H2020-SC6-GOVERNANCE-2018-2019-2020

DT-GOVERNANCE-05-2018-2019-2020

ACROSS

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

D3.7 Legal Report

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	D3.7 Legal report
Work package	WP3
Nature	Report
Dissemination Level	Public
Date	30/04/2024
Status	Final
Editor(s)	Hans Graux, TLX , Jolien Clemens, TLX
Contributor(s)	-
Reviewer(s)	VARAM and GRNET
Document description	This deliverable will detail the legal work done in ACROSS explaining how the legal requirements which have been identified at the beginning of the project have been integrated into the results, as well as providing guidelines on how to implement and use the results in a legally compliant manner.

About

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

DISCLAIMER

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V1.1	24/10/2023	First draft	Jolien Clemens (TLX)
V.1.2	09/04/2024	Final draft ready for internal review	Hans Graux (TLX) Jolien Clemens (TLX)
V.1.3	25/04/2024	Updated version based on feedback made by partners	Jolien Clemens (TLX)
V.2.0	26/04/2024	Version ready for submission	Jolien Clemens (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 deliverable builds further on the initial deliverable D3.6 which provided the legal requirements in relation to the ACROSS project and its general functional and infrastructural vision. The purpose of this Deliverable is to reflect back on how these requirements that were initially identified were actually implemented into the results of ACROSS.

The legal requirements were gathered directly from applicable legislations, notably the data protection legal framework (the GDPR and the ePrivacy Directive), e-government and the once-only principle (the Single Digital Gateway Regulation or SDG), the identification and authentication requirements (the eIDAS Regulation) and the Data Governance Act.

Because these identified legal frameworks are of an ever-evolving nature, this deliverable takes into account important updates to the legal frameworks, notably the eIDAS 2 Regulation and the Implementing Act for the Single Digital Gateway Regulation. It also looks into some other legal frameworks that were not yet taken into account in the first deliverable, such as digital spaces and the Data Act.

Table of Contents

1 INTRODUCTION 1

1.1 PURPOSE AND SCOPE 1

1.2 APPROACH FOR WORK PACKAGE AND RELATION TO OTHER WORK PACKAGES AND DELIVERABLES 2

1.3 METHODOLOGY AND STRUCTURE OF THE DELIVERABLE 3

2 IMPLEMENTATION OF THE DATA PROTECTION LEGAL REQUIREMENTS 5

2.1 THE IDENTIFIED LEGAL FRAMEWORK AND LEGAL REQUIREMENTS 5

2.1.1 Update on the identified legal framework 5

2.1.2 The identified legal requirements 6

2.2 IMPLEMENTATION OF THE LEGAL REQUIREMENTS IN ACROSS 7

3 IMPLEMENTATION OF THE E-GOVERNMENT AND PUBLIC SERVICES LEGAL REQUIREMENTS 18

3.1 THE IDENTIFIED LEGAL FRAMEWORK AND LEGAL REQUIREMENTS 18

3.1.1 Update on the identified legal framework 18

3.1.2 Relevance for ACROSS 20

3.2 IDENTIFIED LEGAL REQUIREMENTS FOR ACROSS 21

3.3 IMPLEMENTATION OF THE LEGAL REQUIREMENTS IN ACROSS 22

4 IMPLEMENTATION OF THE IDENTIFICATION AND AUTHENTICATION LEGAL REQUIREMENTS 25

4.1 THE IDENTIFIED LEGAL FRAMEWORK AND LEGAL REQUIREMENTS 25

4.1.1 Update on the identified legal framework 25

4.1.2 Relevance for ACROSS 26

4.1.3 The identified legal requirements 28

4.2 IMPLEMENTATION OF THE LEGAL REQUIREMENTS 29

5 IMPLEMENTATION OF THE GOVERNANCE AND SOVEREIGNTY LEGAL REQUIREMENTS 32

5.1 THE IDENTIFIED LEGAL FRAMEWORK AND LEGAL REQUIREMENTS 32

5.1.1 Update on the legal framework 32

5.1.2 Relevance for ACROSS 33

5.2 IDENTIFIED LEGAL REQUIREMENTS FOR ACROSS 35

5.3 IMPLEMENTATION OF THE LEGAL REQUIREMENTS IN ACROSS 35

6 IMPACT OF NEW AND FUTURE LEGISLATIONS ON ACROSS 37

6.1 IDENTIFIED NEW AND FUTURE LEGISLATIONS 37

6.1.1 Data spaces in the European Union *37*
6.1.2 The European Data Act *40*
6.2 LEGAL REQUIREMENTS 42
6.3 HOW DOES ACROSS TAKE THEM INTO ACCOUNT? 43
7 CONCLUSIONS: LESSONS LEARNED 44
8 REFERENCES 45

List of Figures

FIGURE 1 STRUCTURE OF D3.7 3

List of Tables

TABLE 1 METHODOLOGY FOR ASSESSING THE IMPLEMENTATION STATUS 3
TABLE 2 IDENTIFIED DATA PROTECTION LEGAL REQUIREMENTS 6
TABLE 3 IMPLEMENTATION STATUS OF THE DATA PROTECTION LEGAL REQUIREMENTS 7
TABLE 4 IDENTIFICATION OF THE EGOVERNMENT AND PUBLIC SERVICES LEGAL REQUIREMENTS 21
TABLE 5 IMPLEMENTATION STATUS OF THE EGOVERNMENT AND PUBLIC SERVICES LEGAL REQUIREMENTS 22
TABLE 6 IDENTIFICATION OF THE IDENTIFICATION AND AUTHENTICATION LEGAL REQUIREMENTS 28
TABLE 7 IMPLEMENTATION STATUS OF THE IDENTIFICATION AND AUTHENTICATION LEGAL REQUIREMENTS 29
TABLE 8 IDENTIFICATION OF THE GOVERNANCE AND SOVEREIGNTY LEGAL REQUIREMENTS 35
TABLE 9 IMPLEMENTATION STATUS OF THE GOVERNANCE AND SOVEREIGNTY LEGAL REQUIREMENTS 35
TABLE 10 IDENTIFICATION OF THE LEGAL REQUIREMENTS IN NEW AND FUTURE LEGISLATIONS 42
TABLE 11 IMPLEMENTATION STATUS OF THE LEGAL REQUIREMENTS IN NEW AND FUTURE LEGISLATIONS 43

List of Terms and Abbreviations

Abbreviation	Definition
GDPR	General Data Protection Regulation
eIDAS	Electronic Identification and Trust Services
SDGR	Single Digital Gateway Regulation
UJSE	User Journey Service Engine
OOP	Once-Only Principle
OOTS	Once-Only Technical System
PIMS	Personal Information Management System
DGA	Data Governance Act

1 Introduction

1.1 Purpose and Scope

This report builds upon D.3.6 legal requirements which provided a detailed overview of the legal requirements in relation to the ACROSS project. As noted in this Deliverable, the pilot activities that happened within ACROSS were realistic, but were not based on real life scenarios, i.e. piloting was done through personas (realistic but fictitious use cases), so that non-compliance with the legal requirements had no impact on real persons or real situations.

None the less, the main objective of ACROSS is of course to deliver 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, D.3.6 assessed the applicable legal frameworks, and the legal requirements were identified therein.

This deliverable (**D.3.7 legal report**) is **reflective of nature** and aims to look at how the legal requirements that were identified at the beginning of the project have been implemented. It will provide a detailed overview of how the identified legal requirements have been integrated into the results. Therefore, we will not repeat the legal framework that was identified in D3.6 but will rather focus on the legal requirements checklists that were provided in this Deliverable, and identify how these have been implemented. However, for each of the identified applicable legal frameworks (i.e. data protection, e-government, identification and authentication and governance) the legal partner will identify any updates in the EU sphere regarding these frameworks (i.e. new relevant legislation, implementing acts, guidance by competent authorities which might be relevant to the ACROSS project. Additionally, for each of the requirements the legal team will assess the implementation status following the methodology that is explained below under section 1.3. Lastly, D3.6 will look into new legislation that has been introduced on EU level and the impact these might have on the ACROSS project and the way in which ACROSS already took these new legislations in account.

D2.7 (**legal and regulatory considerations**) will focus more on the legal and regulatory considerations when defining the user journey methodology and the co-creation and co-delivery tracks and processes for cross-border service delivery. Whereas, D3.7 gives the entire overview of the legal work that has been done in relation to the ACROSS project, D2.7 will provide the actual templates and compliance documents that were created during the project. Moreover, it will D2.6 identify any gaps with respect to the regulatory dimension of the project.

