H2020-SC6-GOVERNANCE-2018-2019-2020

DT-GOVERNANCE-05-2018-2019-2020

D3.6 Legal requirements

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	D3.6 Legal requirements
Work package	WP3: ACROSS Data Governance framework
Nature	Report
Dissemination Level	Public
Date	30/07/2021
Status	Final
Editor(s)	Hans Graux (TLX)
Contributor(s)	-
Reviewer(s)	VARAM, GRNET/GFOSS
Document description	This deliverable details the legal requirements gathered directly from applicable legislation, which the consortium must take into account during the development of ACROSS results.

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. The project kicked off its activities in February 2021, with an energising online meeting, where all partners took the floor to present their plans to make the project a great success.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V0.1	26/07/2021	Initial draft	TLX
V1.0	30/07/2021	Final version	TLX

Executive Summary

This deliverable is drafted in the context of Work Package 3 (ACROSS Data Governance framework), notably Task 3.3 - Legal requirements for data governance and data sovereignty in cross border public services. This report aims to detail the legal requirements in relation to the ACROSS project and its general functional and infrastructural vision.

The legal requirements are gathered directly from applicable legislation, notably in relation to data protection (the GDPR and the e-Privacy Directive), e-government and the once-only principle (the Single Digital Gateway Regulation), and identification and authentication (the eIDAS Regulation). It also takes into account emerging legislation such as the proposed Data Governance Act, the proposed e-Privacy Regulation, the proposed eIDAS 2 Regulation, and the proposed Implementing Act for the Single Digital Gateway Regulation, in order to ensure future usability of ACROSS outcomes.

These legal frameworks are analysed in the present deliverable, including a short description of their scope and applicability to ACROSS, and the resulting compliance requirements during piloting and in the longer term.

The legal requirements are then assessed and tested against prior reference projects (MyData and DECODE), in order to identify which building blocks are available, and which modifications are required to ensure their fitness for purpose in the ACROSS project.

Finally, a series of legal compliance principles are posited, which the consortium must take into account during the development of ACROSS results. Compliance with these principles will be continuously monitored throughout the further activities of WP3, and all lessons learned and further implementing activities will be reported on in D3.7 - Legal report, due at the end of the ACROSS project.

Table of Content

List of Figures

List of Tables

List of Terms and Abbreviations

Abbreviation	Definition
ABC	Attribute Based Credentials
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EEA	European Economic Area, comprising all Member States, Iceland, Liechtenstein and Norway
eIDAS Regulation	Regulation on electronic identification and authentication services
GDPR	General Data Protection Regulation (EU) 2016/679
PET	Privacy Enhancing Technology
PIMS	Personal Information Management System
SDG	Single Digital Gateway
SDGR	Single Digital Gateway Regulation

1 Introduction

1.1 Purpose and Scope

In order to achieve the general vision of the ACROSS infrastructure, and particularly to ensure that the project results are usable in real life situations, it is important to ensure that legal requirements are identified at an early stage of the project, and to ensure that both the general architecture and its application to use cases complies with these requirements. For the avoidance of doubt, it should be noted that the piloting activities planned within ACROSS are realistic, but not real life: piloting shall be done through personas – realistic but fictitious use cases – so that noncompliance with legal requirements has no impact on real persons or real situations. Therefore, the project carries no legal consequences in case of noncompliance.

None the less, the objective of ACROSS is of course to facilitate the delivery of real life cross-border services ensuring data sovereignty, in a manner that can and should be used in operational environments by real persons in the future. For that reason, Work Package 3 (ACROSS Data Governance framework) comprises a specific Task 3.3 - Legal requirements for data governance and data sovereignty in cross border public services, in which the relevant legal frameworks are assessed, and legal requirements are identified.

This report therefore aims to detail the legal requirements in relation to the ACROSS project and its general functional and infrastructural vision.

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

As noted in the proposal for the ACROSS project, 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 will be based on existing solutions such as the MyData model for human-centered personal data management and processing, and built on experiences around Attribute-Based Credentials approaches in the DECODE project; but it will also include generic data usage policies when the private data needs to be transferred among several stakeholders.

The results from this Work Package will be integrated into the platform created in Work Package 5 and will demonstrate the functionality of the use cases in WP6.

1.3 Methodology and Structure of the Deliverable

Given the desired outcome, the following structure and methodology is applied:

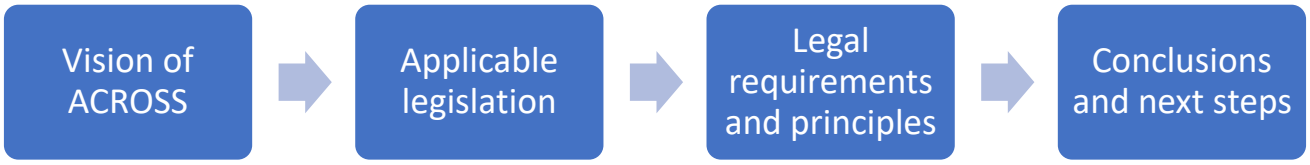

Figure 1 – Structure of D3.6

- **Section 2** below briefly summarises the **General vision of the ACROSS project**. The objective is to describe the general policy context and operational goals in which ACROSS operates, thereby setting the scene to determine the use cases for the ACROSS architecture, and allowing the identification of relevant legislation.
- **Section 3** describes **relevant legislation at the EU level**. It outlines which legal frameworks will govern the architecture and use cases on the basis of the descriptions in section 2, and derives specific legal requirements for the ACROSS architecture or at the use case level. The emphasis is on EU level legislation rather than on national regulatory requirements, since the objective is for ACROSS to be generically usable, in any Member State and for any use case.
- **Section 4** then provides a **summary of the legal requirements, and posits foundational compliance principles for the ACROSS project.** This is done by aggregating the results of the legal frameworks analysed in section 3, and deriving more accessible high level principles.
- Finally, **section 5** provides a summary of the **principal findings,** and outlines **future action points and compliance monitoring strategies.**

2 General vision of the ACROSS project

2.1 High level principles and objectives

The central vision for ACROSS, as described in the proposal, is:

- To build a **user-centric central platform/gateway for European citizens** to find and interact with **national administrative services and private sector services** in **cross-border scenarios.**
- To **facilitate intra-European cross-border mobility**, therefore the projects focus is set on the domains of "**Studying abroad**" and "**Working abroad**".
- To provide a **holistic solution** that allows **public administrations** to deliver a **user-centric interoperable cross-border mobility service compliant with the current European regulations (e.g., the Single Digital Gateway**, European Interoperability Framework) where the private sector can also interconnect their services while **ensuring data sovereignty of the citizens**, who can **set the privacy level** that will allow the public and private sector access to his data based on his decisions whether to allow this.

Thus, a platform must be established that places users at the centre. User control and user sovereignty are key objectives, and users must be able to determine which information is made accessible by whom, and for which purpose. Data protection and sovereignty are therefore guiding principles for the project.

2.2 Intended use cases

As the summary above notes, the ACROSS project in particular considers **public sector (e-government) services**, including (but not limited to) those covered by the recent Single Digital Gateway Regulation (SDGR), which will be described in detail in section 3 below.

None the less, ACROSS is not a purely public sector driven project. **Private stakeholders** can be involved both as providers of the platform itself (i.e. as the service provider offering data to third parties), as providers of data managed via the platform (i.e. as issuers of documents or information that the user may try to exchange), and even as services relying on information from the platform (i.e. as companies or institutions who receive and use information managed via the platform on the basis of the users' consent).

Thus, e-government use cases are one of the key targets of the ACROSS infrastructure, but they are not the exclusive focus. This implies that requirements from e-government focused legislation (such as the SDGR) will be taken into account and must be conceptually supported by ACROSS, even though the requirements from this legal framework will not always be relevant for all use cases.

In practical terms, the ACROSS use cases aim to focus on citizen mobility, notably in relation to working and studying abroad, including all legal and administrative practicalities that this entails. The use cases are therefore citizen centric (rather than company centric), implying also that privacy protection and data protection are central topics in the project. This is reflected in the analysis below.

2.3 General note on co-creation in ACROSS and its link to piloting

The development and piloting of a user-centric central platform is not the only innovation in ACROSS. It also aims to directly involve various categories of stakeholders – including the users (citizens) themselves – in the creation, analysis, design and evaluation of the services provider, in a so-called co-creation track. This implies that the inputs from real persons (potential users of the platform) are collected and analysed for the purposes of the project, in so-called co-creation sessions. In practical terms, co-creation sessions are workshops, interviews, discussion sessions, and any number of other interactive input collection techniques.

The co-creation sessions obviously must comply with all applicable legal requirements as well. These will however **not be examined in detail in the present deliverable,** since the principal legal requirements in these sessions are addressed by the ACROSS ethics activities within Work Package 8. The principal ethics concerns relate to the processing of personal data in accordance with the EU's fundamental right to data protection, and compliance with data protection law (notably the GDPR [1]). **All GDPR compliance requirements related to the co-creation sessions are exhaustively addressed by WP8 deliverables**, including consent templates and procedures, transparency statements, appointment of a data protection officer, security principles, anonymisation strategies, and so forth, as described in the 14 Ethics deliverables of Work Package 8. These are not repeated here for the sake of readability.

Inversely, the ethics deliverables do not examine architectural and piloting requirements in ACROSS. This is because the ACROSS project applies a two-tiered approach in relation to its personal data processing activities:

- In relation to the **pilots** in different Member States, the ACROSS use cases will not involve real end users (i.e. data subjects), but rather 'personas', using a test bed designed to emulate operational services they are using or intend to use through the ACROSS platform. Personas are in effect fictitious persons, which are credible and realistic, but not directly or indirectly based on identifiable real persons. Therefore, **personas are not humans** (or data subjects in the sense of the GDPR), **nor are they research participants** in the sense of this deliverable. Reliance on personas allows in-depth emulation, analysis and research, without triggering any data protection

or privacy concerns. **Since no real persons are involved, the data protection requirements do not apply to piloting activities in ACROSS.**

- Real persons will however be engaged in **co-creation sessions**, where participants are asked (on the basis of their free, informed and specific consent) to give their opinion on relevant procedures. The **participants in co-creation sessions are real humans** (and data subjects in the sense of the GDPR), **and therefore the GDPR applies**.

Only the co-creation sessions result in the processing of personal data as defined by the GDPR. For that reason, ethics deliverables in Work Package 8 only assess the risks in relation to co-creation data processing activities, not in relation to the ACROSS architecture or pilots.

That would of course leave a significant gap in the project's legal activities, which is filled by the present report, since architectural and piloting requirements are covered here, both with respect to data protection, and more generally.

Collectively, this deliverable in combination with all Work Package 8 deliverables thus cover the entirety of ACROSS activities.

3 Relevant legislation at the EU level

3.1 Priority topics for examination

The main characteristics of the ACROSS platform, its main features and use cases have been summarily described above. On the basis of those elements, four legal areas will be examined in detail in this deliverable:

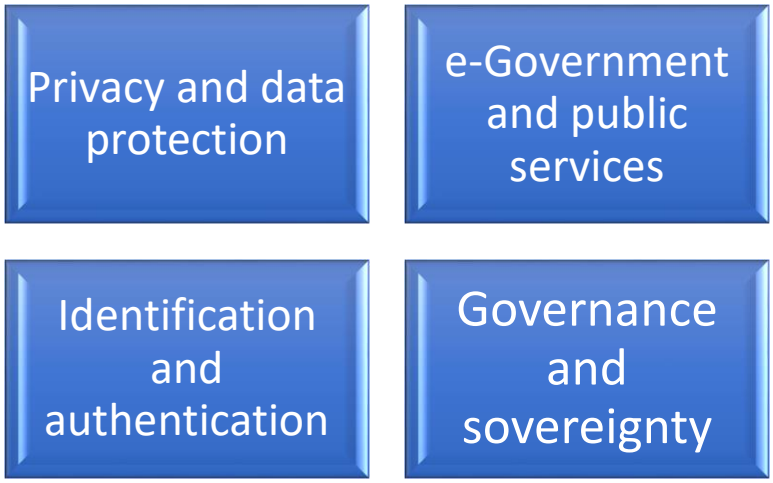

Figure 2 – Priority legal topics for examination

More specifically:

- **Privacy and data protection** is arguably the key requirement for the ACROSS platform, which aims to create a user centric platform that gives users control over their data. Taking into account that users in this project are always natural persons, information relating to them will be qualified as personal data, as defined under EU law. The platform thus needs to be designed with privacy and data protection in mind, in accordance with the **privacy by design and privacy by default** principles of European data protection law.
- **e-Government and public services** are the second key vector. While ACROSS isn't designed or intended exclusively for public sector use cases as indicated above, one of the main objectives is to provide a platform that allows information management in accordance with recent e-government legislation, including specifically the Single Digital Gateway Regulation. With that in mind, this legal framework needs to be assessed too, to ensure fitness for purpose.
- **Identification and authentication** are a cross cutting – i.e. non-sector specific and non-use case specific – requirement. In order for the ACROSS platform to be useful, the users have to be identifiable in most use cases. Moreover, any information that they make available through the

platform must be shared in a way that allows integrity and authenticity to be ensured appropriately. In this context, 'integrity' implies the possibility to verify that information hasn't been modified or corrupted; and 'authenticity' implies the possibility to link information to a specific source. In this way, the recipient can determine to what extent the information can be trusted.

