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

D2.7 Legal and Regulatory considerations

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	D2.7 Legal and regulatory considerations
Work package	WP2: ACROSS New Governance Model
Nature	Report
Dissemination Level	Public
Date	30/04/2024
Status	Final
Editor(s)	Hans Graux and Jolien Clemens (TLX)
Contributor(s)	Hans Graux and Jolien Clemens (TLX)
Reviewer(s)	VARAM and GRNET
Document description	This Deliverable will identify 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. This Deliverable will also provide the actual templates and compliance documents that were created during the project.

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
V0.1	25/03/2024	First draft	Jolien Clemens (TLX)
V0.2	18/04/2024	Draft ready for review	Jolien Clemens (TLX)
V0.3	26/04/2024	Implementation of feedback of partners	Jolien Clemens (TLX)
V1.0	29/04/2024	Final version ready for submission	Jolien Clemens (TLX)

Executive Summary

This Deliverable provides an overview of the legal and regulatory considerations that were taken into account during the co-creation and co-design sessions and in the ACROSS Project in general. This Deliverable will focus mainly on data protection aspects as this was mainly of importance during the research activities of the project, which entailed the involvement of research participants (citizens) and expert stakeholders. The Annex to this Deliverable provides the actual templates and compliance documents which were developed during the course of the ACROSS project.

It should be noted that the general overview of the applicable legal framework, the legal requirements that are derived from this framework and the implementation of these requirements in ACROSS, have been investigated in more detail in other Deliverables, notably D3.6 (“legal requirements”) and D3.7 (“legal Report”). This work will not be repeated in this Deliverable.

Table of Contents

1 INTRODUCTION 7

1.1 PURPOSE AND SCOPE 7

1.2 METHODOLOGY AND STRUCTURE OF THE DELIVERABLE 8

2 GDPR CONSIDERATIONS IN ACROSS 9

2.1 GDPR REQUIREMENTS FOR THE RESEARCH ACTIVITIES (CO-CREATION AND CO-DELIVERY SESSIONS) 9

2.1.1 Introduction 9

2.1.2 The concept of personal data in research activities 9

2.1.3 The Consortium's partners responsibilities under the GDPR 10

2.1.4 Checklist of the main GDPR requirements for the research activities 11

2.1.5 GDPR requirements for the ACROSS platform 16

2.2 DESCRIPTION OF THE DELIVERED COMPLIANCE WORK 16

2.2.1 GDPR compliance work in relation to the co-creation sessions and co-delivery sessions 16

2.2.2 GDPR compliance work in relation to the ACROSS platform 18

2.3 LEGAL GAP ANALYSIS IN RELATION TO THE GDPR COMPLIANCE WORK 21

3 LEGAL CONSIDERATIONS IN RELATION TO THE VIRTUAL ASSISTANT 22

3.1 DATA PROTECTION 22

3.1.1 Data protection considerations 22

3.1.2 Implementation in ACROSS 23

3.2 AI ACT 24

3.2.1 Applicability of the AI Act to the ACROSS Virtual Assistant 24

3.2.2 AI Act requirements for the ACROSS VA 28

3.2.3 How did the ACROSS VA take the AI Act into account? 29

4 CONCLUSIONS 30

5 REFERENCES 31

6 ANNEXES 32

6.1 PRIVACY POLICY FOR ACROSS PLATFORM 32

6.2 CODE OF CONDUCT FOR SERVICE PROVIDERS 41

6.3 DATA PROTECTION IMPACT ASSESSMENT ON ACROSS PLATFORM 51

List of Tables

TABLE 1 OVERVIEW OF THE MAIN GDPR REQUIREMENTS 11
TABLE 2 LIST OF WP8 DELIVERABLES 16
TABLE 3 OVERVIEW OF THE MAIN TEMPLATES AND COMPLIANCE DOCUMENTATION 19
TABLE 4 PROPOSED MITIGATING MEASURES 21
TABLE 5 GDPR REQUIREMENTS FOR VIRTUAL ASSISTANTS 23
TABLE 6 MAIN REQUIREMENTS UNDER THE AI ACT FOR THE ACROSS VA 28
TABLE 7 ACROSS VA/AI ACT 29