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 citizens to control how their data are created or used by businesses, governments, or data brokers, giving individuals the power to determine how their data can be used and by whom it can be used. The ACROS Data Governance Framework will be based on existing solutions such as:

- **The MyData Model** which was developed as part of the MyData project as an initiative to give individuals control over their data (i.e. human centric system), and to be able to decide at a granular level what is done by whom with their data[1];
- **The DECODE project** provided open source and privacy-enhancing tools that put individuals in control of whether they keep their personal data private or share it for the public good.[2] The tools that were developed during the course of this project were a cryptographic virtual machine, a blockchain stack, a modular mobile app to access services privately, a dashboard for data visualization and a passport scanner.

The results of this Work Package has been integrated in the ACROSS platform which has been created in Work Package 5 and demonstrates the functionality of the use cases in Work Package 6.

It must be noted that this Deliverable has been drafted based on input gathered from other deliverables:

- D3.5 implementation of the ACROSS Data Governance Framework for data sovereignty – Final
- D4.3 Components for adaptation for SDG, OOP, eEIDAS for National public services – Final
- D5.2 System Architecture and Implementation Plan – Final
- D5.5 ACROSS Platform Prototype and applications – Final

Of course, this specific Deliverable is closely linked to D3.6 ("legal requirements") which provided the initial assessment of the legal framework and the legal requirements at the beginning of the project.

[1] For more information on the MyData model, we refer to the published White Paper which can be accessed through the following link: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78439/MyData-nordic-model.pdf?sequence=1&isAllowed=y.
[2] More information on the DECODE project can be found on the project website: https://decodeproject.eu/index.html.

1.3 Methodology and Structure of the Deliverable

Given the reflective nature of this report, the following structure and methodology is applied:

Figure 1 Structure of D3.7

This Deliverable will follow a similar structure as was followed in D3.6 ("legal requirements"): it will first look at the initial identified legal framework. Without repeating the description of the legal framework that was given in D3.6, this deliverable will nevertheless provide an update of the legal landscape (i.e. on new legislation, implementing acts, guidance by Competent Authorities, etc.). This is necessary as the European legal landscape is of a fast changing nature, and therefore identifying any changes to the existing legislation or new legislation is of paramount importance. The legal partner (Timelex) has closely monitored this legal landscape throughout the project in order to ensure that the ACROSS solution remains compliant with the new and changing legislations on EU level.

For each of the identified legal requirements the level of implementation will be scored using the following methodology:

Table 1 methodology for assessing the implementation status

Implementation status	Description
Fully implemented	The legal requirement has been fully implemented in ACROSS.
Partially implemented	The legal requirement has been partially implemented in ACROSS. There are only minor discrepancies between the status quo in ACROSS and the legal requirement that was identified. This partial implementation can be justified by the project partners.
Not implemented	The legal requirement has not been implemented in the project.
Not applicable	The legal requirement has been justified to be not applicable.

Finally, this Deliverable will also look into any **new and future legislations** that have emerged during the course of the ACROSS project, i.e. legislation on EU level that are currently still in the proposal phase or have been newly adopted during the project course and which have an impact on ACROSS (and specifically on the organization(s) that would further exploit ACROSS). This is important as by staying informed about upcoming changes, the project partners can anticipate and ensure that the ACROSS platform and framework is compliant with any relevant laws and regulations, thereby also ensuring the long-term sustainability of the project.

2 Implementation of the data protection legal requirements

2.1 The identified legal framework and legal requirements

2.1.1 Update on the identified legal framework

As explained in detail in D3.6 the main applicable data protection legal framework will be the **General Data Protection Regulation (GDPR)**, which outlines the requirements for a fair and lawful processing of personal data.[3]

Next, the **ePrivacy Directive** was also identified as a legal framework that needed to be taken into account.[4] Whereas, most rules in this Directive specifically addresses the telecommunications industry and are not applicable to personal information management systems (PIMs) such as ACROSS, it was not discussed in great detail. 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. The default rule in the ePrivacy Directive is that 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.

D3.6 also discussed the fact that the abovementioned ePrivacy Directive has been under revision for quite some time to better align with the GDPR rules. The status of the **ePrivacy Regulation** (the revised ePrivacy Directive) remains uncertain and has been so for almost 6 years as the initial proposal dates back to 2017. The proposal seems to be stalled in the council stage where the presidencies have been unable to reach compromises on essential parts of the proposal. We can therefore conclude that the same ePrivacy Directive principles and requirements as described in D3.6 remain applicable and that there will be no changes to this framework within the nearby future.

[3] 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).
[4] 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).

2.1.2 The identified legal requirements

Table 2 identified data protection legal requirements

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 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.

2.2 Implementation of the legal requirements in ACROSS

Table 3 implementation status of the data protection legal requirements

Identifier	Implementation status update	Status
DP-01	In the initial D3.6 it was identified that the **primarily legal basis** for both the platform operator and the service providers for the use of the personal data of the citizens is his or her **consent**. The consent under the GDPR is subject to certain conditions, namely it must be specific, freely given, unambiguous	

	and informed.[5] Moreover, the GDPR requires that the consent of the data subject is revokable (Article 7.3 GDPR). This means that the citizen should be able to choose to stop using the ACROSS platform, and to stop the additional data sharing with service providers, since both of these processing activities are based on the consent of the citizen. The consent requirements of the GDPR have been implemented in the ACROSS platform as follows: • The ACROSS platform provides a **consent management module** that enables citizens to manage their consents and to easily withdraw any prior given consents. In case a consent is withdrawn, the *future* data sharing with public and private service providers is immediately ceased. Note that in this case, the ACROSS platform operator will not require the third party who has received the citizens' data to delete the data which they had acquired prior to the withdrawal (the data sharing prior to the withdrawal of the consent was indeed lawful). Citizen users can in this case use the e-mail link which can be easily found in the ACROSS Platform (in the Service Description) to directly contact the DPO of the service provider to request a data deletion. The citizen user has been made aware of his/her data subject rights and specifically on the implications of his/her withdrawal of consent in the privacy policy. • Next, it goes without saying that users can also always **opt to stop using the ACROSS platform** altogether (by, removing the legal basis for processing via the ACROSS platform, and resulting in data deletion of any personal data stored on the platform.	
DP-02	With regards to the **principle of purpose limitation** it should be noted that the ACROSS platform is an intermediate service that enables data sharing between citizens and third party service providers upon request made by the citizen. Therefore, the ACROSS infrastructure allows trusted third parties to use their services if they promise to use the data for the purposes to which the citizen consented (i.e. respect of the principle of purpose	

[5] See Article 7 GDPR for the requirements of a valid consent.

	limitation is an essential requirement for lawful use of the platform by the service providers). Admittedly, the ACROSS platform operator cannot fully control what a service provider intends to do with the data they receive through the platform. The contractual approach between the ACROSS platform and the service providers and between the service provider and the end-user (citizen), does mitigate this risk of misuse significantly. The ACROSS platform takes an extra step in this regard by also enforcing a code of conduct[6] which specifically obliges service providers to only use the data which is provided through the platform for the purposes of which the user has been informed, and to which the user consented.	
DP-03	**Age verification control measures** have not yet been implemented on the ACROSS platform to ensure that children under 13 years old cannot use the platform without parental consent. The reasoning for this was the fact that the ACROSS platform was not yet used on real persons during the project, it was only tested during the assessment phase on individuals above the age of 18. However, this requirement can be easily enforced through eIDAS registration.	
DP-04	This legal requirements has been implemented in several ways: • The **code of conduct for service providers** attaches great importance to the data protection principles and in general to what is considered unacceptable behaviour by both a user and a service provider when using the ACROSS platform (e.g. discrimination, spread of false information and hate speech, hacking, etc.). • The **principle of data minimization** is enforced through the code of conduct[7] which obliges service providers to carefully consider what data is strictly necessary for the provision of services.	

[6] The ACROSS code of conduct can be found here: https://citizen-webapp-citizen-application-dev.k8s.across-h2020.eu/login?_gl=1*zdp6mk*_ga*MTc3NjQzNDMwMi4xNzEwOTI3MDM5*_ga_E593PVG4PL*MTcxMTY0MTYxOC4zLjEuMTcxMTY0MTY4MC4wLjAuMA..&_ga=2.20300283.2104651359.1711641619-1776434302.1710927039.

[7] The ACROSS code of conduct can be found here: https://citizen-webapp-citizen-application-dev.k8s.across-h2020.eu/login?_gl=1*zdp6mk*_ga*MTc3NjQzNDMwMi4xNzEwOTI3MDM5*_ga_E593PVG4PL*MTcxMTY0MTYxOC4zLjEuMTcxMTY0MTY4MC4wLjAuMA..&_ga=2.20300283.2104651359.1711641619-1776434302.1710927039.