- **Governance and sovereignty** refers to the ability for users to determine if, where and to what extent their information can be accessed and used. This implies that no exchange of information occurs without their knowledge and consent; and that they are able to monitor exchanges at all time, and have the possibility to withdraw any access and usage permissions.

The principal EU level legal frameworks for all four of these topics will be briefly described and assessed below, in four different subchapters. Each subchapter will:

- Briefly **describe** the relevant legislation and its main features;
- Assess the **applicability** to the ACROSS project, at the infrastructural level or for specific use cases;
- Conclude with a summary of **resulting legal requirements.**

3.2 Data protection and privacy

3.2.1 Relevant legislation

Both the right to privacy and to protection of personal data are fundamental rights, enshrined in the **EU Charter of Fundamental Rights** [2], respectively in Articles 7 and 8 of the Charter. The right to privacy generally relates to the right to respect for an individual's private and family life, home and communications. The right to protection of personal data relates to the right of any individual to have data relating to them processed (i.e. collected or used) in a fair and lawful manner. More specifically, the Charter requires that such data is only "*processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified"*. The Charter furthermore requires that compliance with these rules is subject to control by an independent authority.

These generic descriptions are outlined in greater detail specifically in the **General Data Protection Regulation (GDPR)** [2], which outlines the requirements for fair and lawful processing of personal data. The GDPR applies in principle to any processing (i.e. collection and any other use, including simple exchanges) of personal data, defined as any information relating to an identified or identifiable natural person (a 'data subject') (Article 4 (1) of the GDPR). Since personal data includes any information that can

be linked to an identifiable persons, and the entire concept of ACROSS focuses on allowing persons to govern data, it is unambiguously clear that the architecture of ACROSS must be implemented with GDPR compliance in mind, and that any use cases of the ACROSS architecture must also be executed in compliance with the GDPR.

For the avoidance of doubt, the GDPR explicitly notes that it applies to the processing of personal data in the context of the activities in the Union, regardless of whether the processing takes place in the Union or not; and to the processing of personal data of data subjects who are in the Union, even if the processing is done by an organisation that is *not* established in the Union, if the processing activities are related to the offering of goods or services to such data subjects in the Union. In other words, application of the GDPR cannot be avoided by using infrastructure outside of the EU, or by focusing only on usage of the ACROSS infrastructure by service providers (governments or private companies) located outside the EU. As long as either the service providers operate in the EU, or the citizens include European citizens, the GDPR will apply. Clearly, ACROSS therefore needs to comply with the GDPR in order to be practically usable in the future.

The GDPR contains the following fundamental principles (Article 5.1 of the GDPR):

- personal data must be processed in a **lawful and transparent manner**, ensuring fairness towards the individuals whose personal data is being processed ('lawfulness, fairness and transparency');
- there must be **specific purposes** for processing the data and the company/organisation must indicate those purposes to individuals when collecting their personal data. A company/organisation can't simply collect personal data for undefined purposes ('purpose limitation');
- the company/organisation must collect and process **only the personal data that is necessary to fulfil that purpose** ('data minimisation');
- the company/organisation must ensure the personal data is accurate and up-to-date, having regard to the purposes for which it is processed, and correct it if not ('accuracy');
- the company /organisation can't further use the personal data for other purposes that aren't **compatible** with the original purpose;
- the company/organisation must ensure that personal data is **stored for no longer than necessary** for the purposes for which it was collected ('storage limitation');

- the company/organisation must install appropriate **technical and organisational safeguards** that ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technology ('integrity and confidentiality').

Other principles include the obligation to implement **data protection by design** and **data protection by default** in any new initiatives (Article 25 of the GDPR, sometimes also referred to as privacy by design and privacy by default), implying respectively that data protection compliance must be built into architectural designs at the earliest possible stage, and that any features that protect personal data must be activated by default.

Finally, the GDPR adopts the **accountability principle** (Article 5.2 of the GDPR**,** meaning that the organisation determining the means and purposes of data processing (the so-called data controller) is responsible for, and be able to demonstrate compliance with, its compliance obligations. In practical terms, that means that the controller must not only assess its compliance, but also that it must retain sufficient documentary evidence in order to prove its compliance at all times.

Furthermore, the GDPR contains numerous operational and procedural safeguards, including the supervision of data processing activities by an independent authority (a data protection authority, Article 51 and following), a limitation on transfers of personal data to countries outside the European Economic Area (EEA) (Article 44 and following), safeguards against the processing of special categories of personal data (such as data concerning health; Article 9) and against automated individual decision-making, including profiling (Article 22 of the GDPR), and rules and procedures on how to deal with incidents involving personal data (so-called personal data breaches, Article 33 and following).

The GDPR comprises the general legal framework for personal data processing in the EU. Similar and comparable legislation exists for the processing of personal data by EU institutions [3] or in the context of law enforcement [4], but since these are not the key focus of ACROSS, they will not be examined in any detail here. For completeness, it is worth noting that a *prima facie* assessment of the legislation on the processing of personal data by EU institutions showed no fundamental impacts on the legal requirements for ACROSS – i.e. while the issue was not examined in detail, it would appear that EU institutions should be able to use the ACROSS architecture under conditions that are no more stringent that any other service provider.

A last legal source that warrants inclusion in this report is the **e-Privacy Directive** [5], as amended in 2008. This Directive governs generally how providers of electronic communication services, such as telecoms companies and Internet service providers (ISPs), should manage their customers' data, and creates certain

rights for those customers. Most of the framework relates specifically to the telecommunications industry, and is not applicable to personal information management systems (PIMs) such as ACROSS.

However, the Directive also contains rules on the use of cookies, and more generally tracking technologies that require storage of information and/or access to information on the equipment of a user. This is only allowed on the condition that the user has given his or her consent, having been provided with clear and comprehensive information about the purposes of the processing. This general principle is more broadly applicable, and has given rise to strict cookie consent management practices in the EU.

Moreover, the e-Privacy Directive has been under revision for some time, in order to align it better to the approach of the GDPR, and to ensure that the Directive also covers online services (so-called information society services), which would likely include platforms such as the ACROSS infrastructure. While the proposed e-Privacy Regulation [6] has not yet been adopted, and likely wouldn't enter into application during the running time of ACROSS, it is therefore prudent to observe the rules of this framework, in terms of safeguarding communications confidentiality, abstaining from the use of tracking technologies without consent, and not capturing location data without user consent.

3.2.2 Applicability to the ACROSS project

3.2.2.1 General considerations

Both the GDPR and the e-Privacy Directive apply to the ACROSS platform as a whole, and to its use in specific cases. More in detail, their applicability can be broken down as follows:

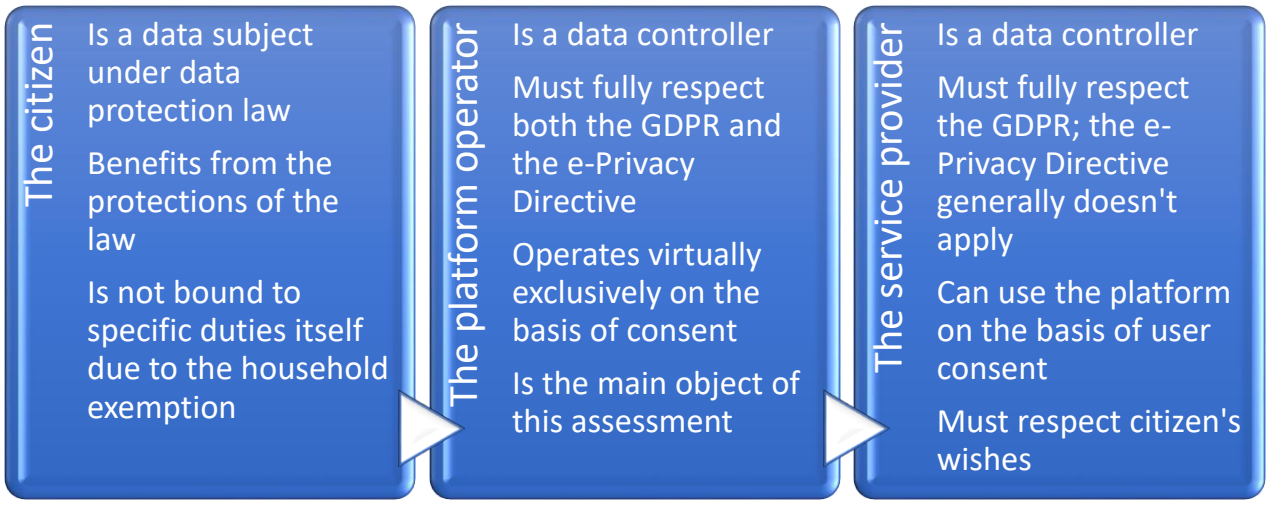

Figure 3 - Applicability of data protection law to ACROSS

As the overview summarily shows:

- The **citizen** is a data subject under EU data protection law, since their personal data at a minimum will be processed via ACROSS infrastructure. It is conceptually possible that the personal data of other persons than the citizen using ACROSS is processed as well, e.g. in the case of parents submitting information in relation to their children. For that reason, lawfulness and transparency practices in ACROSS must cover all data subjects, not just the direct users. The data subjects are generally the beneficiaries of data protection law, and can benefit from its protections, including the data subject rights created by data protection law. They fundamentally don't bear specific duties themselves under data protection law, because (and to the extent that) their use of the ACROSS platform is governed by the so-called household exemption: Article 2.2 (c) of the GDPR notes that it doesn't apply to processing of personal data "by a natural person in the course of a purely personal or household activity", and thus with no connection to a professional or commercial activity. The recitals to the GDPR clarify that "*personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities*". On the basis of this rule, citizens themselves shouldn't be struck by any GDPR obligations or constraints, unless they start using the system other than for the purposes of their own personal data governance needs.
- The **platform operator** (i.e. the entity hosting citizen personal data, including substantive data such as identity information, documents or certificates; and metadata such as data on user activity, profile or behaviour) is a data controller as defined under data protection law. They determine the purposes and means of the platform, and therefore are responsible for complying with data protection law, including the GDPR and e-Privacy Directive. This means that they are required to ensure that they have a legal basis for running the platform and for sharing user data with specific service providers, which generally will be the consent of the end user, at least when the platform operator is an independent service. Conceptually, it is also possible that the citizen data not held by an independent service, but rather that the ACROSS architecture is implemented as a range of modules or tools that are integrated by existing data holders. In that case, the data holders still act as data controllers, but another legal basis for holding and processing their data could apply, such as notably a specific legislation (at the EU or national level) that obliges an organisation to run such a platform. For independent operators, consent is the main possibility for ensuring the lawfulness of the platform. For that reason, the responsibilities of the platform operator are the main focus of this deliverable. For completeness, it should be noted that the

various functions of an operator can be split across multiple legal entities, and that data governance infrastructures can also be instantiated in a fully decentralised mode, e.g. by storing data on a blockchain. In that case, there is no platform operator, since there is no organisation that determines the purposes and means of data processing. This is however not envisaged in the context of ACROSS, which has a more limited role for blockchain use.

- Finally, the **service providers** (i.e. the organisations with whom the user chooses to share its data via ACROSS) are independent data controllers, separate from the platform operator. They determine the purposes and means of their own use cases, and therefore are responsible for complying with data protection law, including the GDPR. The e-Privacy Directive generally will not apply to them, as they have no means to breach confidentiality or track user behaviour in ACROSS infrastructure. Again, this means that they are required to ensure that they have a legal basis for their data processing activities. Generally, this legal basis will be the consent of the user in relation to the transfer of data from the platform to their own systems. A completely different legal basis can apply for their processing activities after receiving the data – this can again be the consent of the citizen, but especially for public sector service providers, the legal basis may also be that they have a legal mandate under national legislation to provide a public service. In that case, their legal basis will be the necessity of data processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6.1 (e) of the GDPR), rather than consent (Article 6.1 (a)).