List of Terms and Abbreviations

Abbreviation	Definition
GDPR	General Data Protection Regulation
DPIA	Data Protection Impact Assessment
VVA	Virtual Voice assistant
DPO	Data Protection Officer
DPA	Data Processing Agreement
AIA	AI Act
LLM	Large Language Models
GPAI	General purpose AI

1 Introduction

1.1 Purpose and Scope

This Deliverable provides an overview of the legal and regulatory considerations which were made throughout the project.

The primary focus of this Deliverable will be on GDPR compliance in two aspects of the project:

- GDPR compliance in the research activities in general (co-creation sessions, surveys, workshops, etc.);
- GDPR compliance in the ACROSS platform (which has also been discussed extensively in D.3.7 “legal report”).

The other legal frameworks that are applicable to the ACROSS project have been investigated and discussed in D3.7 “legal report”. Deliverable D3.7 already provides an in-depth analysis of the legal framework, the identified legal requirements and describes the ways in which these requirements have been implemented into the ACROSS platform and project in general. Therefore, this work will not be repeated in this Deliverable. We have therefore decided to focus more in this deliverable on some of the GDPR compliance work that has been undertaken during the course of this project, as the GDPR was identified as one of the main applicable legal frameworks for the ACROSS project.

Finally, this Deliverable will provide the actual templates and compliance documents that were delivered throughout this project. These can be found in the Annexes of this Deliverable, and will be referenced to throughout the text.

1.2 Methodology and Structure of the Deliverable

As described above, this Deliverable will mainly focus on the GDPR compliance work that has been undertaken throughout the ACROSS project. Given this intended perspective, section 2 of this Deliverable will first focus on the general GDPR considerations taken into account in this project.

- **Section 2.1** of this Deliverable will look into the GDPR requirements that were specifically identified for the research activities (organizing of the co-creation and co-delivery sessions) and for developing the ACROSS platform in general.
- **Section 2.2** of this Deliverable will describe the actual delivered compliance work in this respect, also referring to the actual templates and compliance documents that were developed, and which can be found annexed to this document.
- **Section 2.3** provides the legal gap analysis which identifies some GDPR legal gaps that are currently still present, and a plan on how to mitigate them in the future.

Section 3 of this Deliverable will focus on the legal considerations that were taken into consideration for the Virtual Assistant (VA) in particular:

- **Section 3.1** will look into the data protection considerations for the VA
- **Section 3.2** will look into the AI act considerations for the VA
- **Section 4** concludes the report, while **Section 5** presents the references.
- **Section 6** provides the annexes. **Annex 6.3** presents the updated version of the Data Protection Impact Assessment.

2 GDPR considerations in ACROSS

2.1 GDPR requirements for the research activities (co-creation and co-delivery sessions)

2.1.1 Introduction

During the context of this Project several co-creation and co-delivery sessions were organized to ensure that the views of external experts and citizens were considered when designing the ACROSS platform. As these research activities would necessarily involve the personal data processing of real persons, it was of importance to ensure compliance with the General Data Protection Regulation (EU) 2016/679 ("GDPR"). The research activities primarily existed out of survey data collection, organizing workshops and interview sessions with certain stakeholders.

Next to the research activities in general, the legal team was responsible for ensuring that the ACROSS Platform that would be developed throughout the course of the project meets the GDPR principles and requirements. Even though the ACROSS platform would not be used on real users during the course of the project, it was nevertheless important to identify the GDPR requirements in an early phase and to ensure compliance with these requirements.

2.1.2 The concept of personal data in research activities

The General Data Protection Regulation[1] (hereinafter "GDPR") provides basic provisions constituting the general legal framework applicable in all Member States of the European Economic Area in relation to the protection of personal data.

The GDPR will be applicable to the processing of information relating to a natural person that is identified or identifiable. It must be clear that in the context of the co-creation sessions, both direct and indirect identifiable information of the research participants will be collected.