	• Next, this principle is also enforced technically by the set-up of the ACROSS platform through the **template Service Description Data Model** (i.e. the service provider has to pre-define the data elements it will request from the users of the service). This also ensures that the platform operator maintains a clear oversight of the data that is asked by the service provider to deliver the services. When the ACROSS platform would be deployed in real life, this would also allow the platform operator to intervene in cases where they would notice that a certain service provider requests excessive information.	
DP-05	The ACROSS platform is designed with the transparency principle in mind. The **transparency dashboard** enables citizens to control the usage of their data by service providers and to manage their consents (i.e. grant, withdraw, deny). The users are also informed about among others the purpose, legal basis and the personal data requested by the service (mandatory and optional) through the service description in the service catalogue. Moreover, citizen users are informed about the processing of their personal data via the **privacy policy**[8] on the ACROSS platform, which provides detailed information on the personal data processed, purposes, retention periods, security measures, data subject rights, etc.	
DP-06	The ACROSS platform foresees features to ensure that data is not processed without user consent. These features are the following: • The **transparency dashboard** includes a consent management module which allows the citizen user to grant consent for the processing of his/her personal data by the service provider for each specific service in the service catalogue. Moreover, it allows the citizen to granularly define his/her consent (i.e. the citizen can	

[8] The Privacy Policy for the ACROSS Platform can be found here: https://citizen-webapp-citizen-application-dev.k8s.across-h2020.eu/login?_gl=1*fqdoml*_ga*MTc3NjQzNDMwMi4xNzEwOTI3MDM5*_ga_E593PVG4PL*MTcxMjY0NjQ1NC40LjEuMTcxMjY0Njc5Ny4wLjAuMA..&_ga=2.136658162.315497993.1712646455-1776434302.1710927039.

	choose to click the "select all" option or "select only mandatory" or can select each data element separately, this means that no tick boxes are pre-ticked, and that the citizen has to provide an active and specific consent).
	• The transparency dashboard allows the citizen to have **an oversight of the consents he/she has given**. They can grant, deny or withdraw consents for individual service providers and services in the service catalogue:
	  ○ Grant: giving consent for a new service optional data element or enabling a previously denied consent;
	  ○ Deny: not giving a consent for a new service or for an optional data element (for mandatory data elements, consent is needed to initiate the service, a citizen can still decide not to grant a consent, but will in this case not be able to initiate the service. The citizen is sufficiently informed about this through the interfaces of the ACROSS platform);
	  ○ Withdraw: revoke a previously given consent. There is even a possibility to "revoke all consents".
	• Interfaces in the ACROSS platform **technically prevents the usage of personal data** by the service provider beyond the consents granted. When a service is requested by a citizen user, the User Journey Service Engine (UJSE) will check the consents to use personal data by that specific user for that service. Each time a service is used, the UJSE will update the data usage in the Transparency Dashboard so that the user is informed (this will be done by using event logs).	

DP-07	The ACROSS platform provides a personal data management web-application (i.e. **the transparency dashboard**) for citizens to manage and monitor how their data is being used and accessed by third parties. This is further enabled by the possibility for the citizen user to define data usage policies as an instrument to control the usage of their personal data. The citizen user can decide to activate the following data usage policies:	

	• Duration usage: this means that the service provider can only use the personal data for a specific pre-defined time period (starting date and time and end date and time can be pre-defined). It should be noted that in case the data usage is subject to a minimum data retention period set in national legislation, the citizen will not be able to limit this minimum retention period; • Usage notification: the user will be notified when the service provider uses the personal data. The citizen will in this case receive a notification through the Transparency Dashboard; • N times usage: the citizen user can restrict the amount of times that a certain service provider can access and use his/her personal data through the ACROSS platform. • Usage logging: the ACROSS platform has implemented a data access control component to ensure authorisation enforcement by restricting unauthorized access to data resources, by relying on role based models. Once the consents are granted and the data usage policies (this is an optional feature) are defined, the user can monitor the usage of their personal data through the Transparency Dashboard because all actions are logged as Event Logs and updates are notified through the Transparency Dashboard.	
DP-08	The ACROSS platform does indeed provide **data subject rights interfaces**. As already discussed above, ACROSS is an intermediate service that enables data sharing with third party (public and private) service providers, and therefore does not store any substantive personal data on the platform itself (only minimal account information, such as account name, password, and technical information on the usage of the platform). Nevertheless, ACROSS does facilitate the data subject rights of the citizen user by providing e-mail links to the DPO or data protection contact point of the relevant service provider. This means that the ACROSS platform does initiate the communication to the service provider, but it must be highlighted that the communication happens outside of the platform infrastructure. The platform operator will not and cannot intervene in this	

	interaction, since it is legally not allowed to monitor the communications between user and service provider (this is prohibited by Article 5 of the ePrivacy Directive which protects the confidentiality of private communications). The privacy policy does give detailed information to the citizens on how they can exercise their rights and what restrictions might be applicable, i.e. a request to delete personal data may be denied because a service provider might have a legal obligation to further process the personal data.	
DP-09	The **principle of data storage limitation** is also implemented both on the ACROSS platform itself and enforced towards the service providers: • **Within the ACROSS platform itself**, this principle is technically enforced, since data obtained from third party sources, shared with service providers, is deleted as soon as technically feasible. Substantive personal data is not stored on the platform (except of course account data and session data necessary to manage connections to service providers); • **Towards service providers**, storage limitations are difficult to enforce, since e.g. public sector service providers may sometimes legally required to retain data under national applicable law, e.g. by entering into official public registers. In this case, it is not legally possible (or desirable) to enforce lower storage limits. Nonetheless, to guide this issue to some extent, the Code of Conduct to which service providers sign up as part of their onboarding process to the ACROSS platform requires them to assess whether storage is strictly necessary (e.g. because it is legally required), and if not, then they may not store data locally, i.e. wherever possible, they may not use ACROSS as a source from which to create copies of the data – rather they should use ACROSS as a source from which to access data when needed for a specific transaction whenever this is possible (i.e. only when a citizen has initiated a certain service and provided the necessary consents).	

DP-10	The ACROSS platform has been designed with the **data protection by default** principle in mind. The sections above describe in great detail the data protection features that have been implemented on the platform to ensure compliance with the principle of purpose limitation, data minimization, transparency, etc. Moreover, the ACROSS platform does not allow any sharing or use of the personal data without the explicit consent of the user (this is the default rule). The User Journey Service Engine (UJSE) even technically prevents that the service provider can manipulate this process, i.e. obtaining personal data without the consent of the user is made impossible by the technical set-up of the platform. This is because the UJSE communicates with the Data Governance Framework (transparency dashboard) within the ACROSS platform to obtain information about whether the user has given consent or not and if there are any specific data usage policies applicable.	
DP-11	The ACROSS platform has implemented **high-level technical and organizational security measures**. The more technical deliverables (notably D4.9, D5.2, D5.5) and the Data Protection Impact Assessment (DPIA) provide more detailed information on the implemented security measures on the ACROSS platform.	
DP-12	Regarding the **transfer control measures** that are implemented on the ACROSS platform. Firstly, it must be noted that during the ACROSS project there has not been any collection of real user data on the ACROSS project (except during the co-creation sessions and usability testing sessions, but in this case the user data and session data was deleted immediately after the session ended. Users were also encouraged to use fake data in the testing phase). Moreover, the project is focussed on EU-based user journeys (the pilot countries were Germany, Greece and Latvia). This means that there were no third country transfers identified during the project. However, we are aware that beyond the scope of this project, the ACROSS project might be used for other use cases and even for travels for work/study to countries outside the EEA. Therefore, the legal/ethics team has decided to provide some guidelines with regards to data transfer	Not fully implemented during the project due to the fact that there were no identified data transfers, but

	control measures that should be implemented should the ACROSS platform be used in the future in such a way: • In cases where there is no adequacy decision for that third country[9], the citizens data can nonetheless be shared with a data recipient outside the EEA on the basis of his/her **explicit consent** (Article 49 a) GDPR). It is important to mention that the user should also be informed about the risks of the transfer of their data to that third country due to the absence of an adequacy decision for that country. Note that Article 49 1) a) GDPR requires an explicit consent, which means that this is held to a higher standard as the consent in Article 6 GDPR. • The "**explicit" requirement** for the consent means that the consent for the data transfer must be obtained through a positive and affirmative action, for example, by letting the citizen check an unchecked box in the transparency dashboard. This checkbox should state the following: "*By clicking this check box you explicitly consent to the transfer of your personal data to a third country, by doing so you are aware that by initiating this action that your personal data will be transferred to a third country that might not be subject to the same level of data protection as the level provided by the GDPR. Nevertheless, the ACROSS Platform has taken appropriate measures to ensure that your personal data remains secure and protected, for more information regarding data transfers, we refer to our Privacy Policy.* " • Moreover, the consent should be **specific** for a particular data transfer or set of transfers, i.e. the consent mentioned above should be asked for each service that is initiated by the user for a specific service provider, and not in general for that service provider.	guidance provided in this Deliverable.