The discussion of a legal basis is not a merely academic difference: the GDPR requires consent to be revokable (Article 7.3 of the GDPR), which is a possibility that does not exist for other legal bases. That means that a citizen can *always* choose to stop using the ACROSS platform, and to stop any data sharing with service providers, since both of these are based on consent. However, a citizen cannot *always* stop a service provider from using data they submitted through ACROSS, since the legal basis isn't always consent. This is also perfectly intuitive and natural: if a citizen e.g. sent information to a government in order to obtain a permit, then that government must have a legal mandate to collect and retain that data. Allowing the citizen to demand that its data should be deleted by the government by withdrawing its consent would disrupt the functioning of public services. For that reason, the distinction between the lawfulness of the platform and the lawfulness of the service providers is important to understand. In this deliverable, the platform is the main target of evaluation, although we will also examine how the platform must interact with service providers.

3.2.2.2 ACROSS as a Personal Information Management System (PIMS)

ACROSS can unambiguously be qualified as a Personal Information Management System (PIMS). As described in greater detail in a 2021 Tech Dispatch published by the European Data Protection Supervisor[7], "*PIMS are products and services that help individuals to have more control over their personal data. PIMS enable individuals themselves to manage and control their online identity.*

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

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

The Dispatch identified several examples of PIMS, some of which will be further discussed in the sections below. From a data protection compliance perspective, it highlighted seven key data protection priorities:

- **Individual empowerment plus data protection by design and by default** - when correctly designed, PIMS could help data controllers to implement the obligations of privacy and data protection by design and by default and to support them to demonstrate compliance with the GDPR.
- **Consent management** - PIMS deliver their full potential when they rely on users' consent. Individuals would keep full control and would be free to share their personal data according to their own preference and delete them whenever they want.
- **Transparency and traceability -** PIMS would allow for transparency both at the level of shared policies and by technical design, disclosing what services are processing which data for what specific purposes. Information can be given in real time. Personal data dashboards can help individuals to follow their data and their processing.
- **Exercise of individual's rights of access, to rectification and erasure or "right to be forgotten" -** PIMS provide features for individuals to be able to access their personal data, as well as to rectify

or erase them, as provided for by the GDPR, either because the data are in repositories under their direct control or because all shared data are linked to a source, which is again in the control of the individual.

- **Data accuracy -** In PIMS, individuals are responsible for the data they provide. At the same time, when other organisations are accountable for personal data (e.g. banks, utility providers), certain PIMS can provide proof of origin/validity from those organisations, thus granting the necessary level of reliability.
- **Data portability and interoperability -** PIMS can usually offer personal data and other metadata describing their properties in machine readable formats, as well as programming interfaces (APIs) for data access and processing. This last feature implies the use of standard policies and system protocols.
- **Data security -** PIMS must also ensure the security of personal data at rest and in transit from unauthorised or accidental access or modification. Data minimisation and anonymisation services should also be provided. One feature of many PETs is the use of cryptography.
- **Data minimisation –** a PIMS supports data minimisation techniques (e.g. attribute-based credentials), to ensure that third parties can access only necessary pieces of information, thus avoiding the disclosure of the full identity of the individual.

These principles can also be found in the 2020 Opinion 9/2016 on Personal Information Management Systems from the European Data Protection Supervisor [8], which supervises data protection compliance and practices by EU institutions. The general priorities and requirements were largely the same, although the Opinion added three further components:

- **Transfer controls –** a PIMS should help ensure that any transfer of personal data beyond the borders of the European Union will be done in compliance with the rules of the GDPR relating to international transfers. PIMS may also help empower users to decide for themselves how far they wish to share their data geographically. Depending on the specifications of the individuals concerned, as gatekeepers, PIMS may help ensure that data will travel only insofar as the individual wishes it to do so.
- **Liability and responsibility –** a PIMS acts (at a minimum) as an intermediary, and for that reason it is important to clearly specify their role and liability vis-a-vis the individuals who entrust their data to them, and towards relying parties (i.e. the service providers). While there is usually no doubt that the PIMS will act as a controller, it should be made clear whether the PIMS themselves are entitled to further process the data, and if so, for what purposes and subject to what terms.

- **Authorising and managing use, rather than 'selling' data –** the Opinion highlighted that the PIMS can also allow personal data to be valorised, in a model that's more nuanced than the simple notion of 'selling' personal data – which is a concept that's difficult to reconcile with the fundamental right to protection of personal data. As a matter of principle PIMS will not be in a position to 'sell' personal data, but rather, their role will be to allow third parties to use personal data, for specific purposes, and specifics periods of time, subject to terms and conditions identified by the individuals themselves, and all other safeguards provided by applicable data protection law.

Thus, there is a fairly mature and comprehensive body of law and guidance on the data protection rules that apply to an infrastructure such as ACROSS.

3.2.3 Summary overview of resulting legal requirements

Based on the overview provided above, a shortlist of legal requirements can be derived:

Table 1 - Legal requirements related to data protection

Identifier	Description
DP-01	Any citizens are free to choose to use the ACROSS infrastructure, on the basis of their **consent,** which must satisfy the requirements of the GDPR. This implies that alternatives must be available, and that consent can be withdrawn, which must result in their data being removed from the platform. This legal basis doesn't necessarily apply to the service providers use of any received information.
DP-02	Any platform operator of the ACROSS infrastructure **may not use the data for other purposes** than those to which the citizen consented. This includes a prohibition on tracking, profiling, data selling or trading, surveillance, or direct marketing – except where a user consented to this.
DP-03	Given the consent requirement, the ACROSS platform **may not be used by minors under 13 without parental consent,** nor by any other persons who are not capable of providing legally binding consent.
DP-04	ACROSS must implement policies and interfaces towards the service providers that **specify what service providers are allowed to do, and what they are not allowed to do.** This includes a clear communication of the purposes of use, and a legal commitment to respect this constraint; and implementation of the data minimisation principle – no service provider may request more data than they strictly need.

Identifier	Description
DP-05	ACROSS must foresee **transparency notices** that inform citizens of their rights and of the key features of ACROSS.
DP-06	ACROSS must foresee features that ensure that **no personal data is shared with third parties without user consent.**
DP-07	ACROSS must foresee **transparency interfaces towards the citizens** that allow them to manage data storage, availability and use, including at a service provider specific level, and that allow them to monitor present and past use of the platform (including any prior authorised data exchanges).
DP-08	ACROSS must foresee **data subject rights interfaces**, allowing citizens to see, update and delete their personal data on the ACROSS platform; and that allow them to obtain copies of that data (data portability).
DP-09	ACROSS must implement **storage limitation policies –** by default, data should be deleted after a pre-set period of time, which the citizen may set or modify.
DP-10	ACROSS must implement the **data protection by default principle,** meaning that any data protection features must be enabled (not disabled) by default. This includes data deletion by default after a set period of time, and no sharing or monetisation of data by default (without user consent).
DP-11	ACROSS must implement appropriate technical and organisational **security** features. At a minimum, this entails: • Access controls: data on the platform may not be accessible to third parties without citizen consent. Data can be effectively encryption, and/or it may be protection by other suitable access controls (such as multifactor authentication). • Transfer controls: any personal data sent from the ACROS infrastructure to a service provider must be protected against unlawful interception through effective encryption. • Logging and audit trails: exchanges of information to and from the ACROSS infrastructure must be logged in a way that allows interactions to be identified and examined. Logs should comprise metadata only.
DP-12	ACROSS must implement **third country transfer controls,** meaning that the citizen must be able to see whether data will be sent to a recipient outside of the EEA prior to consenting to sending that data. The transfer must satisfy the requirements of the GDPR.

Identifier	Description
DP-13	Prior to piloting, a **data protection impact assessment** should be conducted on the general ACROSS architecture, given the innovative use of new technologies that can conceptually pose risks to the rights and interests of the citizens.
DP-14	Both the platform operators and any service providers with whom the citizen chooses to interact must be **clearly and unambiguously identified to the citizen,** including a description of their role and responsibility.

3.3 E-government and public services

3.3.1 Relevant legislation

As was explained in the preceding sections (specifically in Section 2 – General vision of the ACROSS project), the ACROSS infrastructure is not designed specifically or exclusively for an e-government context. Both the platform operator and the service providers can also be private sector entities. More in detail:

- Information that the citizen can make accessible to a service provider (such as identity information, attestations, certificates etc.) can originate from either private or public sector parties. They can even be self-signed declarations from the citizen.
- The platform operator can conceptually be a private or public sector party; or indeed it can follow a 'mixed-mode' approach where some modules are operated by a public sector entity, and others by the private sector. The topic of modules and functionalities of the platform will be further detailed below.
- The service providers themselves finally can also be private or public sector parties – i.e. the ACROSS platform can be used by a citizen to make its data accessible to public administrations in an e-government context (e.g. to a city administration to organise a change of address), or to private administrations in purely private contractual circumstances (e.g. to a bank for the purposes of opening a new account).

Thus, conceptually the ACROSS platform is not an exclusively e-government initiative.

None the less, the public sector is particularly important to the ACROSS project. As explained immediately in the abstract of the ACROSS project proposal, part of the background of ACROSS is the recent EU initiative to establish a Single Digital Gateway (SDG). The SDG is conceived as a platform that creates a bridge between the Member States, and "*will facilitate online access to the information, administrative procedures and assistance services that citizens and businesses need to get active in another EU*

country.[..] By the end of 2023 at the latest, they will be able to perform a number of procedures in all EU member states without any physical paperwork, like registering a car or claiming pension benefits.

The single digital gateway will guide citizens and companies to information on national and EU rules, rights and procedures and the websites where they can carry out these procedures online. And users looking for assistance will be guided towards problem-solving services" [9].

As a part of the SDGR, a search function on the 'Your Europe' portal will give access to:

- Information. Citizens will be able to easily find reliable, qualitative information on EU and national rules that apply to them when they want to exercise their Single Market rights.
- Procedures. Citizens will find out exactly how to carry out administrative procedures and what steps they need to follow.
- Assistance services. If users are still confused about which rules apply or have trouble with a procedure, they will be guided to the EU or national assistance service most suited to address their problem.

In order to bring about the SDG, a specific regulation was adopted, the Single Digital Gateway Regulation (SDGR, [10]). The SDGR creates a legal basis for the establishment of the SDG in general. More importantly from the perspective of the ACROSS project, it also creates a legal basis for the cross-border exchange of digital evidences between competent authorities in a range of public services. In that way, the objective of the SDGR is to enable the implementation of the once-only principle in European e-government procedures: rather than requiring the citizen to search for his/her own documentary evidences and requiring them to transfer these from one administration to another, the goal is for reliable evidences to be transferred directly between the relevant public administrations. This increases efficiency, decreases the possibilities for fraud and mistakes, and enhances user friendliness.

In order to achieve this goal, Article 14 of the SDGR contains the main rules and principles for the cross-border automated exchange of evidence and application of the 'once-only' principle. These can be briefly summarised as follows:

- In terms of **covered services,** the SDGR only applies to a closed list of services. These include online procedures in the context of public procurements (Directive 2014/24/EU and 2014/25/EU), recognition of professional qualifications (Directive 2005/36/EC), access to markets under the Services Directive (Directive 2006/123/EC), and most importantly a long list of online procedures listed in Annex II to the Regulation. That Annex is also appended to the present deliverable, but for the purposes of the ACROSS project, it is mainly important to note that both moving and

studying abroad are included in this list. Given that these are key piloting areas, the SDGR is thus directly relevant to ACROSS.