- **Direct identifiable information**: in order to contact research participants, their name, which is the most known and intuitively understood form of directly identifiable personal data.
- **Indirect identifiable information**: in the context of the co-creation activities, the following information that will be collected will only indirectly identify the research participants, i.e. when connected with other information, such as contact information, information about their personal experiences when moving to another country for work or studies, etc.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural personas 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).

Due to the very broad concept of 'identifiable' under the GDPR, the ACROSS project ensured GDPR compliance in all the research activities established, including where a questionnaire would be sent out to research participants and the results would only be connected to a pseudonym (an alphanumeric number). The necessary safeguards were nevertheless implemented because the content of their answers may be considered highly personal (i.e. experiences while moving for work or studies) which might reveal the identity of the participant.

2.1.3 The Consortium's partners responsibilities under the GDPR

The GDPR defines two main concepts for entities that are processing personal data:

- **The controller**, which is the entity which decides the purposes and the means of the processing (i.e. the why and the how the data is processed);
- **The processor**, which processes the data solely on behalf of and on the basis of instructions made by the controller (even though technical decisions can be made by the processor as well, i.e. which security measures are in place for the protection of the personal data).

In a research, project such as ACROSS, all partners will typically act as controllers for their own research and when implementing the different tasks in the description of action for their respective work package(s) (WP). Specifically, when organizing the co-creation session and collecting/processing the data that derives from them, each partner will act as a controller. It is true that that partner will take directions from information in other WP (such as WP8 on the ethics requirements) or may discuss with the legal partner certain processing activities it wishes to engage in, but this does not mean that they don't decide for themselves what personal data they will use, re-use and share with the other consortium partners. This means that each partner that organizes co-creation sessions and other research activities will make their own decisions on the purpose and the means of the data processing. Section **Error! Reference source not found.** below will provide a GDPR checklist of the main requirements for the ACROSS Consortium partners. It is important to highlight that this checklist will solely be a summary of the more elaborate information that was provided in other WP deliverables (notably D3.6 on the legal requirements for ACROSS and WP8 on the ethics requirements for research projects).

Processors will be involved in ACROSS in the form of service providers, e.g. hosting service providers (such as Microsoft Teams, or other storage solutions used by the project partners). The partner that is in charge of the processing activity for which a service provider was involved, was fully responsible for ensuring that the necessary contracts were in place, i.e. a data processing agreement that fulfils the requirements of Article 28 of the GDPR.

2.1.4 Checklist of the main GDPR requirements for the research activities

The table below will give an overview of the main GDPR requirements that were taken into account when conducting the research activities (in particular the co-creation and co-design sessions):

Table 1 Overview of the main GDPR Requirements

GDPR requirement	Explanation
Legal ground (lawfulness)	Controllers must make sure that any processing activity relies on one of the six legal grounds mentioned in Article 6 GDPR, i.e.: • the data subject has given prior **consent** to the processing of his or her personal data for one or more specific purposes; • processing is necessary for the **performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; • processing is necessary for compliance with **a legal obligation** to which the controller is subject; • processing is necessary in order to protect **the vital interests** of the data subject or of another natural person; • processing is necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller; • processing is necessary for the purposes of **the legitimate interests** pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. In the context of the research activities in ACROSS the main legal bases that were relied on were consent and legitimate interest. The consent of the research participant will be necessary to process his/her data and to use the processed data in the research results. When relying on consent, it must be kept in mind that the consent must be: • freely given (the data subject cannot be pressured into giving his/her consent);