[9] The EU Commission has the power to determine, on the basis of Article 45 of the GDPR whether a country outside the EU offers an adequate level of data protection. For more information on which countries have been recognized, we refer to the website of the EU Commission: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

	• Lastly, as with the legal basis consent under Article 6, the consent under Article 49 should also be revokable at any time. The withdrawal of consent by the user again only has an impact on any future data sharing, which means that any data sharing before the withdrawal of consent remains lawful.	
DP-13	Initially, the internal ACROSS legal/ethics team assessed the need for a DPIA in Ethics Deliverable D.8.13. Based on an analysis of the requirements in the GDPR and of the guidance from the European Data Protection Board[10], it was concluded **that no DPIA was necessary for ACROSS**. The principle consideration behind this decision was that the ACROSS platform would only be tested through personas ('fake persons'). This consideration was correct, however, the platform is intended to be used in the future for real life use cases, likely after the ACROSS project ends. The lack of a DPIA meeting the requirements of the GDPR could hamper the real-life usability of the platform, or at least would make the life of real-life platform users significantly harder, as they may need to complete one themselves. This led to the conclusion that a DPIA should be performed during the course of the ACROSS Project. Taking the above in account, the DPIA has not been preformed before the pilot activities, but rather in the third year of the project This was more beneficial as the legal partner (Timelex) could assess an almost finished product in comparison to an idea/concept which would have been the case if the DPIA would have been preformed at the beginning of the project. This allowed an in-debt assessment of the implemented data protection principles and technical and organizational measures. Moreover, performing a DPIA on an almost-finished product allows you to perform a more detailed risk analysis and to identify any action points. The action points that have been identified during the performance of the DPIA have been implemented in the ACROSS platform.	
DP-14	This last data protection requirement is fulfilled by: • Identifying the platform operator in the privacy policy;	

[10] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248rev.01.

	• The service providers are identified in the Service Catalogue. The Service Catalogue has a Personal Data Handling module which provides information on the Data Controller (identification and contact details, including contact details of the data protection officer of the service provider).	

3 Implementation of the e-government and public services legal requirements

3.1 The identified legal framework and legal requirements

3.1.1 Update on the identified legal framework

D3.6 gives a detailed overview of the **Single Digital Gateway Regulation (SDGR)** and its main rules and principles for cross-border automated exchange of evidence and the application of the 'once-only' principle ("OOP").[11] We will not repeat the general framework of the SDGR in this Deliverable, and we refer to the description in section in D3.6. However, it is important to highlight some of the recent legal developments with regards to the SDG, which are related and relevant for ACROSS.

D3.6 also touched upon the fact that the Commission was obliged to implement secondary legislation – a so-called Implementing Act – by 12 June 2021, which it had not done in time. The Implementing Act needed to set out the architectural and technical requirements for the Once-Only Technical System ('OOTS'), that is to be established by the European Commission in cooperation with the Member States. The Implementing Act (known as the Implementing Regulation 2022/1463) has been adopted on the 5th of August of 2022 and sets out the technical and operational specifications of the technical system for the cross-border automated exchange of evidence and the application of the 'once-only' principle (also known as the 'Once-only Technical System' or the 'OOTS').[12]

The key provisions of the Implementing Regulation are the following:

- **Objective and Scope**: The regulation aims to define the architecture, roles, obligations, and operational guidelines for the 'once-only technical system' (OOTS). It covers the exchange of evidence required for online procedures listed in Annex II to Regulation (EU) 2018/1724 and procedures in Directives 2005/36/EC, 2006/123/EC, 2014/24/EU, and 2014/25/EU.
- **Definitions:** Key terms are defined, including 'once-only technical system' (OOTS), 'evidence provider', 'evidence requester', and 'eDelivery Access Point'. These definitions are crucial for understanding the operational framework of the OOTS.

[11] 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, https://eur-lex.europa.eu/eli/reg/2018/1724/oj.

[12] Commission Implementing Regulation (EU) 2022/1463 of 5 August 2022 setting out technical and operational specifications of the technical system for 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1463.

- **Architecture and Components of the OOTS**: The regulation outlines the main components of the OOTS architecture, including the roles and obligations of the Commission, Member States, evidence requesters, evidence providers, and intermediary platforms in establishing the overall architecture of the OOTS. It emphasizes the importance of a log system for monitoring exchanges and delineates responsibilities for maintenance, operation, and security.
- **Operational Specifications**: Detailed operational specifications are set, including the process for evidence exchange, the use of the eDelivery Access Point for secure communication, and the establishment of a log system for transparency and accountability.
- **Security and Data Protection**: The regulation underscores the necessity of adhering to high standards of data protection and security, in line with existing EU data protection regulations (the GDPR). It mandates measures to ensure the integrity, confidentiality, and security of the data exchanged through the OOTS.
- **Implementation and Cooperation**: Member States are required to cooperate with the Commission in the establishment and operation of the OOTS. The regulation also allows for the development of detailed, non-binding technical design documents to support the implementation of the OOTS.

It is also worth mentioning that the Commission published an OOTS onboarding playbook which provides a check-list for each of the actors involved (i.e. evidence requesters, evidence providers, intermediary platforms, etc.) in order to implement the OOTS.[13]

Lastly, the Commission has published in September 2023 **an implementation report**[14], providing a comprehensive assessment of the implementation and the current functioning of the SDG. The report focusses on different aspects of the SDG:

- **Functioning of the SDG:** the report describes how the SDG currently operates, highlighting the progress made towards digitizing procedures and implementing the OOTS in Member States. The report also identifies areas for further improvement and expansion of the SDG to enhance eGovernement services, thereby supporting a competitive Single Market and facilitating the free movement of citizens.

[13] The onboarding playbook can be accessed through the following link: https://www.google.com/search?q=onboarding+playbook+OOTS&oq=onboarding+playbook+OOTS&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBCDYyMjhqMGo3qAIAsAIA&sourceid=chrome&ie=UTF-8.

[14] COM (2023) 534 Report from the Commission to the European Parliament and the Council – First Implementation Report on the Single Digital Gateway, 12 September 2023, https://single-market-economy.ec.europa.eu/publications/first-implementation-report-single-digital-gateway_en.

- **SDG Pillars**: the report furthermore focuses on the SDG pillars already available online through the "Your Europe" portal. These include information services, assistance services, and the feedback tool on the Single Market obstacles. It also discusses forthcoming SDG pillars related to online procedures and the OOTS. By the end of 2023, Member States are expected to ensure that administrative procedures in 21 key areas are made fully accessible online.

Despite the progress identified above, there are calls for Member States to dedicate sufficient resources to swiftly implement the SDG in a SME-friendly way, providing user-centered information on single market rules and administrative procedures. This is where ACROSS comes into the play: ACROSS provides a user-centered platform to access information on both public and private services (and their administrative procedures). In the section that follows we will zoom into the role that ACROSS can play in the SDG initiative of the EU.

3.1.2 Relevance for ACROSS

It is important to highlight again that the ACROSS project goes beyond the mere scope of a mere e-government initiative, i.e. it is not only a data exchange between 'covered entities' in the sense of the SDGR. The ACROSS platform is also open to be used by private service providers which are outside the scope of the SDGR if they are considered purely private sector transactions and have no administrative procedural aspect (i.e. opening a bank account, applying for a job with a privacy company, applying for a study grant with a private investment fund, etc.).

Next, the user-centric approach of the ACROSS project also goes beyond the objective of the SDGR, i.e. direct exchange of evidence between competent authorities without the need of the user as a middle-man (i.e. the citizen does not need to search and provide his/her own documentary evidence to the competent Authority). ACROSS goes further in the sense that it wants to give the citizen user control and ownership of his or her data and documents. Therefore, the user is in the steering wheel position, it can freely choose to interact with a certain public or private service provider (not only 'competent authorities' as defined under the SDG Regulation), and can also freely decide which documents/data it wants to share (not only 'evidence' as defined under the SDG Regulation). This is a completely different set-up as the SDG set-up, where the citizen does not hold the information, and pre-defined information ('evidence') can be interchanged between a closed network of competent authorities, for a pre-defined number of services (which are included in an Annex II to the SDG Regulation).

As was already stated in D3.6, the objective for ACROSS is not to follow each of the legal requirements of the SDGR and the implementing act in detail. Nevertheless, we want to highlight the high-level legal requirements in SDGR and the implementing act that have added value for all the ACROSS use cases (and not only the pure e-government services). These high-level legal requirements mainly focus on security and data protection of the information/documentation that is shared through ACROSS, such as:

- Having in place a *secure and appropriate system* allowing user identification (i.e. by supporting to use of eIDAS nodes for secure user authentication);
- *Supporting the once-only-principle in general* by eliminating the need for citizens to submit the same information/documentation multiple times to different public and/or private stakeholders in order to reduce administrative burdens and to improve the efficiency of both public and private services;
- *Transparency requirements* with regards to the data processing through the OOTS to ensure that the user can make an informed decision and making sure that the user have an option to view the "evidence" (documentation and data in general for ACROSS) that is going to be shared so that they can decide freely to proceed or not;
- *Logging requirements* with regards to the evidence transmitted through the OOTS;
- *Security requirement* with regards to monitoring and security incident reporting.