- In terms of **covered entities**, the SDGR applies to competent authorities. These are defined in the SDGR as "any Member State authority or body established at national, regional or local level with specific responsibilities relating to the information, procedures, assistance and problem-solving services covered by this Regulation" (Article 3 (4) of the SDGR). The notion can therefore also include private entities, but only on the condition that they've been given specific responsibilities in an administrative procedure. Purely private sector transactions (e.g. opening a bank account, or applying for a job directly with a private company) are out of scope of the SDGR.
- In terms of **covered information,** the SDGR means to facilitate exchanges of 'evidence', defined generically as "any document or data, including text or sound, visual or audiovisual recording, irrespective of the medium used, required by a competent authority to prove facts or compliance with procedural requirements" under the SDGR (Article 3 (5) of the Regulation). In the context of Article 14, the evidences must of course be electronic (since direct online exchanges are required), but there is otherwise no constraint. Evidences may therefore be in any data format, and the evidences can be both structured (e.g. XML documents) or unstructured (e.g. visual PDF scans of originally paper documents).
- In terms of **architectural choices,** the SDGR requires exchanges of evidence between competent authorities under the once-only principle to take place via a so-called 'technical system', to be established by the Commission in cooperation with the Member States. The logical components are to be set out in an Implementing Act, which shall be described further below.
- In terms of **procedural safeguards,** the SDGR principally requires that (Article 14):
    - Use of the technical system is **voluntary.** I.e. citizens must always have an alternative available to them, which can be either electronic or paper-based.
    - Evidence may only be exchanged through the technical system based on the **prior request** of the user, i.e. the user must ask for evidence to be exchanged between competent authorities. It is thus not possible for authorities to exchange information without the user's consent, even if this would be in the public interest. Exceptions can exists where there is specific legislation that allows exchanges without any prior request.
    - Evidence may only be exchanged through the technical system after the user has been able to **preview** the evidence, i.e. the user must be able to see evidence before it is sent to a competent authority, and can then decide whether they wish to proceed or not. In that way, the user can verify the accuracy of the evidence, and can also determine whether exchanging it is in their best interest.

- Exchanges must of course be **secure and interoperable,** to allow trustworthy use of the evidence.
- Exchanges must be **limited to what is strictly necessary** to what has been requested, and may only be used by the receiving authority for the purpose of the procedure for which the evidence was exchanged.

Most of these safeguards reflect the need to ensure a high level of trustworthiness, data protection, confidentiality and good governance. None the less, the choices of the SDGR are also indicative of a specific vision of e-government, or rather a vision of implementing evidence exchanges. The goal, as explicitly stated in Article 14.7 of the SDGR, is to require the competent authorities to "request evidence directly from competent authorities issuing evidence in other Member States through the technical system. The issuing competent authorities shall make such evidence available through the same system".

In other words, the objective is direct exchange between competent authorities, without requiring the user to act as a middle man. In that sense, the SDGR does not adopt a comprehensive PIMS approach that allows the users to exclusively control their own data. The users control data flows between authorities (through the requirements of a prior request and a preview possibility), but they do not assume ownership or exclusive control over the data themselves. That data originates with a competent authority, and flows directly to another competent authority, with the user acting as a gatekeeper but not as a data holder.

The SDGR is the principal legal framework for once-only information exchanges in the EU, and certainly also the principal source of legal requirements for ACROSS, at least insofar as ACROSS use cases fall within the remit of the SDGR. However, the SDGR is not an entirely comprehensive framework. Under Article 14.9 of the SDGR, the European Commission was obliged to adopt secondary legislation – a so-called **Implementing Act** – by 12 June 2021, to set out the technical and operational specifications of the technical system.

While significant advances were made and an advanced draft proposal is available [11], the Commission ultimately has not been able to meet this deadline, and at the time of submission of the present deliverable (31 July 2021), no finalised Implementing Act is available. The main reason is a political disagreement between the Commission and Member States on whether the draft Implementing Act remains entirely within the mandate of the SDGR. Specifically, the proposed draft Implementing Act would allow the Commission some future margin to set out "a high-level architecture and technical design documents ensuring interoperability", which is arguably a competence that the SDGR did not foresee. The matter is currently undergoing a review procedure, which should result in a future Implementing Act.

None the less, on the basis of the aforementioned draft proposal [10], the Commission's vision for the high level architecture of the technical system can be summarily described. The proposal foresees that the technical system comprises both a set of common EU services to be operated by the Commission, and a range of Member State services.

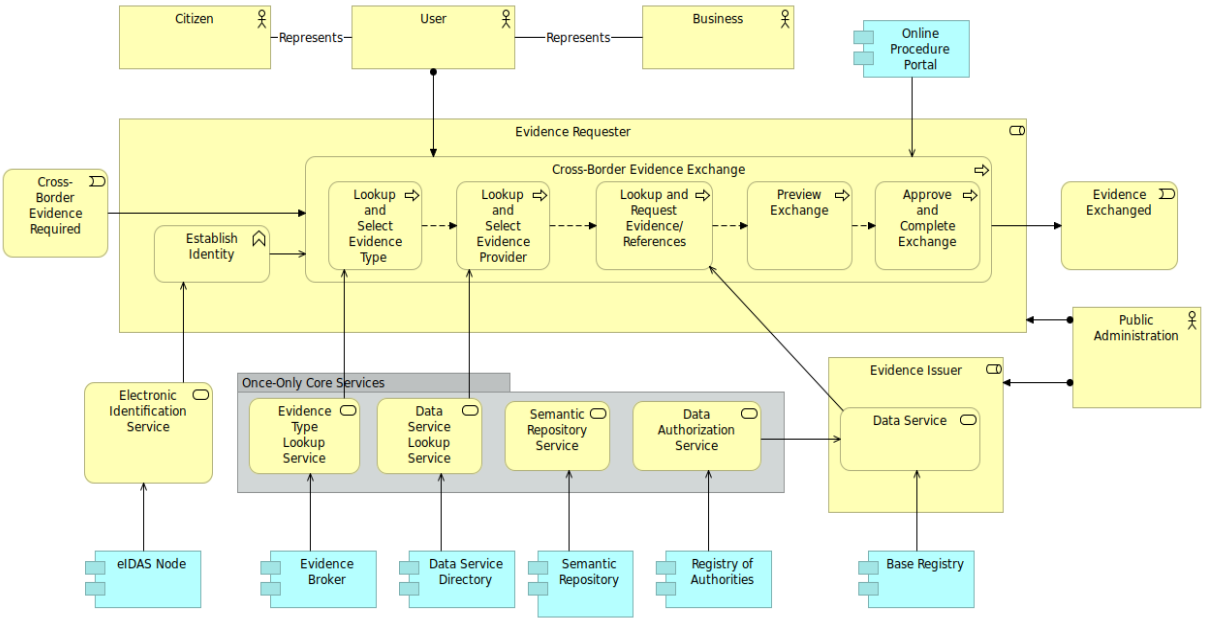

Figure 4 - High Level View of the Once-Only Technical System (Source: SDG Working Group - Once-Only Technical System High Level Architecture Version [0.4])

Without endeavouring to go into excessive detail on the regulatory requirements for the technical system, the **common services** (operated at the EU level) comprise:

- a data service directory, containing a list of competent authorities acting as evidence providers, a list of available evidences, and semantic data; as well as identification requirements imposed by the Member States for accessing these evidences;
- an evidence broker, in charge of determining equivalence between evidences between Member States;
- a semantic repository, which identifies data models, associated schemata and data formats for each type of evidence.

At the **national level**, Member State services comprise:

- the procedure portals of competent authorities that require evidences (evidence requesters) or and the data services of competent authorities that issue evidences (evidence providers);
- intermediary platforms for providers/requesters that connect to common services. This is an optional component that allows Member States to build an intermediary between the technical system and certain competent authorities, in order to avoid that a very large number of sometimes smaller organisations are required to all maintain the relevant infrastructure individually;
- any national registries and services that are equivalent to the EU data service directory or broker, i.e. that Member States may choose to build to identify relevant authorities, evidences and equivalences at the national level; these must be either accessible to Member States, or copied to the EU data service directory or broker;
- eIDAS nodes for user authentication and identity matching, i.e. the services that allow citizens to identify themselves both towards the evidence issuers and evidence recipients (see also section 3.4 on identification and authentication below)
- eDelivery Access Points, i.e. standardised infrastructure to send or receive evidence, which must be used for providers/requesters/intermediaries;

The legislative framework is thus relatively prescriptive in terms of scoping, safeguards and architectural logic; but relatively vague with respect to actual standards, protocols and data formats.

3.3.2 Applicability to the ACROSS project

It was already noted above that the goal of the ACROSS project is not to create an e-government specific system, let alone to create a pilot implementation of the technical system. Indeed, other EU funded projects such as TOOP [11] and DE4A [12] (among others) already assumed that task. For that reason, the objective of ACROSS should not be to build an alternative implementation of the requirements of the SDGR or the Implementing Act.

ACROSS starts from a different philosophy. The operation of the SDG is a meaningful step forward in helping citizens to solve the challenges posed by many cross-border procedures. Towards these challenges, ACROSS aims to propose a novel framework, aiming to substantially complement the SDG and the Your Europe portal by leveraging the advanced capabilities of the cloud, privacy-preserving, semantic interoperability, and mobile technologies, to build a next generation public service ecosystem, while maintaining the highest privacy level. ACROSS aims to enable user-centric design and to support the implementation of interoperable cross-border public digital services, compliant with the current

European regulations, but where the private sector can also interconnect their services, while ensuring the data sovereignty of the citizens.

In other words, ACROSS starts from a different philosophy. The SDGR starts from the conviction that citizens are best served through a government controlled system that allows competent authorities to directly exchange predefined information, in a predefined closed network of authorities, for a predefined and closed list of services. The citizen determines when the system can be used to exchange data, but does not control it. The information is not held by the citizen.

In contrast, ACROSS gives the citizen even greater control, and opens up an ecosystem to more types of information (not just the evidences of the SDGR), more service providers (not just competent authorities), and more procedures (not just those defined in the SDGR). For that reason, the architectural approach of ACROSS is also quite different:

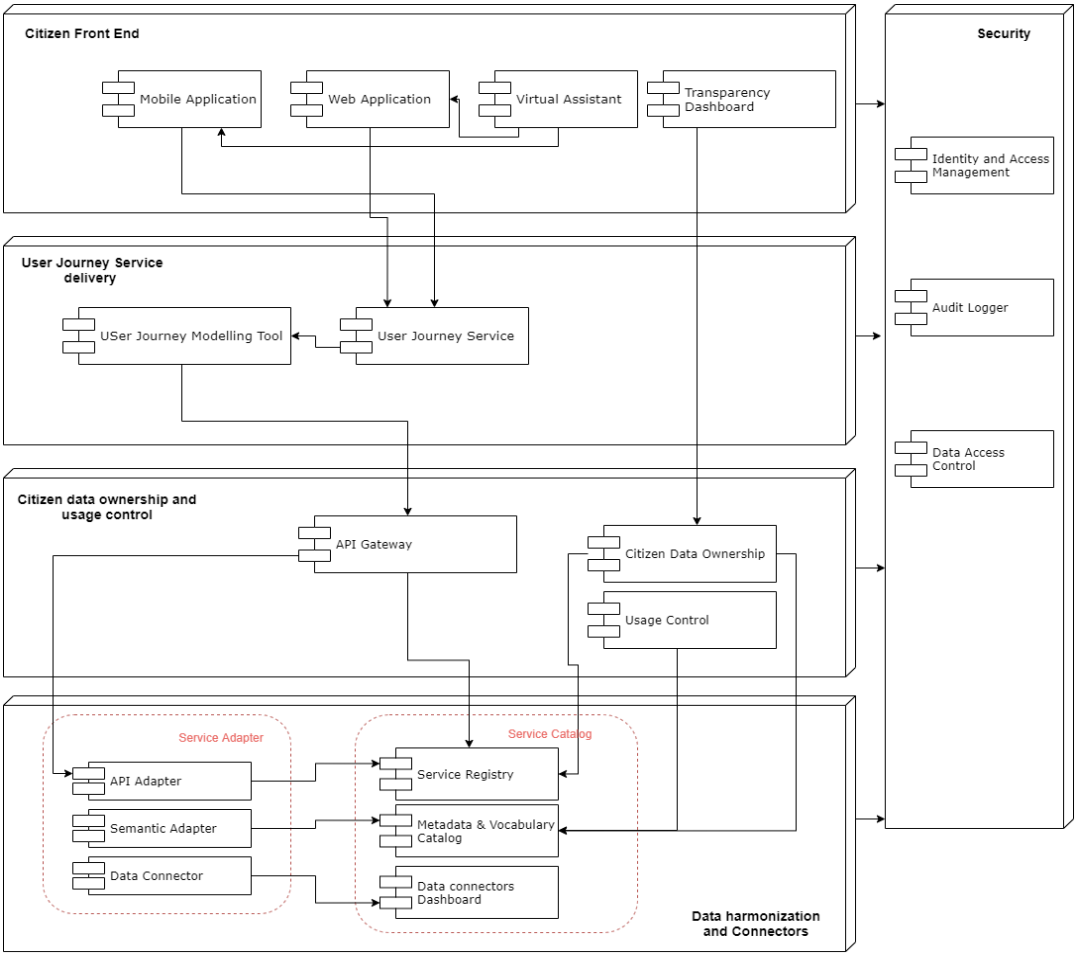

Figure 5 - Component View of ACROSS Platform. Source: ACROSS D5.1 - Architecture components (internal draft version)

The technical system and architectural model of the SDGR and the Implementing Act is not readily recognizable in this architecture. While that means that the ACROSS platform cannot be considered an implementation of the SDGR's legal requirements, this is not problematic, since the objective of ACROSS is not to implement the SDGR, but to complement it in a more open and user centric fashion.

