next sections include some links to a private git repository, since the software is still in a development phase (intermediate version). The final version (D3.5 Implementation of the ACROSS Data Governance framework for data sovereignty – Final) will be published in a public repository as open source.

4.1 Configuring keycloak Identity and Access Manager

First of all a Keycloak server must be installed because the Data Governance framework components interact with the Keycloak Identity Manager. Specifically, the Open Id Connect protocol upon the OAuth2 Authentication will be used to authenticate the end users that access to the framework through the Transparency Dashboard Frontend, and to authenticate any software client that wants to use the API-s provided by the Transparency Dashboard Backend and the Usage Control component.

The following steps must be carried out to configure Keycloak:

- Create a realm called “across-dev”.
- Register 3 clients with the following client ID-s:
    - “transparency-dashboard-backend”:
        - Client protocol: openid-connect
        - Access type: bearer-only
        - Create a role inside the client called “citizen”.
    - “transparency-dashboard-frontend”:
        - Client protocol: openid-connect
        - Access type: public
        - Create a role inside the client called “citizen”.
    - “usagecontrol”:
        - Client protocol: openid-connect
        - Access type: bearer-only
        - Create a role inside the client called “citizen”.

- Create at least one user in this realm. E.g: "citizen1" and from the "Role Mappings" section, assign the following Client Roles to the user:
  - "transparency-dashboard-backend" client-> "citizen" Role
  - "transparency-dashboard-frontend" client-> "citizen" Role
  - "usagecontrol" client-> "citizen" Role

4.2 Installing Transparency Dashboard

The Transparency Dashboard consists of the following components/docker containers:

- MySQL database: this component is where all the information related to the consents is stored.
- Transparency Dashboard Backend: this component manages the process of giving/withdrawing consents and logging the activities related to the consents. It also receives notifications related to new services to be invoked by the end-user and it accesses the Service Catalogue to get the information of the personal data required by each service. This component is implemented as Spring Boot services.
- Transparency Dashboard Frontend: this component is the GUI for the end user to manage his consents and to check the actions he has carried out so far with his consents. This component is implemented with Fuse Angular.

These components are installed as docker containers, and the files to do this dockerization are located in the same GitLab repo where the source code is located, that is, at https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui . The dockerization is carried out using the following files:

- docker-compose.yml file located at https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui/-/blob/main/docker-compose.yml .
- mysql.env file to configure the database configuration parameters, and which is located at https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui/-/blob/main/mysql.env .
- transparency_dashboard_backend.env file to configure the Transparency Dashboard Backend (database connection string, Keycloak authorization and URL-s for accessing the Service Catalogue and the Usage Control component), and which is located at https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui/-/blob/main/transparency_dashboard_backend.env .

- environment.ts file that contains the URL-s of the Service Catalogue, Usage Control component and Keycloak, and which is located at https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui/-/blob/main/transparency_dashboard_frontend/environment.ts .
- Dockerfile of Transparency Dashboard Backend, located at https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui/-/blob/main/transparency_dashboard_backend/Dockerfile .
- Dockerfile of Transparency Dashboard Frontend, located at https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui/-/blob/main/transparency_dashboard_frontend/Dockerfile .

The following steps must be followed to install he Transparency Dashboard component:

- Install Git, if not installed in your system.
- Get the source code from the repository, by executing the following command at the command prompt:

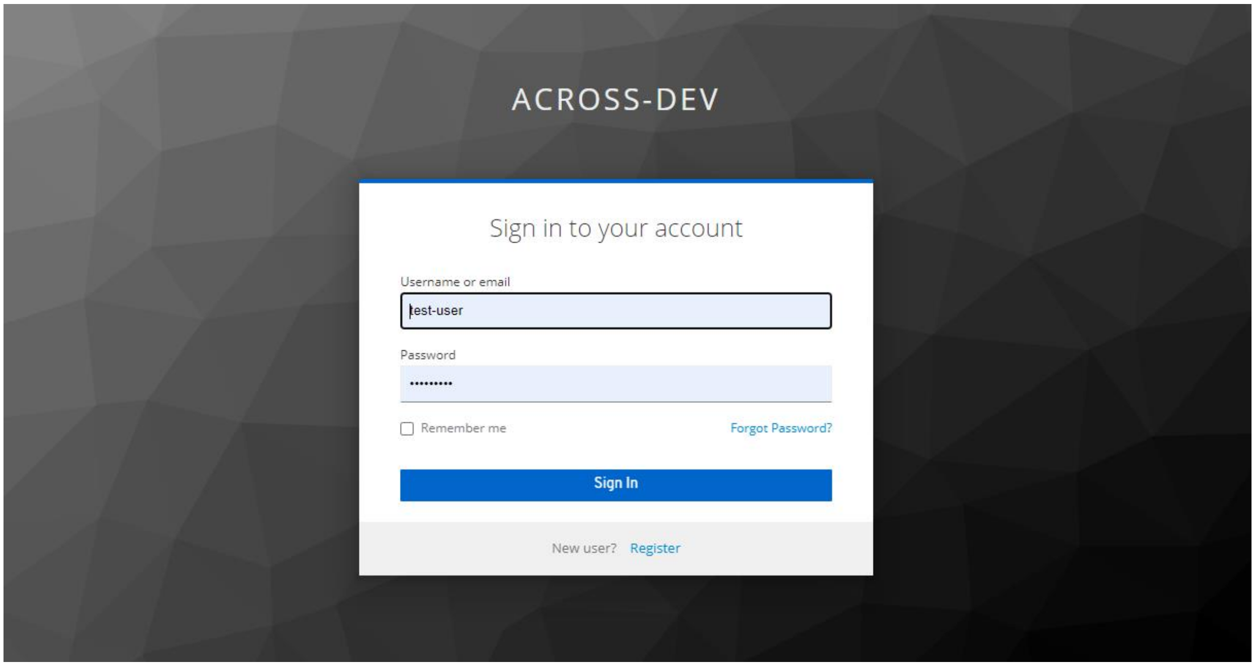
```
git clone https://git.code.tecnalia.com/across/private/citizen-front-end/transparency-dashboard/transparency-dashboard-ui.git

cd transparency-dashboard-ui
```

- Change, if required, the values of the following properties in “transparency_dashboard_backend.env” file, so that they point to the correct Keycloak Authentication Server used, the Usage Control component and the Service Catalogue:
  - SPRING_SECURITY_OAUTH2_RESOURCESERVER_JWT_ISSUER_URI=https://keycloak-security-dev.k8s.across-h2020.eu/realms/across-dev
  - KEYCLOAK_AUTH_SERVER_URL=https://keycloak-security-dev.k8s.across-h2020.eu
  - URL_DATA_USAGE=https://uc-dev.k8s.across-h2020.eu/across/AcrossDataUsage/1.0/
  - URL_SERVICE_CATALOG=https://service-catalogue-server-v1.k8s.across-h2020.eu/service-catalogue/api/v2/services
- Change, if required, the values of the following properties in “environment.ts” file located at the “transparency-dashboard-ui/transparency_dashboard_frontend” folder, so that they point to the correct Service Catalogue, Usage Control component, Transparency Dashboard Backend, and Keycloak Authentication Server:
  - publicServicesApiUrl: "https://service-catalogue-server-v1.k8s.across-h2020.eu/service-catalogue/api/v2/services"
  - dataUsageApiUrl:"https://uc-dev.k8s.across-h2020.eu/across/AcrossDataUsage/1.0"

  - ○ `consentManagementApiUrl: "https://transparency-dashboard-be-td-dev.k8s.across-h2020.eu"`
  - ○ `authApiUrl: "https://keycloak-security-dev.k8s.across-h2020.eu",`
  - ○ `keycloackUrl: "https://keycloak-security-dev.k8s.across-h2020.eu"`
- Install docker-compose software, if not installed in your system.
- Execute the following command at the command prompt to run the docker-compose file, which will bring up all the containers of the Transparency Dashboard:

```
docker-compose up -d
```

Now, every component of the Transparency Dashboard will be running. To access the frontend, write the following URL in a Web Navigator at the machine where the installation has been made: http://localhost:4200/admin.



ACROSS-DEV

Sign in to your account

Username or email: test-user

Password: ••••••••••

4.3 Installing Usage Control

The Usage Control consists of the following components/docker containers:

- PostgreSQL database: this component is where all the information related to the usage policies is stored.
- Datausage: this component offers an API to manage the usage policies defined by the end user to specify how his personal data can be used (time interval in which the data can be used, number of times the data can be used, etc.) and to do the enforcement of these usage policies. This component is implemented as Spring Boot services.