3.2 Identified legal requirements for ACROSS

Table 4 identification of the eGovernment and public services legal requirements

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.

3.3 Implementation of the legal requirements in ACROSS

The ACROSS components adaptation for SDG, OOP, eIDAS for National Public Services has been discussed extensively in D4.3, the table below will only provide a summarized overview of the implementation work that has been done. For any details in this regard, please refer to D4.3.

Table 5 implementation status of the eGovernment and public services legal requirements

Identifier	Description	Status
SDG-01	Although the option of using the ACROSS infrastructure is intended to make the life of citizen users easier, it is **not mandatory** for either the service provider or the citizen user to use the platform to exchange data and documents. The citizens can still decide to do the actual document sharing in person or through other means, e.g. by email. In no way, does ACROSS exclude any alternative data sharing mechanisms that may be available to the citizen.	
SDG-02	The identification of the Service Provider is done in the Service Catalogue (one of the main components of the ACROSS Platform). The services are	

	defined in the Service Catalogue by using the CPSV-AP model, which is recommended in the SDGR to ensure interoperability. The Service Catalogue also provides an IDS connector which allows a Citizen User and a Service Provider to exchange, share and process data in a secure way. The IDS connector provides a trusted layer, from an operation and governance point of view between the Service Connector, acting as a proxy invocation from the ACROSS platform and the actual external service.	
SDG-03	Data exchange in ACROSS can **solely take place on the basis of the explicit request of the citizen user**. The citizen can freely select the services (public or private) he/she wants to initiate, and will have to consent to the data sharing with these service providers (after having received detailed information on which data is going to be exchanged, for which purpose, etc.).	
SDG-04	The ACROSS platform (more specifically the transparency dashboard) allows the citizen user to browse through all the available services, and to receive **detailed information with regards to the requested data and documents** (prior to the exchanging of the information). When initiating a specific service (e.g. applying for a university), the user will be able to see the specific information that is requested (either mandatory or optional), and will be able to granularly grant consent to the data sharing with that specific service provider. The citizen will be able to decide at any point to stop the initiation process of that service.	
SDG-05	The service provider will not be informed by ACROSS about the fact that a citizen user decided not to share any information with that specific service provider after pre-viewing it. The service provider will also not be informed by ACROSS about the reasons for which the citizen user decided to withdraw his/her consent or decided not to grant a consent in the first place.	
SDG-06	The transparency dashboard includes a *consent management module* which allows the citizen user to grant consent for the processing of his/her personal data by the service provider for each specific service in the service catalogue. Moreover, it allows the citizen to **granularly define his/her consent** (i.e. the citizen can choose to click the “select all” option or “select only mandatory”	

	or can select each data element separately). The consent tick boxes will not be pre-ticked, and the user can granularly select which types of information it wants to share. We have to highlight the fact that for certain services, some data/information will need to be shared (mandatory). In that case, the citizen will not be able to initiate the service, if he/she does not grant consent for the data sharing of these mandatory data/information. The citizen will be informed of the mandatory/optional information before initiating the service. It will be the service provider that decides which data element/information that is requested will be mandatory or optional when they register their service in the service catalogue. However, the platform operator of ACROSS does have an important role here during the onboarding process of a new service provider, i.e. it needs to be checked for each of the requested data elements whether they are limited to what is strictly necessary for initiating that service.	
SDG-07	The **Once-Only Principle ('OOP')** is the core of the ACROSS platform. We refer to D4.3 ('components adaption for SDG, OOP, eIDAS for National Public Services – Final') for more information on how the ACROSS components are exactly adapted to the OOP. As will be explained below, the ACROSS platform uses the eIDAS Keycloak extension which provides components that are fully compliant with the OOP: users' data needed for accessing the services offered in ACROSS, need only to be registered once, in their respective national ID providers, and can be utilized for authentication and authorization services directly.	

4 Implementation of the identification and authentication legal requirements

4.1 The identified legal framework and legal requirements

4.1.1 Update on the identified legal framework

D3.6 provided an extensive overview of the applicable legislation, notably the **eIDAS Regulation**, which defines the EU level rules in relation to electronic identification, trust services, and electronic documents. As described in that deliverable, the legal framework is and remains very relevant to ACROSS, since the eIDAS Regulation describes the general requirements for electronic identification towards online public sector services across the EU. While ACROSS has a broader scope – since it can also be used towards private sector services, rather than eGovernment services only – the eIDAS Regulation thus remains the principal legal yardstick to determine the legal value of electronic identification solutions.

As was also highlighted in D3.6, the eIDAS Regulation is under revision, and a **proposal for an update to the eIDAS Regulation** was published in June 2021. Among other innovations, the proposal requires Member States to offer a **European Digital Identity Wallet** to their citizens – a mobile identification and authentication solution that can be used via their mobile devices such as smartphone. Such a Wallet should allow users to store identity data, credentials and attributes linked to their identity, and to:

> a) provide them to relevant relying parties on request and to use them for authentication, online and offline, for a service; and
>
> b) sign digital transactions via qualified electronic signatures.

While the amendment to the eIDAS Regulation has not yet formally gone through the full legislative process, the EU level negotiations around the proposal are far advanced. Following a range of amendments, the European Parliament adopted a compromise version on 29 February 2024, and after adoption by the Council, it will be published in the EU's Official Journal and enter into force. This is expected to occur before the next European elections.

Within a six month timeframe after the entry into force of the amendment, the eIDAS amendment will also require various Implementing Acts to be adopted in relation to the Wallets, including notably on:

- The core functionalities of the Wallets (art. 5a), specifically how they will ensure the safety and security of the technology, and their support for pseudonymous identification and electronic

signatures, as well as the possibility to exercise data subject rights towards relying parties with whom the user has interacted;

- Certification of the Wallets (art. 6c.4), i.e. the process for ensuring that the Wallets comply with a uniform EU level standard of security and trustworthiness;
- Wallet relying parties (art. 6b), i.e. the procedures and technologies to be used to ensure that third parties with whom the users interact are trustworthy;
- Publication of a list of certified Wallets EUDIW (art. 5b), i.e. the procedures and technologies to be used to verify that a specific Wallet indeed complies with EU level standards;
- Security breaches (art. 5e), i.e. the procedures for dealing with incidents that affect the security and trustworthiness of the Wallets, including specifically by notifying security breaches and revoking or suspending Wallets;
- Requirements for qualified attribute assertions (art.45d), i.e. the requirements that collectively ensure that information stored in the Wallet is trustworthy for any relying party;
- Verification of attributes against authentic sources (art.45e), i.e. the technologies through which information from the Wallet can be verified against official governmental databases;
- Requirements for attribute assertions issued by/on behalf of a public sector body (art.45f.6 and art.45f.7), i.e. requirements that must be implemented to ensure that a recipient of a document from a Wallet can determine that it originated from a governmental body;
- Cross border identity matching (art. 11a), i.e. the requirements to determine whether a specific user of a Wallet is already registered in a relying party's own databases as a user.

None of the texts above have been finalized or released to the public yet – neither the eIDAS 2 amendment, nor any of the Implementing Acts – but the ACROSS team has followed legislative and policy discussions closely throughout the project, and has been able to access and verify draft versions of the legal package under preparation.

4.1.2 Relevance for ACROSS

The eIDAS Regulation and its proposed amendments and implementing acts are highly relevant to ACROSS, for various reasons. Firstly, the existing eIDAS framework is a cornerstone of European digital policy, as a central building block that enables pan-European cross border identification and authentication. Essentially, to create a service at the EU level that supports secure identification and

reliable authentication services (as is required for ACROSS to function), support for the eIDAS framework is a basic requirement, as no other alternative is currently available that covers the entirety of the EU.

Secondly, it is clear that the future eIDAS revision will be based on mobile solutions with a strong emphasis on personal data governance. Wallets are expected to become a critical infrastructure to support digital citizen interactions in the EU in the future. While ACROSS did not intend to develop its own mobile identification and authentication solution, it was important to consider how interactions with future eIDAS Wallets would occur, both technologically and in practical terms, and to implement solutions that support the foundational principles of trustworthiness and user control that underpin the eIDAS amendment.

For that reason, it is important to note that ACROSS is built on several key principles that align directly with the expected evolutions of the eIDAS framework in the future. Firstly and of course most critically, ACROSS is centered around the concept of supporting used control and user governance over their own data. ACROSS is not a central data hub where the user's personal data is stored, but rather acts as a solution that allows the user to manage data sharing relationships. This decentralized model is very well aligned to the Wallet approach of eIDAS, where the Wallet can be used to identify the user and to manage interactions with other services, but where the data does not need to be stored in a single central location.