For that reason, it should also not be required to follow each legal requirement of the SDGR and the Implementing Act in detail. For instance, it would not be useful to require that the ACROSS infrastructure contains an evidence broker service, or that it integrates eIDAS nodes or eDelivery Access Points, or that it follows semantic requirements under the SDGR (which are still undergoing work and will likely continue to be worked on for months and years to come). It is far more important to focus on high level legal requirements that have an added value for all potential use cases of the ACROSS architecture, even those that do not focus specifically on e-government services under the SDGR. These requirements are summarized in the following section.

3.3.3 Summary overview of resulting legal requirements

Based on the overview provided above, a shortlist of legal requirements can be derived in relation to e-government, the SDGR and once-only. Note that requirements that were already represented under the GDPR section above are not reprised here in order to avoid overlaps; and neither are requirements in relation to identification and authenticity (captured by the next section) included here. For the avoidance of doubt: these requirements apply only in cases that aim to satisfy the SDGR's requirements.

Table 2 - Legal requirements related to e-government and the SDGR

Identifier	Description
SDG-01	Citizens must always have an **alternative** to using the ACROSS infrastructure. The alternative may be electronic, analogue or physical, but the alternative may not be made artificially difficult or inaccessible.
SDG-02	Recipients of information from the ACROSS infrastructure must always be able to determine the **identity of the entity that issued it**. This may be a private entity, public authority, or the citizen itself; and the identity may be a pseudonym; but the identity must always be assessable to relying parties.
SDG-03	No information exchange relating to the citizen may occur via the ACROSS platform without the **prior request** from the citizen.
SDG-04	Prior to exchanging any information relating to the citizen, the citizen must be **given the opportunity to view the information, and to decide whether to proceed or cancel.** It is not

	mandatory that the citizen actually previews the information; it must only be possible for them to do so.
SDG-05	If the citizen decides not to exchange any information via the ACROSS system after previewing it, **then this may not be visible to the relying party.** The relying party should only be able to detect whether an exchange was successful or not, but not whether the failure occurred before or after a preview. Otherwise, the ACROSS platform inadvertently creates a profiling option, since citizens who decide to cancel an exchange after previewing the information may be considered as suspicious profiles.
SDG-06	Information exchanges must be **granular.** I.e. the citizen must be informed of the information that the service provider wants, and when multiple sets of information have to be provided to relying parties, the citizen should be able to select which sets of information (if any) it would like to exchange; the decision should not be 'all or nothing'.
SDG-07	In order to support **once-only** information exchanges, the ACROSS architecture should be conceptually capable of retrieving data from one source and sending it to its destination in a single integrated step, rather than requiring multiple and unconnected actions from the citizen.

3.4 Identification and authentication

3.4.1 Relevant legislation

A central and cross cutting requirement for trustworthy electronic transactions is that the identity of the participants can be verified, and that the integrity and authenticity of exchanged information can be determined by relying parties. For the avoidance of doubt, this does not imply that fully **anonymous** transactions (where it is entirely impossible to identify a citizen, even with the cooperation of other parties such as law enforcement bodies) are not valuable for the European information society. Indeed, they are arguably critical for a democratic society. However, in order for transactions to be trustworthy for relying parties, it will typically be necessary for them to be verifiable.

Similarly for the avoidance of doubt, **pseudonymous** transactions where a user is not directly identifiable for a relying party, but where the accuracy of the pseudonymous statements can be verified, are on the other hand very important for an advanced PIMS architecture such as ACROSS. Indeed, the ability to make minimal statements in relation to a citizen without necessarily divulging their identity ("This person is an adult"; "This person has the German nationality"; "This person is a qualified doctor") are a key feature of any PIMS. In those cases, the relying party cannot learn the identity of the claimant but knows that the identity of the claimant is known by a third party that vouches for the accuracy of that statement. This

philosophy is central to the so-called Attribute-Based Credentials model that's supported by other EU projects, and that must be incorporated into ACROSS as well.

The EU has developed an advanced legal framework in relation to electronic identification and authenticity, through the so-called **eIDAS Regulation** [13]. This Regulation addresses three principal topics: electronic identification, trust services, and electronic documents. All three of these are relevant in the context of ACROSS.

With respect to **electronic identification,** the central objective of the eIDAS Regulation is to support the mutual recognition of certain electronic identities between Member States, specifically with a view to enabling access to e-government services. At a high level, the eIDAS Regulation allows Member States to notify electronic means of identification used by the public sector (e.g., eID cards or mobile identification apps), and to allow an objective assessment of the reliability of those means of identification on the basis of common EU standards (their so-called level of assurance, which can be rated as high, substantial, or low). Once the notification and assessment is completed, citizens holding those means of identification can use them to access e-government services in other Member States, provided that their means of identification offers at least the same level of assurance as required domestically – i.e. a Member States that allows its own citizens to log onto an e-government application with means of identification at the substantial level, must also allow other EU citizens to log on if they use a notified means of identification that are similarly at least substantial in quality. The notified identification schemes (and the supported means of identification) are published online [15]. As the publication shows, 17 Member States have submitted a notification at the time of submission of this deliverable (although not all assessments have been completed). eIDAS identification schemes are thus relatively common, but by no means universally available.

It is important to stress the constraints of the approach of the eIDAS Regulation with respect to electronic identification. The Regulation emphatically does not regulate purely private sector schemes that are not used by the public sector, nor does it affect schemes that Member States choose not to notify (for whatever reason). Notification also provides no universal seal of approval or guarantee – it only ensures that the means of identification issued under that scheme should be legally acceptable in e-government services across the EU. It does not ensure that the underlying service is available to the citizen (this can depend on many other factors than successful identification), nor that any private company would need to attach any value to the means of identification.

Finally, it should also be noted that the eIDAS Regulation comprises more than a purely legislative framework. Substantial development, implementation and development work has been organised at the

EU and national level, resulting in the creation of the so-called eIDAS nodes [16]. The eIDAS nodes can be understood as a standardised reference implementation software that Member States must deploy, operate and maintain, and which is capable of supporting cross border identification using notified eIDs. An overview of the deployment status of eIDAS nodes is publicly available [17] – at the time of submission of this deliverable, 21 Member States have eIDAS nodes in production. This is also relevant in the context of the SDG, since the technical system envisaged by the SDGR requires support of the eIDAS nodes to enable trustworthy information exchanges.

With respect to **trust services,** the eIDAS Regulation creates a uniform legal framework for certain trust services, including electronic signatures, electronic seals, timestamps, and electronic registered delivery. Essentially, these comprise key building blocks of many digital transactions:

- Electronic signatures allow natural persons to sign electronic information;
- Electronic seals allow companies and administrations to ensure the integrity and authenticity of electronic information;
- Timestamps allow the objective determination that a certain piece of electronic information existed at a specific moment in time;
- Electronic registered delivery allows anyone to exchange electronic information securely and confidentiality, in a manner that allows the identity of the sender and recipient to be validated, as well as the time of sending and receipt.

Unlike electronic identification, trust services are considered as a market service that can be both offered and used by the private sector and the public sector on equal footing – no prior notification by a Member State is required.

However, the Regulation does define certain quality requirements that apply to all trust services and to trust service providers. Additionally, most trust services are regulated at multiple quality assurance tiers: basic trust services are regulated at a basic level; advanced trust services are more strictly regulated; and so-called qualified trust services are most rigidly regulated, also requiring a prior conformity assessment by a third party auditor, which is thereafter validated by a national supervisory body. Qualified trust service providers are included in publicly available national trusted lists, which are aggregated at the EU level [18], thus allowing relying parties to determine whether a trust service is indeed qualified.

While the use of qualified trust services (such as qualified signatures) is usually not legally mandatory, there is a clear benefit to using them, since they have a predefined equal legal value across the EU, and must be recognised as such across the EU. E.g. a Belgian qualified electronic signature can be verified as such across the EU, and satisfies any legal requirement for electronic signing across the EU. Nonqualified

trust services on the other hand always require an assessment of their quality in terms of their ability to ensure the integrity and authenticity of a specific transaction. This process is complex and resource intensive, especially in cross border situations. For that reason, it is critical that qualified trust services are supported and recognisable as such in cross border initiatives in the EU.

Finally with respect to electronic documents, the eIDAS Regulation contains a simple non-discrimination rule, noting only that an electronic document may not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form. In other words, an electronic document may not be rejected as legally invalid merely because it is electronic. Of course, there is a myriad of other reasons why an electronic document could be rejected (e.g. because it is not an original document, not signed, does not contain all required information, etc.).

The eIDAS Regulation is also supported by a broad framework of Implementing Acts, both in relation to electronic identification and in relation to trust services [19]. Without going into detail in this deliverable, these Acts establish the criteria for assessing the level of assurance of eIDs, reference standards and norms for trust services, define notification procedures and cooperation mechanisms, and create a trust mark for qualified trust services.

The eIDAS Regulation has been imperative to creating a common understanding of identification and authenticity requirements in the EU, and it is also used as a key building block for virtually all cross-border e-government services. None the less, it also contains some weaknesses and misalignments with market evolutions. For that reason, the Regulation is presently undergoing revision, and a **proposal for an update to the eIDAS Regulation** was published in June 2021 [20].

Among other topics, the proposal provides better support for mobile based approaches, including remote signing solutions. It also creates a **legal recognition of electronic attestations of attributes** (for which no specific legal basis existed yet), and provides both a definition, a non-discrimination principle and a **legal recognition of electronic ledgers** (defined as “a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering”).

More significantly, it requires Member States to offer a **European Digital Identity Wallet** to their citizens. Such a Wallet should allow users to store identity data, credentials and attributes linked to their identity, and to:

> a) provide them to relevant parties on request and to use them for authentication, online and offline, for a service; and

b) sign via qualified electronic signatures.

Wallets could also be technically standardised in a more consistent manner across the EU. Thus, the Wallets potentially could become the principal access keys to public and private services in the EU. For the purposes of ACROSS, it is also significant that the Wallets represent an unambiguous shift towards greater individual data sovereignty, since they do not merely comprise a tool for basic identification and signing functionalities, but also act as a secure repository of trustworthy data under the user's control. In effect, the Wallets are a component of the vision that ACROSS aims to realise.

The eIDAS Regulation (and its potential future evolution with the June 2021 proposal) thus creates a flexible and powerful legal toolset for identification and validation at the cross border level. For that reason, it's also directly referenced and mandated by the SDGR and its draft Implementing Act, which requires once-**only exchanges to use and recognise eIDAS nodes, and to apply a single sign-on (SSO) mechanism in once-only exchanges covered by the SDGR.**

It is also important to recognise the role of the eIDAS Regulation as a mechanism to both support and manage legal **responsibility and liability** for the accuracy of information. An intermediary platform such as ACROSS would be incapable of assuming and bearing legal liability for the integrity, authenticity and accuracy of all information exchanged via the platform. Thanks to eIDAS, that would also not be required. If exchanged information is signed or sealed by the issuer in accordance with the eIDAS Regulation, it is possible for a relying party to assess integrity and authenticity itself (including by identifying the person or organisation that originally issued the information), and to make its own determination of adequacy of these assurances. In that manner, the user centric and decentralised philosophy of ACROSS can also be applied to its legal responsibility and liability model.

In effect, the role of the ACROSS platform is then essentially focused on its tasks as an intermediary service provider, acting as a hosting service for information assertions. As a hosting service – that does not assume responsibility for the accuracy, integrity and authenticity of information on the platform – its liabilities are principally scoped and delimited by the national transpositions of the **e-Commerce Directive** [21]**.** Broadly, this Directive provides that hosting services have no general obligations to monitor activities on their services (Article 15 of the Directive), and that they are not liable for the stored information if:

(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

This approach can be generally relied upon to mitigate the legal responsibilities and liabilities of ACROSS platform operators.

3.4.2 Applicability to the ACROSS project

The ACROSS project is not under any formal legal obligation to implement any support of the eIDAS Regulation. As a research project, the recognition of notified eIDs is not mandatory, and while the use of basic electronic signatures, seals and timestamps is likely technically inevitable, there's no formal legal requirement to use qualified trust services.