These components are installed as docker containers, and the files to do this dockerization are located in the same GitLab repo where the source code is located, that is, at https://git.code.tecnalia.com/across/private/citizen-data-ownership-and-usage-control/usage-control/usagecontrol . The dockerization is carried out using the following files:

- docker-compose.yml file located at https://git.code.tecnalia.com/across/private/citizen-data-ownership-and-usage-control/usage-control/usagecontrol/-/blob/main/docker-compose.yml .
- postgres.env file to configure the database configuration parameters, and which is located at https://git.code.tecnalia.com/across/private/citizen-data-ownership-and-usage-control/usage-control/usagecontrol/-/blob/main/postgres.env .
- datausage.env file to configure the Usage Control (database connection string, keycloak authorization and URL-s for accessing the Service Catalogue and the Transparency Dashboard Backend component), and which is located at https://git.code.tecnalia.com/across/private/citizen-data-ownership-and-usage-control/usage-control/usagecontrol/-/blob/main/datausage.env .
- Dockerfile of the Usage Control, located at https://git.code.tecnalia.com/across/private/citizen-data-ownership-and-usage-control/usage-control/usagecontrol/-/blob/main/Dockerfile .

The following steps must be followed to install he Usage Control component:

- Install Git, if not installed in your system.
- Get the source code from the repository, by executing the following command at the command prompt:

```
git clone https://git.code.tecnalia.com/across/private/citizen-data-ownership-and-usage-control/usage-control/usagecontrol.git

cd usagecontrol
```

- Change, if required, the values of the following properties in “datausage.env” file, so that they point to the correct Data Usage component, Transparency Dashboard Backend, Service Catalogue and Keycloak Authentication Server used:
    - URL_DATA_USAGE_PIP_ENDPOINT=https://uc-dev.k8s.across-h2020.eu/across/AcrossDataUsage/1.0/datausage/admin/access
    - URL_CONSENT_MANAGER=https://transparency-dashboard-be-td-dev.k8s.across-h2020.eu/api/rest/v1
    - URL_SERVICE_CATALOG=https://service-catalogue-server-v1.k8s.across-h2020.eu/service-catalogue/api/v2/services

  - `KEYCLOAK_AUTH_SERVER_URL=https://keycloak-security-dev.k8s.across-h2020.eu`
- Install docker-compose software, if not installed in your system.
- Execute the following command at the command prompt to run the docker-compose file, which will bring up all the containers of the Transparency Dashboard:

```
docker-compose up -d
```

Now, every component of the Usage Control will be running. To see the API offered by this component, write the following URL in a Web Navigator at the machine where the installation has been made: http://localhost:8080/across/AcrossDataUsage/1.0/swagger-ui/index.html?configUrl=/across/AcrossDataUsage/1.0/v3/api-docs/swagger-config .

5 Conclusions and next steps

ACROSS offers the citizen the possibility of defining which public and private organization will be allowed to *access which data and for what purpose* through the **ACROSS Data Governance Framework.** The main aim is to give the citizen the chance of **govern the access to** their data, profiting from a set of usage policies that implement levels of access and they can be the **sovereign owner** of such data.

The ACROSS Personal Data Governance Framework is part of the so-called ACROSS platform, useful in the context of cross-border public/private services for the citizens. However, it has been designed to be an independent framework useful also for the individuals to manage their personal data according to the GDPR in any other context.

ACROSS data governance framework does not cover the following functionalities included in other initiatives:

- Secure Data Storage and data minimization techniques: These will be provided by personal wallet technologies being developed by other projects.
- Secure Data transfer among services

Furthermore, ACROSS extends the MyData operator with data usage control based on data usage policies.

The **service catalogue** functionality is a fundamental part of the personal data framework, since it provides the list of services available to be used by the user, along with all the associated information. However, the catalogue has been designed and implemented as a separate module, so that the personal data framework is designed to be used with any available catalogue provided that it implements the services catalogue API defined by the framework.

The current version of Data Governance Framework already covers the whole set of required functionalities.

Therefore, the final version of the framework will focus on improving its usability and user experience. The following improvements have been envisaged based on the validation process by the pilots:

- Reorganization of the main menu to reflect the workflow associated with consent management
- Include help pages to describe the processes and concepts included in the consent management process
- Homogenize the user interface
- Facilitate the management of personal data consents while complying with the GDPR.

6 References

[1] D3.1Design of the ACROSS Data Governance framework for data sovereignty – Initial

[2] D3.3Implementation of the ACROSS Data Governance framework for data sovereignty – Initial

[3] D3.2Design of the ACROSS Data Governance framework for data sovereignty – Final

[4] D2.4 Report for cross-border service gap analysis – Final

[5] D6.2 Use case evaluation and impact assessment– Initial

[6] D5.2 System Architecture & Implementation Plan – Final