Moreover, the eIDAS amendment requires certain functionalities for which ACROSS has been able to pioneer certain solutions. By way of example, the eIDAS amendment requires that users can exercise their data protection rights towards third parties that have received the users' personal data via the Wallet. ACROSS has implemented a rudimentary solution that services this exact purpose for its platform, thus both demonstrating that the requirement is achievable in practice, and providing a potential technological solution.

As a second example, the eIDAS amendment will also contain certain legal obligations towards the relying parties that receive the user's data. This is done notably by imposing registration requirements on relying parties to ensure that they can be identified and trusted, and by creating an interface specification that ensures that the relying parties are authenticated before they can receive a Wallet user's data. This issue is tackled in ACROSS as well, by providing an onboarding framework for service providers on the ACROSS platform, including a statement of the service providers' rights and obligations within ACROSS. In this way, ACROSS end users have a relatively homogenous basis of trust, in the sense that service providers in ACROSS are bound by a baseline of legal obligations. Here too, ACROSS providers a valuable example to further EU level developments.

Inversely of course, ACROSS has also learned from the discussions around the EU level legal framework, including in relation to data subject rights, data protection and user control, which have been incorporated into the ACROSS platform. In that way, the requirements of the eIDAS framework have co-driven the design and implementation of ACROSS.

As noted above, the ACROSS project did not develop its own Wallet solution. However, it did assess interactions with mobile authentication solutions from other Horizon Europe projects such as mGov4EU, to ensure that these could indeed interact with ACROSS, and discussions around the EU level Architecture and Reference Framework for the EU Wallets were followed as necessary. Moreover, compatibility with the currently already existing eIDAS infrastructure (including national identification schemes and the eIDAS nodes) was tested and evaluated, as shown in the table below.

4.1.3 The identified legal requirements

The following legal requirements were already identified in earlier ACROSS deliverables in relation to identification and authentication:

Table 6 identification of the identification and authentication legal requirements

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.

4.2 Implementation of the legal requirements

Table 7 implementation status of the identification and authentication legal requirements

Identifier	Description	Status
IA-01	ACROSS incorporates the **Keycloak identity management server** which supports eIDAS notified identification. The **implementation status of the eIDAS nodes in ACROSS** is the following: • The connection to the German eID scheme is implemented through the use of middleware; • The Greek and Latvian nodes are connected directly to the ACROSS components. When a citizen wants to log-in for the first time on ACROSS, the user will have to follow a custom log-in process. First, the citizen will have to indicate his/her country of origin. After doing so, the citizen will be forwarded to the eIDAS specific connector. The citizen will need to login on the country's identity provider and provide the necessary authorizations, the user will then be redirected to Keycloak and will need to create an account.	

IA-02	There is a **working connection** between German and the Latvian eIDAS nodes. There is also a **working connection** between the German and the Greek eIDAS nodes. ➔ This means that Latvian and Greek citizens can be authenticated for services provided in Germany using their national eID, and vice versa. There is **not yet a full connection** between the Latvian and the Greek eIDAS nodes. The reason for this is that the Greek eIDAS node is not as of yet fully notified. This is however a shortcoming in the current eIDAS node implementation, not in the ACROSS project; the ACROSS platform is inherently capable of supporting any available eIDAS nodes.	
IA-03	Through the use of Keycloak, the ACROSS platform is capable of **supporting electronic attestations of attributes** (specifically in JSON format). An administrator (i.e. service provider) will need to set-up at least the attributes which are required by the eIDAS specifications and can also request additional optional attributes. After the citizen completes the above described log-in process in his/her country of origin, the set of requested attributes will be safely transmitted to the Keycloak server (which is acting as a eIDAS service provider).	
IA-04	The linkability requirement is satisfied through the support of eIDAS compliant notified electronic identification means, and communication via eIDAS nodes. Since these only function if the user authenticates fist, any pseudonymous transaction within the ACROSS platform is thereby linkable to an identifiable citizen with the assistance of eIDAS node operators (i.e. with support from the competent public sector authorities), provided that an eIDAS notified eID is used for the authentication of the users (since this is a prerequisite for enabling trustworthy cross border identifiability).	

IA-05	The support requirement in relation to qualified signatures and qualified seals is also satisfied, since ACROSS supports transfers of unmodified documents from their source without modification. Since the requirement relates only to protection of the integrity of signed or sealed electronic documents – and not to any ability to re-sign or re-seal, which would need to be done outside of the platform - original signatures and seals remain intact and verifiable to relying parties.	
IA-06	The ACROSS architecture supports single sign-on, as required.	
IA-07	The liability and responsibility of ACROSS platform operators is governed by a bespoke services agreement that was created in the course of the ACROSS project. During the onboarding of service providers on the ACROSS platform, the service providers are required to accept these terms, which include provisions in relation to the quality, integrity and authenticity of any information provided via the platform, and ACROSS' responsibilities and liabilities in this respect.	

5 Implementation of the governance and sovereignty legal requirements

5.1 The identified legal framework and legal requirements

5.1.1 Update on the legal framework

D3.6 already briefly introduced the new proposed legislation, known as **the Data Governance Act ("DGA")**.[15] The DGA entered into force on 23 June 2022, and has been applicable since September 2023 (following a 15 month grace period).

The key aspects of the DGA are the following:

- **Facilitating Data Sharing**: The DGA aims to stimulate the sharing of data among businesses, both against remuneration (a reasonable fee may be asked) and for other benefits. This includes a harmonized framework for data exchanges and setting basic requirements for data governance in order to increase trust. Operationally, the DGA establishes a novel framework for *data intermediation services*, which are services that connect data holders (individuals or companies) with data users to facilitate data sharing. These services may charge for facilitating the data sharing between the parties, but they cannot directly use the data that they intermediate for financial profit (i.e. by selling it to another company or using it to develop own products).
- **Public Sector Data Reuse**: It provides a framework for the reuse of public sector data, ensuring that such data can be made available for innovative and societal purposes, while respecting the existing rights of others.
- **Personal Data Spaces**: The Data Governance Act supports the creation of personal data spaces, designed to help individuals exercise their rights under the General Data Protection Regulation (GDPR), thereby enhancing control over their personal data.
- **Data Altruism**: It introduces a framework for the voluntary sharing of data by individuals or organizations for purposes that are beneficial to the society (the common good), without seeking financial compensation. The DGA introduces a specific framework to support data altruism in the EU by introducing a framework for the registration of so-called *data altruism organizations*. These organizations will collect and process data made available for altruistic purposes (they will provide trusted tools that will allow data to be shared in an easy way for the benefit of the society). Such organizations can register as an 'data altruism organization recognized in the Union' if they fulfil

[15] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.

certain specific requirements (i.e. must have a non-for-profit character and meet transparency requirements). When registered they will be subject to specific governance and operational and security requirements to ensure their trustworthiness.[16] Interestingly, these data altruism organizations will be required to provide specific tools for obtaining consent from data subjects (or permissions from data holders in case of organizations) for the altruistic use of their data. Additionally, there must be a possibility of an easy withdrawal of such consent or permission, ensuring individuals retain control over their data.

- **European Data Innovation Board**: on an operational level, it establishes a European Data Innovation Board that envisages to support the implementation of the data governance framework, by facilitating the exchange of best practices, promoting interoperability standards, and contributing to the development of common European data spaces in strategic sectors.

5.1.2 Relevance for ACROSS

It must be clear that the overall goal of ACROSS extends beyond mere data sharing and data altruism purposes. The ACROSS project aims to provide citizens with a trusted service for data sharing with cross-border private and public entities, while safeguarding the right to self-determination of the citizen regarding their personal data. Therefore, the data governance rules that are provided in the DGA are of importance to ACROSS as the main goal is to provide the citizen with a framework for data sovereignty.

At this stage, it is difficult to say whether ACROSS could qualify as either a data intermediation service or a data altruism service. On the website of the European Union, the EU lists as an example of a data altruism service, MyData Global, which has a similar objective, set-up and framework as ACROSS.[17] The implementation of the DGA with regards to the actual registration of data intermediation providers and data altruism organizations is still in a preliminary phase. Based on the latest information on the website of the European Union, in both the EU register of data intermediation services[18] and in the EU register of data altruism organisations[19], there is as of yet only one organization officially registered (Dataspace

[16] These requirements will be laid down in a specific rulebook (which will include information requirements, technical and security requirements, communication roadmaps and recommendations on interoperability standards The rulebook will be developed by the Commission, in close cooperation with data altruism organizations and other relevant stakeholders.

[17] See https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations which lists MyData Global as an example of a Data Altruism Organization.

[18] See https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services for the register of intermediation services.