However, in view of the intended use cases and functional requirements, some degree of eIDAS support is required to allow the ACROSS project to have any productive use. This is especially true since ACROSS aims to act as a complement to the SDGR implementation work, which does formally require re-use of eIDAS components.

Moreover, even when completely disregarding the link to the SDGR, the ACROSS project still has functional needs that should be met. Citizens should be identifiable in a trustworthy manner that can be used in cross border use cases as well, which is an issue for which the eIDAS Regulation has created both a legal framework and a technical infrastructure via the eIDAS nodes. Moreover, recipients of information made available via the ACROSS platform must be able to determine the integrity and authenticity of the information, again taking into account the cross-border perspective. For this issue too, the eIDAS Regulation's support for electronic signatures and electronic seals, in particular at the qualified level where these tools have EU-wide legal recognition, solves a fundamental part of the problem. For these reasons, explicit support for the eIDAS Regulation is highly desirable.

The role and impact of the proposal for revision of the eIDAS Regulation is harder to determine. While its support for electronic ledgers, electronic attribute attestations and mobile identity wallets is directly relevant for ACROSS, it is also worth noting that each of these points requires further detailing in the proposal and implementing legislation. This work is unlikely to be fully complete and legally applicable before the expiration of the ACROSS project. For that reason, these evolutions should be taken into consideration and closely monitored throughout the project, but cannot be reasonably used to derive legal requirements at this stage.

3.4.3 Summary overview of resulting legal requirements

Based on the overview provided above, a shortlist of legal requirements can be derived in relation to electronic identification and authenticity. Note that requirements that were already represented under the GDPR or SDGR sections above are not reprised here in order to avoid overlaps.

Table 3 - Legal requirements related to electronic identification and authenticity

Identifier	Description
IA-01	The ACROSS architecture must be capable of **supporting eIDAS notified identification.** This implies both that it must be possible to log onto the platform using an eIDAS notified eID, and that service providers should be able to determine who the user is and whether they asserted their identity using an eIDAS notified eID, along with the level of assurance of that eID under the eIDAS Regulation. Note that this **doesn't imply that eIDAS notified eIDs must always or exclusively be used in ACROSS.** It is perfectly acceptable for non-eIDAS eIDs to be used. However, eIDAS notified eIDs must *also* be usable and recognisable as such, to allow usability of ACROSS for SDGR purposes.
IA-02	The ACROSS architecture must be capable of **supporting log-on through eIDAS nodes.** As above, this **doesn't imply that eIDAS nodes must always or exclusively be used in ACROSS.** However, eIDAS nodes must *also* be usable, to allow usability of ACROSS for SDGR purposes.
IA-03	The ACROSS architecture must be **capable of supporting electronic attestations of attributes** (attribute based credentials), including through **pseudonymous assertions.**
IA-04	Whenever **pseudonymous** transactions are done (including through pseudonymous electronic attestations of attributes), it should be possible to link these to an identifiable citizen with the assistance of third parties (i.e. fully anonymous assertions which are by definition entirely unverifiable should not be supported).
IA-05	The ACROSS architecture must be capable of **supporting qualified trust services, including qualified signatures and qualified seals.** This only entails that, when the ACROSS platform contains electronic information which is electronically sealed or signed at the qualified level, the architecture does not in any way change, modify , remove or corrupt these seals or signatures. Re-signing or re-sealing is therefore only permissible if the original signatures and seals remain intact and verifiable to relying parties.
IA-06	The ACROSS architecture must be capable of **supporting single sign-on for the citizens.**
IA-07	The **liability and responsibility** of ACROSS platform operators must be clearly and explicitly communicated to service providers interacting with the platform, including notably any exclusions in terms of monitoring, intervention, and quality/integrity/authenticity assurance.

3.5 Governance and sovereignty

3.5.1 Relevant legislation

A final critical legal topic to examine in the ACROSS project is the issue of data governance and data sovereignty. While not formally described in any legislation, data governance generally relates to a framework to define, maintain and enforce a common ruleset in relation to data acquisition and management (including use, sharing, and deletion). In simpler terms, data governance is a system for defining who within an organization or system has authority and control over data assets and how those data assets may be used.

Data sovereignty is a potential aspect of data governance since it generally relates to the ability of European citizens and organisations to act independently in relation to their digital data [22]. Collectively and specifically in the context of ACROSS, data governance refers to the need for a shared ruleset in relation to permissible collection and use of data, and data sovereignty relates to the ability of citizens to retain control over their data through the use of the ACROSS infrastructure.

Neither data governance nor data sovereignty are currently explicitly regulated, although obviously many of the legal frameworks analysed above touch upon key aspects of these topics. The **GDPR** (discussed in section 3.2 above) essentially provides a horizontal framework and legality requirements for the governance of personal data (e.g., by defining acceptable legal bases for data processing and by imposing operational and procedural constraints, as well as independent supervision by national authorities), and provides some measure of data sovereignty to data subjects by granting them data subject rights. The **SDGR** (discussed in section 3.3) contains a governance framework for competent administrations exchanging evidence in the context of once-only procedures and supports a certain degree of data sovereignty for citizens by ensuring that data can only be exchanged upon their request, and after they've been able to preview it. Thus, certain building blocks for governance and sovereignty are indirectly present in EU law, which can and will affect the ACROSS project, as indicated by the legal requirements identified in prior sections.

Beyond these frameworks, a new set of legislation was proposed in November 2020, known as the **Data Governance Act** [23]. While the Act is still in proposal stage and therefor not legally binding, it none the less provides useful insights on potential future legal requirements. The proposed Act aims to provide a legal underpinning for responsible data sharing, especially in sectors where data sharing could be a driving force for the European data economy and for society in general. The proposed Act aims to make more data available and facilitate data sharing across sectors, including by directly creating new legally mature governance mechanisms that can support responsible sharing.

It aims to do so through four pillars of the proposal:

- Firstly, it facilitates the **reuse of certain public sector data** that cannot be made available as open data under current law, due to e.g. intellectual property rights or privacy concerns. The reuse of such data would now be encouraged under the proposal, although specific mechanisms are defined in this case (including supervised data processing in a privacy-preserving manner), to ensure that the confidentiality of the data remains safeguarded. Member States must transparently communicate the conditions that apply to such reuse.
- Secondly, it creates a new role in the data economy: so called **data sharing service providers** that will function as data intermediaries, responsible for trustworthy data sharing or pooling.
- Thirdly, it creates a legal framework for **data altruism**, allowing citizens and businesses to make their data more freely available for the benefit of society, under the auspices of so-called data altruism organisations. Such organisations may choose to undergo a prior registration in the EU if they meet the applicable requirements (including that they must be independent, and may not be for profit), thereafter being permitted to refer to themselves as "data altruism organisation recognised in the Union". Furthermore, they must periodically report on their activities.
- And fourthly, it creates a **framework for cooperation, supervision, and enforcement of these rules**, including both national competent authorities and a new European Data Innovation Board. The latter is charged with advising and assisting the Commission in developing a consistent practice of public sector bodies, competent bodies and competent authorities, advising on the prioritisation of cross-sector standards, advising on interoperability of data, and facilitating the cooperation between national competent authorities through capacity-building and the exchange of information.

The proposal thus contains very relevant ideas on privacy preserving data sharing, data sharing service providers as an independent service, and data altruism in particular. With respect to governance too, the emphasis on independent supervision and complaints resolution can be useful for ACROSS too.

3.5.2 Applicability to the ACROSS project

While not final or binding at this stage, the Act contains several components that could be usefully integrated into ACROSS. These include notably the following:

- The new re-use rules contain explicit provisions in relation to the use of so-called "**pre-processed data**", where such pre-processing by public sector bodies aims to **anonymize or pseudonymise personal data or delete commercially confidential information before allowing it to be re-used**

by third parties, and to the use of secure processing environments (a legally defined concept) when this is required to safeguard the interests in the data.

- The new framework for **providers of data sharing services** (including the legal and procedural safeguards to ensure their **independence and trustworthiness**, and the **quality of their services**) could be used as an input for the creation of any intermediaries that would intervene as a trusted third party in making data accessible (including by pre-processing it where necessary or by providing dynamic data services) to public sector bodies.
- Finally, the Governance Act makes it clear that there should be **supervision** over data sharing ecosystems, which could comprise mechanisms such as audits, certification, notification or registration, and authorisation. In more practical terms, complaints handling mechanisms must be available.

Since the Data Governance Act is still in a proposal stage, it would be imprudent to rely too strongly on its potential impacts. None the less, the issues mentioned above could certainly prove to be beneficial in order to build an efficient and trustworthy ACROSS governance framework.

3.5.3 Summary overview of resulting legal requirements

Based on the overview provided above, a shortlist of legal requirements can be derived in relation to data governance and data sovereignty. As in prior sections, requirements that were already represented elsewhere (e.g., under the GDPR or SDGR sections above) are not reprised here in order to avoid overlaps. These cover several key governance and sovereignty principles already, including the role of consent and citizen rights in relation to the ACROSS platform.

Table 4 - Legal requirements related to data governance and sovereignty

Identifier	Description
GS-01	The ACROSS platform must have clear **decision making mechanisms** in relation to architecture, standardisation, scoping and data usage rules. These can be kept lightweight given ACROSS' status as a research project, but they must be transparent to the citizens, and should never be able to deviate from the primacy of citizen consent.
GS-02	The ACROSS architecture should **create and promote privacy preserving data access** mechanisms**.** While using them should not be mandatory, service providers in particular should be incentivised to assess whether more privacy preserving data access (notably based on smaller or pseudonymous data sets) wouldn't also meet their needs.

Identifier	Description
GS-03	Governance of the ACROSS platform should be **independent and not for profit,** in the sense that it should not be controlled or unduly influenced by the interests of service providers, and that the platform itself should not aim to gain commercial profits or benefits from the data that it holds without the consent of the citizen.
GS-04	The ACROSS platform should establish a **complaints handling mechanism,** so that citizens can direct specific problems to the ACROSS project itself. This does not mitigate or diminish the legal responsibility and liability of service providers, but should provide practical assistance to citizens who may struggle to identify responsible parties themselves.

4 Summary of legal requirements and foundational legal principles

4.1 Summary of the legal requirements and deriving foundational legal principles

The analysis above shows that there are several legal frameworks that already affect the rights of citizens, and the obligations of operators and service providers relying on the ACROSS platform. It also shows that much of the legal framework is in very significant flux, as almost every single topic is presently under review, under amendment, or incomplete:

- The GDPR is clearly mature and established, but the e-Privacy Directive is still under review and may be replaced by an e-Privacy Regulation in the course of the project;
- The SDGR is complete, but an Implementing Act is still only available in a draft stage;
- The eIDAS Regulation is mature and established, but a newly proposed amendment was released one month prior to submission of this deliverable;
- A new Data Governance Act was proposed, and may be adopted in the coming year, also potentially influencing the ACROSS project.

Thus, the present deliverable principally provides a snapshot of critical principles that are certain (or extremely likely) to remain stable for the duration of the project, even as the legal framework evolves and matures.

Attempting to somewhat simplify and derive some foundational legal principles in relation to each of the four topics explored in this deliverable, the following graphic arguably captures the most critical and stable elements:

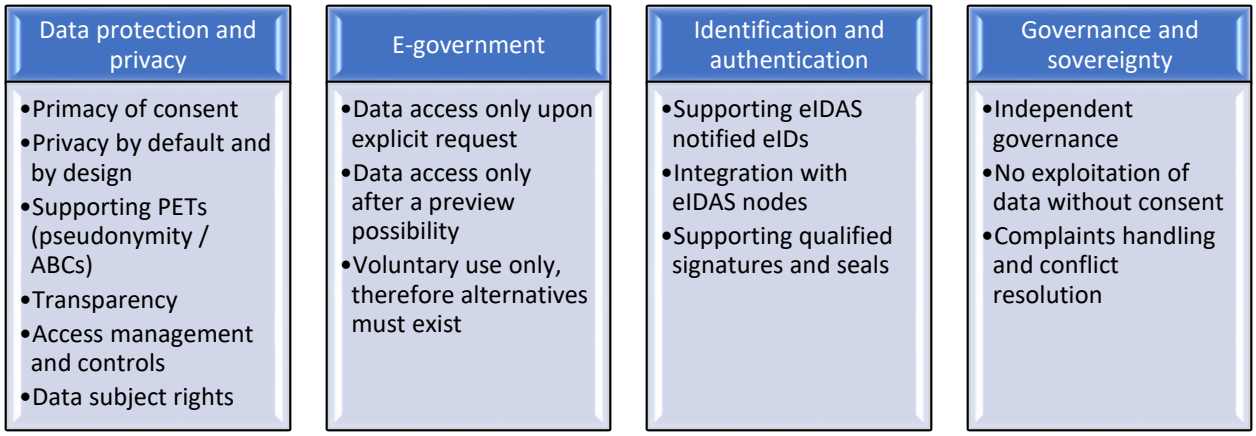

Figure 6 - Foundational legal principles

These principles will be developed further in the sections below, in order to arrive to a short, accessible and comprehensible statement of legal compliance principles in ACROSS.