	• specific and granular (this means that the consent cannot be too broad and vaguely described, allowing the data subject to agree to the processing of certain data for specific well-defined purposes); • informed (this means that the controller must give the data subject sufficiently clear, concise, easily accessible information); • unambiguous (based on a clear affirmative act, for example by ticking a consent box and not by the act of unticking of a pre-ticked consent box).
Fairness	The principle of fairness means that the processing activities that are performed in the context of the ACROSS project must match with the expectations of the data subjects, based on the information that was given to the data subject by the controller. This means that it is forbidden to process personal data without first informing the data subject about this processing activity and/or using personal data for other purposes.
Transparency	This means that the controller must give the essential information to the data subject about the processing, such as the identity of the controller, the purposes of the processing, which personal data will be collected, the implemented safeguards and their data subject rights. The specific information that must be given to the data subjects is specified in Articles 12 to 14 of the GDPR. Information must be given in a concise, transparent and intelligible manner, in clear and plain language and must be easily accessible, free of charge, and adapted to the audience (i.e. particularly when involving more vulnerable research participants such as person's with disabilities).
Purpose limitation	The principle of purpose limitation means that the processing can only be done for specific, explicit and legitimate purposes. The purpose(s) must also be sufficiently communicated to the data subject in advance. For this to be possible, the purpose of the processing operation must be clearly defined by the controller in advance of the processing taking place. This principle provides a safeguard against vague and too broad processing activities which will be considered not compliant with the GDPR.

The GDPR also provides a framework for the re-use of data that is collected for one purpose when it is compatible with that initial purpose. Article 6 (4) of the GDPR sets out the elements that need to be taken into account to assess whether a certain re-use is considered compatible:

- there must be a link between the purposes for which the personal data has been collected and the purposes of the intended further processing;
- the context in which the personal data has been collected, in particular regarding the relationship between the data subjects and the controller (i.e., is there a certain power imbalance, are the data subjects particularly sensitive, etc.?);
- the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10 of the GDPR;
- the possible (negative) consequences for the data subjects of the intended further processing;
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

In the context of the research activities of ACROSS, further re-use of the collected data outside the ACROSS project by the partners was not be allowed. Any use of the data that was collected during interviews and/or through questionnaires, could only be used in the context of the project and for purposes that were communicated clearly to the research participants (i.e. in the informed consent forms and information sheets).

If any re-use of the data was intended, the project partners were encouraged to contact the legal partner (Timelex), who would assess the applicability of the above-mentioned criteria. If the outcome of the assessment is that the intended re-use is not compatible, then the re-use will in principle be forbidden, unless the data subject provides a new consent (or another legal basis is possible, such as legitimate interest). Moreover, the project partners had to ensure that sufficient safeguards were in place to ensure the safety of

	the data that will be re-used (i.e. pseudonymization, encryption, contractual arrangements, etc.).
Data minimization	The data minimization principle means that no more data can be processed than is strictly required to fulfil the intended purpose of the controller. In the context of the research activities, this meant that the project partners had to assess for each of the data collection activities whether they could reach the same goals, through the use of other, less invasive or intrusive means, especially with regards to the amount and/or type of personal data used. As an example: for the purpose of the ACROSS project, there is no need to collect particular sensitive information of the research participants, i.e. information related to their health, religion, sexual preferences, etc., because this is not relevant for the research purpose of ACROSS. In addition, the research partners were also encouraged to assess whether the information needed to be collected in a fully identifiable format, if the answer to this question was no, the research partners opted for pseudonymized or even anonymized data collection (which was for example done for the impact assessment survey).
Data accuracy	This principle requires a data controller to take reasonable steps to ensure that the personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. With regards to the research activities conducted in ACROSS this means that the participants were able to request from the research partners to have their data corrected when incorrect or outdated. It must be highlighted that not all incorrect information is necessarily inaccurate, it could be that a research participant gave factually incorrect information or lied during the interview (which does not make the information inaccurate because it accurately represents the information that was given during the interview).
Storage limitation	This principle requires that personal data is 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'.