[19] See https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations for the register of data altruism organisations.

Europe as Intermediation service, and Associacio Dades pel Benestar Planetari – Datalog as Data Altruism Organization).

Based on the above information, we can therefore carefully presume that the organization who would further exploit the ACROSS platform could qualify as a data altruism organization. Therefore, it is relevant to give an overview of the key conditions for qualifying as a data altruism organization:

- The organization must be a **legal person established in accordance with the laws of a European Member State**;
- The organization must operate on **a not-for-profit bases**: This is a crucial condition to ensure that the organization's activities are aimed at benefiting the general interest rather than generating profit for private stakeholders;
- **The organization must be legally independent**: The independence is necessary to avoid conflict of interest and to ensure that the organization's data altruism activities are not influenced by commercial considerations;
- There must be **a functional separation** between the organization's data altruism activities and any other activities it might carry out. This separation ensures that the data altruism activities are not compromised by other interests or objectives of the organization;
- **Compliance with the Rulebook**: The organization must comply with a Rulebook established by the European Commission, which outlines specific information, technical and security requirements for data altruism organizations. Compliance with the rulebook is essential to ensure that the organization adheres to high standards of data protection, security and ethical conduct. As of today, the Commission has yet to develop this Rulebook;
- **Registration in a Public National Register**: to be an official recognized data altruism organization in the European Union, the organization must apply for and be registered in a public national register of recognized data altruism organizations. This registration process involves submitting necessary information and demonstrating compliance with the conditions above (including the rulebook when established by the EU Commission);
- **Transparency and safeguards**: recognized data altruism organizations are subject to transparency requirements and must implement specific safeguards to protect the right and interests of data subjects and data holders. This includes providing mechanisms/tools for obtaining a valid consent, ensuring data security, and allowing for withdrawal of consent.

5.2 Identified legal requirements for ACROSS

Table 8 identification of the governance and sovereignty legal requirements

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.
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.

5.3 Implementation of the legal requirements in ACROSS

Table 9 implementation status of the governance and sovereignty legal requirements

Identifier	Description	Status
GS-01	The ACROSS platform has put in place a **clear data governance framework** allowing the users to monitor which data is requested by the service provider and ensuring user control by allowing them to make informed decision on data sharing (on the basis of their consent).	
GS-02	As described above, the service provider will need to register the service in the Service Catalogue (which is one of the main components of the ACROSS platform). The service provider will need to introduce the personal data (mandatory or optional) which will be requested	

	from the user when initiating the service. Nevertheless, ACROSS tries to incentivise service providers through the code of conduct[20] to request minimal information from users (i.e. only the information that is strictly necessary for offering the service).	
GS-03	During the course of the project this requirement was fulfilled, the ACROSS platform was governed by the ACROSS consortium. This legal requirement will mainly need to be taken into account when the platform would – after project end – be governed by an external party.	
GS-04	As stated as part of the general governance framework of ACROSS, the project has created a **code of conduct for service providers** which includes information on how a citizen user can notify to the ACROSS platform operator any non-compliance with general conduct rules and the GDPR principles. ACROSS even goes further in this aspect by putting in place an enforcement mechanism in case any non-compliance is reported: • The ACROSS platform operator will investigate any report of non-compliance; • The ACROSS platform operator may take appropriate measures to address the situation at its sole discretion. These measures may include the following: o Warning; o Request to bring activities in compliance with the Code of Conduct; o Temporarily suspension from the ACROSS platform; o Expulsion from the ACROSS platform.	

[20] The ACROSS code of conduct can be found here: https://citizen-webapp-citizen-application-dev.k8s.across-h2020.eu/login?_gl=1*zdp6mk*_ga*MTc3NjQzNDMwMi4xNzEwOTI3MDM5*_ga_E593PVG4PL*MTcxMTY0MTYxOC4zLjEuMTcxMTY0MTY4MC4wLjAuMA..&_ga=2.20300283.2104651359.1711641619-1776434302.1710927039.

6 Impact of new and future legislations on ACROSS

6.1 Identified new and future legislations

During the course of the ACROSS project, the European Union has adopted numerous legislative proposals in response to the rapidly evolving digital landscape. The legal landscape above already provides an extensive overview of the legislations that are currently applicable to the ACROSS project. This section will zoom into the legislations that are either still in the proposal phase of the legislative process in the EU or that have been adopted very recently, and might therefore have an impact on the ACROSS platform. This section will focus on the following two elements:

- Data spaces
- The European Data Act

With ACROSS being a research project it was important to evaluate these new proposals and legislations on EU level and to investigate the impact they might have on the ACROSS platform in the future. The legal partner (Timelex) therefore closely monitored the EU legislative process of these new proposals. The section below will provide an overview of the legal requirements of these new proposals and on how (if necessary) the ACROSS project already took them into consideration.

6.1.1 Data spaces in the European Union

At the beginning of 2020, the European Commission communicated a **European Strategy for Data**[21], which aims to establish the EU as a leader in a data-driven society. The strategy is designed to ensure that the EU can leverage the vast amounts of data generated within the single market, fostering innovation, economic growth and societal benefits while adhering to common European values and regulation, especially regarding data protection and privacy.

The key point of the strategy include:

- **Introduction of common European Data Spaces**: The Strategy proposes the creation of several sector-specific data spaces in the areas of health, industrial manufacturing, energy, mobility, agriculture, and others. These data spaces are intended to facilitate the safe and secure sharing and pooling of data across borders and sectors, enhancing innovation and competition.

[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European Strategy for Data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

- **Empowerment of citizens and businesses**: it emphasizes empowering individuals and businesses to make better decisions based on insights gleaned from non-personal data. It aims to make data available to all, regardless of the size or sector of the entity, ensuring that everyone benefits from the digital dividend.
- **Strengthening of Data Governance**: the strategy outlines measures to improve governance structures for handling data, increase the quality and pools of data available for use and re-use, and ensure that data sharing and processing comply with the EU's strict data protection rules.
- **Investment in Data Infrastructure and Literacy**: The strategy calls for significant investment in next-generation technologies and infrastructures, such as high-performance computing, cloud solutions and data processing capabilities, as well as in digital competences like data literacy. This is to support the creation of European data pools and to facilitate Big Data Analytics and machine learning in a manner compliant with data protection legislation.
- **Enhancement of Cybersecurity**: Recognizing the importance of trust in the data economy, the strategy highlights the need for the highest cybersecurity standards to protect data and the services built upon it. It mentions the role of the EU cybersecurity Certification Framework and the EU Agency for Cybersecurity (ENISA) in achieving this goal.
- **Promotion of international Data Flows**: the strategy advocates for an open but assertive approach to international data flows, ensuring that data can move freely across borders while fully complying with EU law and upholding European values, especially regarding data protection and privacy.

In summary, the European Strategy for Data sets forth a vision and concrete measures for the EU to foster the potential of the data economy, ensuring that data flows freely and securely across sectors and borders, driving innovation and economic growth while protecting individual rights and adhering to European values.

Many of these measures have been included later into the Data Governance Act which has been discussed extensively in section 5 of this Deliverable. In this section, we want to zoom into one specific aspect of the European Strategy for Data, namely the creation of sectoral data spaces. The European Strategy for Data mentions the creation of **sector-specific common European data spaces** in strategic areas relevant to the digital and green transitions. The specific sectoral data spaces mentioned include:

- **Health Data Space**: To advance in preventing, detecting, and curing diseases and to improve the accessibility, effectiveness, and sustainability of healthcare systems while giving individuals control over their health data.

- **Industrial (Manufacturing) Data Space**: To support the competitiveness and performance of the EU's industry, particularly in manufacturing, by capturing the potential value of non-personal data use.
- **Green Deal Data Space**: To support the EU's Green Deal priority actions on climate change, circular economy, zero-pollution, biodiversity, deforestation, and compliance assurance by making relevant data accessible.
- **Mobility Data Space**: To position Europe at the forefront of intelligent transport systems development, including connected cars and other modes of transport, by facilitating access, pooling, and sharing of transport and mobility data.
- **Energy Data Space**: To promote a stronger availability and cross-sector sharing of data in a secure and trustworthy manner, facilitating innovative solutions and supporting the decarbonization of the energy system.
- **Agriculture Data Space**: To enhance the sustainability performance and competitiveness of the agricultural sector through the processing and analysis of production and other data, allowing for precise and tailored application of production approaches at the farm level.
- **Financial Data Space**: To stimulate innovation, market transparency, sustainable finance, and access to finance for European businesses through enhanced data sharing.
- **Public Administration Data Space**: To improve transparency and accountability of public spending and spending quality, fighting corruption, and supporting the effective application of EU law.
- **Skills Data Space**: To reduce the skills mismatches between the education and training system and the labor market needs.