Before doing so however, it is worth verifying the overview above by examining prior initiatives, and their approaches to user centric data governance.

4.2 Reality checking against prior initiatives

As was also explained in the ACROSS project proposal, ACROSS does not start from scratch. There is a range of prior research projects that have also aimed to create a mature user centric data governance model, each of which has managed to contribute a new element or perspective. From the perspective of the present deliverable, the two most relevant initiatives are arguably DECODE and MyData.

4.2.1 DECODE

The DECODE project [24] aims at creating tools that will give people ownership of their data. These tools combine blockchain technology with attribute-based cryptography to give the data owner control of how their data is accessed and used.

Apart from its architectural innovations, which focus on privacy by design and data minimisation approaches, it also produced a range of deliverables with specific legal relevance, including notably:

- A report describing Privacy Design Strategies for the DECODE architecture [25]. This report principally describes how privacy by design can be implemented in architectures that rely on distributed ledger technologies, including in an IoT context.
- A report describing Privacy Interface Guidelines [26]. The report describes how interfaces can be established that facilitate compliance with data protection requirements, in terms of transparency and accessibility. The use of Digital Wallets is discussed, along with some of the main approaches to facilitate user control and user focus.
- A report describing Legal frameworks for digital commons - DECODE OS and legal guidelines [27]. The report reviews the legal frameworks that may hamper the building of digital commons (from free software to data) including the case in which such digital commons concern the use of personal data. Intellectual property legislation and licensing practices are reviewed (including common licenses), as well as the GDPR. Recommendations on facilitating data sharing in an open model are provided.
- A report describing a Legal Ontology to Support Smart Contracts in DECODE Scenarios [28]. The report examines how legal language can be modelled and implemented architecturally in DECODE pilot cases.

Collectively, DECODE takes a strong architectural perspective, focusing on how legal compliance needs can be implemented from a technical perspective. It thus shows a clear commitment to the privacy by design philosophy, and can be considered a good practice case on that topic.

4.2.2 MyData

The MyData project [29] is an initiative that aims to give individuals control over their data, and to be able to decide at a granular level what is done by whom with their data. It defines a specific model for human-centred personal data management and processing. The MyData infrastructure takes into account the different legal bases and requirements for personal data processing stemming from the GDPR. It furthermore fosters compliance with data protection laws and regulations by enabling individuals to exercise control over their personal information. The minimum requirement for MyData is that individuals have the right to access and use their personal data. From an architectural perspective, MyDate provides an open-source reference implementation of its architecture.

From a legal and policy perspective, one of its main outcomes is the Declaration Of Mydata Principles [30]. The Declaration contains a short and accessible statement of the main objectives that need to be achieved in order to realise its vision. Notably, it posits the following priorities:

HUMAN-CENTRIC CONTROL OF PERSONAL DATA

Individuals should be empowered actors in the management of their personal lives both online and offline. They should be provided with the practical means to understand and effectively control who has access to data about them and how it is used and shared.

We want privacy, data security and data minimisation to become standard practice in the design of applications. We want organisations to enable individuals to understand privacy policies and how to activate them. We want individuals to be empowered to give, deny or revoke their consent to share data based on a clear understanding of why, how and for how long their data will be used. Ultimately, we want the terms and conditions for using personal data to become negotiable in a fair way between individuals and organisations.

INDIVIDUAL AS THE POINT OF INTEGRATION

The value of personal data grows exponentially with their diversity; however, so does the threat to privacy. This contradiction can be solved if individuals become the "hubs" where, or through which cross-referencing of personal data happens.

By making it possible for individuals to have a 360-degree view of their data and act as their "point of integration", we want to enable a new generation of tools and services that provide deep personalisation and create new data-based knowledge, without compromising privacy nor adding to the amount of personal data in circulation.

INDIVIDUAL EMPOWERMENT

In a data-driven society, as in any society, individuals should not just be seen as customers or users of pre-defined services and applications. They should be considered free and autonomous agents, capable of setting and pursuing their own goals. They should have agency and initiative.

We want individuals to be able to securely manage their personal data in their own preferred way. We intend to help individuals have the tools, skills and assistance to transform their personal data into useful information, knowledge and autonomous decision-making. We believe that these are the preconditions for fair and beneficial data-based relationships.

PORTABILITY: ACCESS AND RE-USE

The portability of personal data, that allows individuals to obtain and reuse their personal data for their own purposes and across different services, is the key to make the shift from data in closed silos to data which become reusable resources. Data portability should not be merely a legal right, but combined with practical means.

We want to empower individuals to effectively port their personal data, both by downloading it to their personal devices, and by transmitting it to other services. We intend to help Data Sources make these data available securely and easily, in a structured, commonly-used and machine-readable format. This applies to all personal data regardless of the legal basis (contract, consent, legitimate interest, etc.) of data collection, with possible exceptions for enriched data.

TRANSPARENCY AND ACCOUNTABILITY

Organisations that use a person's data should say what they do with them and why, and should do what they say. They should take responsibility for intended, as well as unintended, consequences of holding and using personal data, including, but not limited to, security incidents, and allow individuals to call them out on this responsibility.

We want to make sure that privacy terms and policies reflect reality, in ways that allow people to make informed choices beforehand and can be verified during and after operations. We want to allow individuals to understand how and why decisions based on their data are made. We want to create easy to use and

safe channels for individuals to see and control what happens to their data, to alert them of possible issues, and to challenge algorithm-based decisions.

INTEROPERABILITY

The purpose of interoperability is to decrease friction in the data flow from data sources to data using services, while eliminating the possibilities of data lock-in. It should be achieved by continuously driving towards common business practices and technical standards.

In order to maximise the positive effects of open ecosystems, we will continuously work towards interoperability of data, open APIs, protocols, applications and infrastructure, so that all personal data are portable and reusable, without losing user control. We will build upon commonly accepted standards, ontologies, libraries and schemas, or help develop new ones if necessary.

MyData has a strong focus on citizen consent and citizen's rights, but also (and arguably more importantly) on the creation of infrastructure that makes its possible and even easy to enforce these rights on an architectural level.

5 Conclusions and next steps

5.1 Principal findings

This deliverable has provided a concise overview of the main legal frameworks that apply to the ACROSS project, covering four specific legal policy areas:

- **Privacy and data**
- **e-Government and public services**
- **Identification and authentication**
- **Governance and sovereignty**

For each of these policy areas, the applicable legislation was analysed, and relevant legal requirements were extracted. These are listed in a single table in Annex 7.2 of this deliverable.

This work was cross-checked against other leading projects, notably DECODE and MyData, which affirms the validity of the analysis, and particularly emphasises the importance of privacy by design and user control (including consent), to be built into the ACROSS architecture. While the emphasis of each project differs, this shows that there is a mature baseline to be built on.

From a legal perspective, it was also highlighted that the legal framework is particularly evolutive across the EU at this point in time, with virtually every relevant legislation that applies to ACROSS presently under review or merely in draft stage. This implies that the present deliverable will need to be maintained over time in the course of Work Package 3 efforts.

None the less, a few stable and cross cutting priorities can be extracted, that will undoubtedly remain stable as the central legal pillars to the ACROSS project. These are summarised below.

5.2 Statement of legal compliance principles in ACROSS

General objective

The ACROSS project aims to provide a state of the art user-centric personal data management system, that allows citizens to keep control over their data, including by whom it can be accessed or used, and for which purpose. The ACROSS infrastructure aims to be sufficiently mature to be usable in environments with high confidentiality and security requirements, including in the public sector and for sensitive types of personal data. It therefore was designed to comply with European legal frameworks, including in relation to fundamental rights.

Turning principles into architecture

Privacy by design and privacy by default are central principles behind ACROSS. This implies that the legal compliance principles should not just exist on paper, but must be actively promoted towards all users and stakeholders, and that they should be built into the ACROSS architecture wherever possible. In this way, compliance is not only possible, but actively facilitated.

Principles in relation to data protection and privacy

ACROSS is built on the **primacy of consent** of the individual user. Users should be able to choose which data is available through the ACROSS infrastructure, to whom, and for what purpose. No exploitation (including commercialisation or direct marketing) of user data should occur without their consent.

ACROSS supports **privacy enhancing technologies**, including by supporting and promoting pseudonymous information exchanges where this meets the objectives of a specific use case.

ACROSS supports **access management and controls**. Users should be to grant, deny or terminate access to their data with equal ease, in a sufficiently granular manner to enable effective control.

ACROSS provides **transparency.** Users should be able to see who has (had) access to their data at all times, and who is responsible for complying with data protection laws. Contact information should be easily available to them at all times.

ACROSS supports **data subject rights.** Users should be able to access, amend, correct and/or delete their data at all times, and to be able to obtain a copy of it. Wherever possible, exercising these rights must be built into the architecture; users should not just be referred to a third party if ACROSS is capable of helping.

ACROSS supports **secure storage and exchange.** User data should not be exposed to third parties without user consent, and it should be protected against loss or corruption.

Principles in relation to e-government

ACROSS supports **user control, also towards public authorities.** User data should not be shared with public authorities without the explicit request of the user, and users should always be able to review information before it is shared with public authorities.

ACROSS supports **free choice.** For that reason, the ACROSS platform should never be the only option for citizens, since that would make ACROSS mandatory in some situations, and thus no longer based on consent. An alternative should therefore always exist.

Principles in relation to identification and authentication

ACROSS supports regulated **European electronic identification schemes and European electronic identification infrastructure, in order to enable cross border transactions.** Use of such schemes is however not required to use ACROSS.

ACROSS supports regulated **European electronic signatures and seals, in order to enable cross border verification of the integrity and authenticity of exchanged information.** Use of such signatures and seals is however not required to use ACROSS.

Governance and sovereignty

ACROSS is governed **independently**, prioritising the interests of citizens at all times. Other stakeholder should be consulted, but ACROSS it should not be controlled or unduly influenced by the interests of service providers

ACROSS is governed **on a not-for-profit basis,** meaning that the platform itself should not aim to gain commercial profits or benefits from the data that it holds without consent of the citizens.

ACROSS supports **accessible complaints resolution**. The platform will facilitate alternative dispute resolution mechanisms, and will provide a complaints handling mechanism.

Through these legal compliance principles, ACROSS believes that it can achieve its vision of legally compliant citizen centric information sharing, while ensuring data sovereignty of the citizens.

5.3 Roadmap for future legal work in ACROSS

It is clear that this deliverable – due already in month 6 of the ACROSS project – is not the final word in terms of legal requirements and compliance. To the contrary, it only represents an initial exploration of legal needs and requirements, based on a thorough examination of relevant EU level legislation, and of the best practices established by comparable initiatives in Europe. Both the legislation and the project will however continue to evolve, and the requirements identified in this deliverable will therefore need to be evaluated, maintained and updated over time. Moreover, practical follow-up steps will be needed (e.g. drafting consent statements, transparency notices, data exchange agreements, data protection impact assessments, and so forth.

With that in mind, the analysis in this report will be continuously updated as the project evolves, and more concrete outputs and legal template texts will be drafted, which can also be tested during piloting. Admittedly, piloting in ACROSS is intended to happen based on personas (credible but fictitious persons), so that formal legal texts are not legally essential. None the less, piloting should be realistic from a legal perspective too, and a robust legal follow-up strategy will ensure future usability of ACROSS results.?

All findings and lessons learned will be collected in D3.7 - Legal report, which is due at the end of the project. Interim updates will be provided through the periodic reports.