	When setting the retention periods for the data, the Consortium assessed the need for retaining the data for the identified research purposes. The Consortium set the retention period for the data for ten (10) years after the project has ended, with the understanding that during this period the data can only be used to demonstrate the scientific validity of the project outcomes and to demonstrate that the project was executed in accordance with any applicable legal obligation.
Integrity and confidentiality	The GDPR requires personal data to be '*processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized loss, destruction or damage using appropriate technical and organizational measures*'. The shared baseline technical and organizational measures for the ACROSS project were set out in D8.8 (requirement No. 9). Later on request of the reviewer after the first review meeting, these baseline measures were checked against the actual implemented security measures of the project partners (i.e. the pilot partners that would be conducting research activities) and were found to be sufficient.
Accountability	The last principle is the principle of accountability on which article 5 (2) states the following: "the controller shall be responsible for, and be able to demonstrate compliance with [the other six principles discussed above]." In essence this meant for ACROSS that the necessary documentation should be in place to show both data subjects and supervisory authorities that measures have been taken to achieve compliance with the principles of data processing. One important tool for accountability is the use of data protection impact assessments (DPIAs). DPIAs are mandatory when intended processing is likely to result in high risk processing for data subjects and especially when new technologies are involved. For ACROSS, it was initially assessed that a DPIA is not necessary in the context of the co-creation sessions. This assessment was correct as not a lot of sensitive data will be collected and the data will only be used in the context of the ACROSS Project. However, upon later

	consideration, it was decided to perform a DPIA on the ACROSS Platform in general, because of the fact that the platform could in the future be used on real people. Moreover, would this further benefit the exploitability of the ACROSS platform.

2.1.5 GDPR requirements for the ACROSS platform

Next to the research activities in general, the legal team was responsible for ensuring the GDPR compliance of the ACROSS platform that would be developed during the ACROSS project. Even though the ACROSS platform would not be used on real user during the course of the project, it was nevertheless important to identify the GDPR requirements in an early phase and to ensure compliance with these requirements. It should be noted that the ACROSS platform was indeed tested in the impact assessment phase on real persons, but these users could use fictitious login data.

The GDPR requirements for the ACROSS platform were discussed in detail at the beginning of the project in D3.6, we will therefore not repeat them in this deliverable.

2.2 Description of the delivered compliance work

2.2.1 GDPR compliance work in relation to the co-creation sessions and co-delivery sessions

Most of the GDPR considerations with regards to the research activities were discussed extensively in WP8.1- 8.14 (“ethics requirements”).

The **following deliverables of WP8** include considerations on GDPR compliance for the ACROSS co-creation and co-delivery sessions:

Table 2 List of WP8 Deliverables

Deliverable	Description
D8.1	This deliverable describes the procedures for onboarding co-creation session participants, including their identification, selection, recruitment and record keeping. Particular attention was provided to the valid consent of research participants for their participation (through consent forms and information notices).
D8.2	This ethics deliverable submitted the initial templates of the informed consent forms and information sheets covering the voluntary participation and data protection issues. The consent form templates covered two different interview modalities: simple e-mail confirmations or a formal consent and information notice.

D8.3	This ethics deliverable considers the GDPR considerations with regards to the processing of special categories of personal data during the course of the project.
D8.6	This ethics deliverable confirmed that a Data Protection Officer (DPO) has been appointed and that the contact details are made available to all the data subjects involved in the research.
D8.9	This ethics deliverable provided an overview of the anonymization/pseudonymization techniques that will be implemented in ACROSS.
D8.10	This ethics deliverable describes the informed consent procedures that were implemented for the participation of humans and with regards to data processing (consent under the GDPR).
D8.11 – D8.12	These two ethics deliverables clarified the GDPR considerations that need to be taken into account when processing data that is publicly available (D8.11) and data that has been previously collected (D8.12).
D8.13	This ethics deliverable assessed the need for a Data Protection Impact Assessment (DPIA) under the GDPR in the context of the ACROSS project (in the context of the co-creation sessions).

Throughout the project the legal partner (Timelex) was highly involved in ensuring GDPR and ethics compliance when organizing the co-creation and co-delivery sessions.

This meant that the pilot partners were encouraged to contact Timelex in case they had any GDPR related questions or if they wanted to adapt/tailor the provided informed consent forms and information sheet templates.