These sectoral data spaces are part of the broader vision to create a single European data space, a genuine single market for data, where data flows freely and securely across sectors and borders, driving innovation and economic growth while protecting individual rights and adhering to European values.

Whereas many of these sector-specific data spaces are not directly relevant to ACROSS, we do want to highlight one of them that is directly relevant to ACROSS, namely the skills data space.

The **skills data space** aims to facilitate the sharing and pooling of high-quality data on qualifications, learning opportunities, jobs and skill sets of people. The skills data space has been implemented by the EU through the following initiatives[22]:

[22] The concrete implementation for the Data Space for Skills is done facilitated by the DS4Skills project, https://www.skillsdataspace.eu/.

- Digital Credential Transformation Plans: the EU supports Member States in the development of digital credential transformation plans. This involves preparing re-usable datasets of qualifications and learning opportunities, making it easier for individuals to share their qualifications across the EU in a secure and interoperable digital format.
- Europass Digital Credentials Framework: as part of the Digital Education Action Plan, the Commission developed the Europass Digital Credentials Framework to issue credentials to learners in a secure and interoperable digital format. This framework is a key component of the Skills Data Space, enabling individuals to manage and share their educational and training records easily.
- Governance Model: The Commission plans to establish a governance model for the ongoing management of the Europass Digital Credentials Framework in close cooperation with Member States and key stakeholders. This governance model will ensure that the Skills Data Space operates effectively and meets the needs of its users.
- Investments in Skills and Data Literacy: The funding dedicated to skills under the Digital Europe Programme will contribute to expanding the digital talent pool, including skills related to data. This investment aims to narrow the gap in terms of big data and analytics capacities, supporting the development and roll-out of personal data spaces and enhancing general data literacy.
- Network of Data Stewards: The idea of a network of data stewards from across data-intensive organizations (both businesses and the public sector) will be further explored. This network will play a crucial role in managing and facilitating access to data within the Skills Data Space, ensuring that data is used effectively to match education and training with labor market needs.

6.1.2 The European Data Act

The Regulation on harmonized rules on fair access to and use of data – also known as **the Data Act**[23] – entered into force on 11 January 2024, and is one of the key pillars of the above-mentioned European Data Strategy. The key objective of the Data Act is to make data (in particular industrial data) more accessible and usable, encouraging data-driven innovation and increasing data availability. To achieve this, the Data Act sets clear rules concerning the use of this data by the main actors in the data economy.

These main actors in the data economy are the following:

[23] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

- **Data Holders**: entities that have the authority and control over data. This includes companies that collect, generate and produce data as a result of their operations.
- **Data Users**: entities or individuals that seek access to or wish to use the data held by data holders for various purposes, including innovation, developing new services, or enhancing existing products.
- **Data Recipients**: a broader category that includes any party to which data is made available. This can encompass both data users and public sector bodies, depending on the context of the data sharing or data access scenario.
- **Public Sector Bodies**: governmental or public administration entities that may request access to data held by private companies in specific, exceptional situations, such as public emergencies or for fulfilling other narrowly defined exceptional data needs.
- **Data Intermediation Service Providers**: entities that facilitate data sharing between data holders and data users, ensuring a secure environment for the data exchange. These service providers play an important role in enhancing trust in data sharing and improving interoperability.

The main focus of the Data Act is (i) **connected devices** (Internet-of-Things) with rules regarding access to data generated by these devices and regarding the transfer of this data to other third parties; and (ii) **cloud service providers**, providing a framework for customers to effectively switch between different providers of data-processing services.

It must be clear that ACROSS as an entity will not fall under the definition of a Data Holder or Data User as defined above (i.e. ACROSS does not process any data itself, but solely facilitates the data sharing through a user-centric platform). However, ACROSS could be seen as a Data Intermediation Service Provider as defined in the Data Act. The Data Act explicitly recognizes the importance of data intermediation services (including Personal Information Management Systems "PIMS") in achieving the full potential of the requirements of the Data Act. Recital 33 of the Data Act states that: "*Business-to-business data intermediaries and personal information management systems (PIMS), referred to as data intermediation services in Regulation (EU) 2022/868, may support users or third parties in establishing commercial relations with an undetermined number of potential counterparties for any lawful purpose falling within the scope of this Regulation. They could play an instrumental role in aggregating access to data so that big data analyses or machine learning can be facilitated, provided that users remain in full control of whether to provide their data to such aggregation and the commercial terms under which their data are to be used*."

Next, of relevance for ACROSS are **the requirements regarding interoperability** which can be found in Chapter VIII of the Data Act. These requirements shall be included in the table under section 6.2 below as these will be of significant importance for ACROSS.

6.2 Legal requirements

Table 10 identification of the legal requirements in new and future legislations

EU Skills data space	
SDS-01	In order to align with the main objectives of the EU Skills Data Space, ACROSS needs to **facilitate the sharing and recognition of qualifications and skills** across the EU Member States. This directly supports the mobility of workers by making it easier for individuals to prove their qualifications and skills when seeking employment in another member State.
SDS-02	The process for sharing and recognition of qualifications and skills across the EU Member States in ACROSS needs to be **transparent and accessible** for everyone.
SDS-03	ACROSS needs to adhere to **standardized formats and protocols** for data sharing, ensuring **interoperability** within the EU.
EU Data Act	
DA-01	The first interoperability requirements in the Data Act describes the need for the dataset content, use restrictions, licenses, data collection methodology, data quality and uncertainty to be **sufficiently described**, where applicable, in **a machine-readable format**, to allow the recipient, to find, access and use the data.
DA-02	The second interoperability requirement in the Data Act states that the data structures, data formats, vocabularies, classification schemes, taxonomies and code list, where available, shall be **described in a publicly available and consistent manner**.
DA-03	The third interoperability requirement states that technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be **sufficiently described** to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine-readable format where that is technically feasible and does not hamper the good functioning

6.3 How does ACROSS take them into account?

Table 11 implementation status of the legal requirements in new and future legislations

EU Skills data space		Status?
SDS-01	The ACROSS platform facilitates the application phase of citizens that are moving to another Member State for a job (cross-border), i.e. the applying for a job and the professional recognition. Through ACROSS citizens can easily access services such as for example PIM (which is a German service that issues a digital transcript of a secondary or high school diploma). Therefore, it directly supports the mobility of workers by making it easier to access supporting official documents which prove their qualification and skills.	
SDS-02	ACROSS is designed in a way to make it user-friendly and accessible for everyone. This is mainly done through the **virtual assistant component**, which provides speech and text assistance in multiple languages, allowing citizen users to easily understand the administrative procedure that comes with moving for work or studies.	
SDS-03	One of the main requirements for ACROSS was that the solution needed to **exploit new technologies (e.g. eID, Wallets, Data Spaces, etc.)** and therefore contribute to the acceleration of the digital transformation process. This aspect has also been evaluated in the expert survey sessions, where the experts highlighted the fact that the adoption of the ACROSS Platform could highly facilitate the exploitation of the above mentioned digital innovation.	
EU Data Act		
DA-01	These interoperability requirements have been successfully implemented into the ACROSS platform: • All components, methodology, datasets, etc. are sufficiently described in a machine-readable format; • data structures, data formats, vocabularies, classification schemes, taxonomies and code list are sufficiently described and publicly available.	
DA-02		
DA-03		

7 Conclusions: lessons learned

This deliverable provides an extensive overview of the implementation status of the identified legal requirements in D3.6. Overall, the outcome of this validation exercise is highly positive. The following overall conclusions can be drawn with regards to the implementation of the legal requirements:

- Almost all legal requirements were found to be implemented into the results of the ACROSS project;
- Only a couple of the identified legal requirements were found to be partially implemented. In this case, a clear justification was provided and we can therefore conclude that this has no negative impact on the overall result of the ACROSS project. For example, the eIDAS integration for Greece has not successfully been integrated into the ACROSS platform. This is however a shortcoming in the current eIDAS node implementation in Greece, not in the ACROSS project; the ACROSS platform is inherently capable of supporting any available eIDAS nodes (and therefore also complying with this legal requirement).

Lastly, this Deliverable also looked into the new legislations/upcoming legislations that have emerged in the EU legal landscape. This Deliverable identified the main legal requirements that were applicable to ACROSS, and how they have been taken into account in the ACROSS project.

8 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] 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).

[3] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248rev.01.

[4] 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, https://eur-lex.europa.eu/eli/reg/2018/1724/oj.

[5] Commission Implementing Regulation (EU) 2022/1463 of 5 August 2022 setting out technical and operational specifications of the technical system for 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1463.

[6] COM (2023) 534 Report from the Commission to the European Parliament and the Council – First Implementation Report on the Single Digital Gateway, 12 September 2023, https://single-market-economy.ec.europa.eu/publications/first-implementation-report-single-digital-gateway_en.

[7] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868.

[8] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a European Strategy for Data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066.

[9] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1704709568425.