6 References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance); see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[2] Charter of Fundamental Rights of the European Union, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

[3] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32018R1725

[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended; for a consolidated version, see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219

[6] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), see https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

[7] TechDispatch #3/2020 - Personal Information Management Systems, 6 January 2021, from the European Data Protection Supervisor; see https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information_en

[8] Opinion 9/2016 - EDPS Opinion on Personal Information Management Systems - Towards more user empowerment in managing and processing personal data; see https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_en.pdf

[9] European Commission, DG Internal Market, Industry, Entrepreneurship and SMEs - The single digital gateway; see https://ec.europa.eu/growth/single-market/single-digital-gateway_en

[10] Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R1724

[11] Commission draft implementing regulation (EU) …/… of ... 2021 setting out technical and operational specifications of the technical system for the cross-border automated exchange of evidence and application of the "once-only" principle in accordance with Regulation (EU) 2018/1724 of the European Parliament and of the Council, 4 June 2021; see https://data.consilium.europa.eu/doc/document/ST-9289-2021-INIT/en/pdf

[12] The Once-Only Project (TOOP); see https://www.toop.eu/

[13] Digital Europe For All (DE4A); see https://www.de4a.eu/

[14] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[15] Overview of pre-notified and notified eID schemes under eIDAS; see https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[16] eIDAS node code version 1.5; see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+version+2.5

[17] eIDAS-Node Implementation Country Overview; see https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview

[18] EU Trusted list browser; see https://webgate.ec.europa.eu/tl-browser/#/

[19] Overview of eIDAS Implementing Acts; see https://ec.europa.eu/futurium/en/content/eidas-implementing-acts.html

[20] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, 3 June 2021; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN

[21] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'); see https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32000L0031

[22] Description derived from the European Parliamentary Research Service Ideas Paper on Digital sovereignty for Europe; see https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI%282020%29651992_EN.pdf

[23] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), 25 November 2020; see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[24] DECODE Project; see https://decodeproject.eu/

[25] DECODE Privacy Design Strategies for the DECODE architecture; see https://decodeproject.eu/publications/privacy-design-strategies-decode-architecture-0

[26] DECODE Privacy Interface Guidelines; see https://decodeproject.eu/publications/privacy-interface-guidelines

[27] DECODE Legal frameworks for digital commons - DECODE OS and legal guidelines; see https://decodeproject.eu/publications/legal-frameworks-digital-commons-decode-os-and-legal-guidelines

[28] DECODE Legal Ontology to Support Smart Contracts in DECODE Scenarios; see https://decodeproject.eu/publications/decode-legal-ontology-smart-contracts

[29] MyData Project; see https://mydata.org/initiatives/

[30] Declaration Of Mydata Principles; see https://mydata.org/declaration/

7 Annexes

7.1 Annex II of the SDGR – online procedures to be covered by the SDGR's technical system

Procedures referred to in Article 6(1)

Life events	Procedures	Expected output subject to an assessment of the application by the competent authority in accordance with national law, where relevant
Birth	Requesting proof of registration of birth	Proof of registration of birth or birth certificate
Residence	Requesting proof of residence	Confirmation of registration at the current address
Studying	Applying for a tertiary education study financing, such as study grants and loans from a public body or institution	Decision on the application for financing or acknowledgement of receipt
	Submitting an initial application for admission to public tertiary education institution	Confirmation of the receipt of application
	Requesting academic recognition of diplomas, certificates or other proof of studies or courses	Decision on the request for recognition
Working	Request for determination of applicable legislation in accordance with Title II of Regulation (EC) No 883/2004 [1]	Decision on applicable legislation

	Notifying changes in the personal or professional circumstances of the person receiving social security benefits, relevant for such benefits	Confirmation of receipt of notification of such changes
	Application for a European Health Insurance Card (EHIC)	European Health Insurance Card (EHIC)
	Submitting an income tax declaration	Confirmation of the receipt of the declaration
Moving	Registering a change of address	Confirmation of deregistration at the previous address and of the registration of the new address
	Registering a motor vehicle originating from or already registered in a Member State, in standard procedures [(2)]	Proof of registration of a motor vehicle
	Obtaining stickers for the use of the national road infrastructure: time-based charges (vignette), distance-based charges (toll), issued by a public body or institution	Receipt of toll sticker or vignette or other proof of payment
	Obtaining emission stickers issued by a public body or institution	Receipt of emission sticker or other proof of payment
Retiring	Claiming pension and pre-retirement benefits from compulsory schemes	Confirmation of the receipt of the claim or decision regarding the claim for a pension or pre-retirement benefits

	Requesting information on the data related to pension from compulsory schemes	Statement of personal pension data
Starting, running and closing a business	Notification of business activity, permission for exercising a business activity, changes of business activity and the termination of a business activity not involving insolvency or liquidation procedures, excluding the initial registration of a business activity with the business register and excluding procedures concerning the constitution of or any subsequent filing by companies or firms within the meaning of the second paragraph of Article 54 TFEU	Confirmation of the receipt of notification or change, or of the request for permission for business activity
	Registration of an employer (a natural person) with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Registration of employees with compulsory pension and insurance schemes	Confirmation of registration or social security registration number
	Submitting a corporate tax declaration	Confirmation of the receipt of the declaration
	Notification to the social security schemes of the end of contract with an employee, excluding procedures for the collective termination of employee contracts	Confirmation of the receipt of the notification
	Payment of social contributions for employees	Receipt or other form of confirmation of payment of

		social contributions for employees

7.2 Summary table of legal requirements identified in this report

Identifier	Description
DP-01	Any citizens are free to choose to use the ACROSS infrastructure, on the basis of their **consent,** which must satisfy the requirements of the GDPR. This implies that alternatives must be available, and that consent can be withdrawn, which must result in their data being removed from the platform. This legal basis doesn't necessarily apply to the service providers use of any received information.
DP-02	Any platform operator of the ACROSS infrastructure **may not use the data for other purposes** than those to which the citizen consented. This includes a prohibition on tracking, profiling, data selling or trading, surveillance, or direct marketing – except where a user consented to this.
DP-03	Given the consent requirement, the ACROSS platform **may not be used by minors under 13 without parental consent,** nor by any other persons who are not capable of providing legally binding consent.
DP-04	ACROSS must implement policies and interfaces towards the service providers that **specify what service providers are allowed to do, and what they are not allowed to do.** This includes a clear communication of the purposes of use, and a legal commitment to respect this constraint; and implementation of the data minimisation principle – no service provider may request more data than they strictly need.
DP-05	ACROSS must foresee **transparency notices** that inform citizens of their rights and of the key features of ACROSS.
DP-06	ACROSS must foresee features that ensure that **no personal data is shared with third parties without user consent.**
DP-07	ACROSS must foresee **transparency interfaces towards the citizens** that allow them to manage data storage, availability and use, including at a service provider specific level, and that allow them to monitor present and past use of the platform (including any prior authorised data exchanges).

DP-08	ACROSS must foresee **data subject rights interfaces**, allowing citizens to see, update and delete their personal data on the ACROSS platform; and that allow them to obtain copies of that data (data portability).
DP-09	ACROSS must implement **storage limitation policies –** by default, data should be deleted after a pre-set period of time, which the citizen may set or modify.
DP-10	ACROSS must implement the **data protection by default principle,** meaning that any data protection features must be enabled (not disabled) by default. This includes data deletion by default after a set period of time, and no sharing or monetisation of data by default (without user consent).
DP-11	ACROSS must implement appropriate technical and organisational **security** features. At a minimum, this entails: • Access controls: data on the platform may not be accessible to third parties without citizen consent. Data can be effectively encryption, and/or it may be protection by other suitable access controls (such as multifactor authentication). • Transfer controls: any personal data sent from the ACROS infrastructure to a service provider must be protected against unlawful interception through effective encryption. • Logging and audit trails: exchanges of information to and from the ACROSS infrastructure must be logged in a way that allows interactions to be identified and examined. Logs should comprise metadata only.
DP-12	ACROSS must implement **third country transfer controls,** meaning that the citizen must be able to see whether data will be sent to a recipient outside of the EEA prior to consenting to sending that data. The transfer must satisfy the requirements of the GDPR.
DP-13	Prior to piloting, a **data protection impact assessmen**t should be conducted on the general ACROSS architecture, given the innovative use of new technologies that can conceptually pose risks to the rights and interests of the citizens.
DP-14	Both the platform operators and any service providers with whom the citizen chooses to interact must be **clearly and unambiguously identified to the citizen,** including a description of their role and responsibility.
SDG-01	Citizens must always have an **alternative** to using the ACROSS infrastructure. The alternative may be electronic, analogue or physical, but the alternative may not be made artificially difficult or inaccessible.
SDG-02	Recipients of information from the ACROSS infrastructure must always be able to determine the **identity of the entity that issued it**. This may be a private entity, public authority, or the

	citizen itself; and the identity may be a pseudonym; but the identity must always be assessable to relying parties.
SDG-03	No information exchange relating to the citizen may occur via the ACROSS platform without the **prior request** from the citizen.
SDG-04	Prior to exchanging any information relating to the citizen, the citizen must be **given the opportunity to view the information, and to decide whether to proceed or cancel.** It is not mandatory that the citizen actually previews the information; it must only be possible for them to do so.
SDG-05	If the citizen decides not to exchange any information via the ACROSS system after previewing it, **then this may not be visible to the relying party.** The relying party should only be able to detect whether an exchange was successful or not, but not whether the failure occurred before or after a preview. Otherwise, the ACROSS platform inadvertently creates a profiling option, since citizens who decide to cancel an exchange after previewing the information may be considered as suspicious profiles.
SDG-06	Information exchanges must be **granular.** I.e. when multiple sets of information have to be provided to relying parties, the citizen should be able to select which sets of information (if any) it would like to exchange; the decision should not be 'all or nothing'.
SDG-07	In order to support **once-only** information exchanges, the ACROSS architecture should be conceptually capable of retrieving data from one source and sending it to its destination in a single integrated step, rather than requiring multiple and unconnected actions from the citizen.
IA-01	The ACROSS architecture must be capable of **supporting eIDAS notified identification.** This implies both that it must be possible to log onto the platform using an eIDAS notified eID, and that service providers should be able to determine who the user is and whether they asserted their identity using an eIDAS notified eID, along with the level of assurance of that eID under the eIDAS Regulation. Note that this **doesn't imply that eIDAS notified eIDs must always or exclusively be used in ACROSS.** It is perfectly acceptable for non-eIDAS eIDs to be used. However, eIDAS notified eIDs must *also* be usable and recognisable as such, to allow usability of ACROSS for SDGR purposes.
IA-02	The ACROSS architecture must be capable of **supporting log-on through eIDAS nodes.** As above, this **doesn't imply that eIDAS nodes must always or exclusively be used in ACROSS.** However, eIDAS nodes must *also* be usable, to allow usability of ACROSS for SDGR purposes.
IA-03	The ACROSS architecture must be **capable of supporting electronic attestations of attributes** (attribute based credentials), including through **pseudonymous assertions.**

IA-04	Whenever **pseudonymous** transactions are done (including through pseudonymous electronic attestations of attributes), it should be possible to link these to an identifiable citizen with the assistance of third parties (i.e. fully anonymous assertions which are by definition entirely unverifiable should not be supported).
IA-05	The ACROSS architecture must be capable of **supporting qualified trust services, including qualified signatures and qualified seals.** This only entails that, when the ACROSS platform contains electronic information which is electronically sealed or signed at the qualified level, the architecture does not in any way change, modify , remove or corrupt these seals or signatures. Re-signing or re-sealing is therefore only permissible if the original signatures and seals remain intact and verifiable to relying parties.
IA-06	The ACROSS architecture must be capable of **supporting single sign-on for the citizens.**
IA-07	The **liability and responsibility** of ACROSS platform operators must be clearly and explicitly communicated to service providers interacting with the platform, including notably any exclusions in terms of monitoring, intervention, and quality/integrity/authenticity assurance.
GS-01	The ACROSS platform must have clear **decision making mechanisms** in relation to architecture, standardisation, scoping and data usage rules. These can be kept lightweight given ACROSS' status as a research project, but they must be transparent to the citizens, and should never be able to deviate from the primacy of citizen consent.
GS-02	The ACROSS architecture should **create and promote privacy preserving data access** mechanisms**.** While using them should not be mandatory, service providers in particular should be incentivised to assess whether more privacy preserving data access (notably based on smaller or pseudonymous data sets) wouldn't also meet their needs.
GS-03	Governance of the ACROSS platform should be **independent and not for profit,** in the sense that it should not be controlled or unduly influenced by the interests of service providers, and that the platform itself should not aim to gain commercial profits or benefits from the data that it holds without the citizen's consent.
GS-04	The ACROSS platform should establish a **complaints handling mechanism,** so that citizens can direct specific problems to the ACROSS project itself. This does not mitigate or diminish the legal responsibility and liability of service providers, but should provide practical assistance to citizens who may struggle to identify responsible parties themselves.