For the Impact Assessment Survey, the provided informed consent forms and information sheet templates were slightly adapted by Timelex to better reflect the specific intended data processing activities. The legal partner (Timelex) also organized a specific GDPR workshop for the partners that would be responsible for conducting the Impact Assessment Survey in order to refresh the GDPR principles which needed to be taken into account and to discuss the importance of a valid consent under the GDPR.

The following procedure was used to ensure that the assessment activities were done in a GDPR compliant way:

Activities which were held remotely with citizens/Experts:

1. The pilot partners first sent an email to the participants with attached the consent forms, asking to return them signed;

2. After receiving the signed consent form, the pilot partner have sent the link to the survey, which the research participant was asked to complete;
3. When opening the survey, the participant was provided with an initial disclaimer related to the data processing, and will be asked to tick the following check box:

   "By checking this box, you confirm that you have read the information you have received from us via email related to the processing of your personal data and you consent to the processing of your personal data as described therein."

4. The survey has collected the data in a fully anonymized way. The answers are stored in the EU survey portal, the pilot partners will download the answers from the portal and store them securely.

Activities which were held in person with citizens/Experts:

The same process was followed as described above, with the exception that the consent forms were given to the participants in person and signed on the day of the assessment session.

It is important to highlight that each pilot partner was responsible for collecting and storing the consent forms of their participants. The signed consent forms would not be shared with the other project partners and would also not be stored on the general ACROSS SharePoint. In accordance with the set retention period for the answers to the survey/interview questions (which is 10 years), the signed consent forms can be retained for the same amount of time.

2.2.2 GDPR compliance work in relation to the ACROSS platform

The GDPR compliance work in relation to the design and development of the ACROSS platform is discussed in WP3 (ACROSS Data Governance Framework), more specifically in D3.6 ("legal requirements") and D3.7 ("implementation of the legal requirements"). Most of the GDPR principles that are provided above are also discussed in detail in both deliverables, so in order to avoid redundancy we will not repeat these principles.

However, the table below will give an overview of the main templates and compliance documentation that was delivered to ensure compliance with the GDPR principles identified above. The actual templates are also annexed to this document:

Table 3 overview of the main templates and compliance documentation

GDPR principle	Delivered template/compliance document	Explanation
Accountability	Data Protection Impact Assessment on the ACROSS Platform (see Annex 6.3)	The performed DPIA on the ACROSS platform is the main accountability tool. It allowed the legal team to do an in-debt assessment of the implemented data protection principles, to assess the (remaining) risks to the fundamental rights to data subjects and to propose any mitigating measures, which were then implemented in the final months of the project. The DPIA annexed in Annex 6.3 is the final product of the DPIA exercise that was performed.
Accountability / purpose limitation	Code of conduct for service providers (see Annex 6.2)	The main tool for accountability against the service providers that are using the ACROSS platform is the code of conduct. This code of conduct requires from the service providers that they respect the GDPR principles (i.e. they need to ensure a certain minimum level of respect to these principles), which is mainly done through a statement of adherence which needs to be signed by the service providers during the onboarding process. The Code of Conduct mainly ensures that the service providers respect the principle of purpose limitation as it 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.
Integrity and confidentiality	Data Protection Impact Assessment (see Annex 6.3)	Part of the DPIA focused on the compliance of the ACROSS platform with the technical and organizational security measures (see section on the technical security controls and the organizational security controls in the DPIA, annexed as Annex 6.3). The overall outcome of the DPIA was that most of the technical and organizational measures that need to be in place were appropriately implemented into the ACROSS platform.
Transparency / Fairness	Privacy policy on the ACROSS Platform (see Annex 6.1)	The privacy policy gives information to the user about the data processing activities on the ACROSS Platform.
Transparency / Fairness	Transparency dashboard	The entire design of the ACROSS platform is done with the transparency principle in mind. The transparency dashboard gives the user control of his/her data and informs the user of the purpose, legal basis and personal data that is requested by the service provider.
Legal ground (lawfulness)	Consent Management Module	The main legal basis to process personal data from users in the ACROSS platform is consent. The consent management module enables citizens to manage their consents in a GDPR-compliant way (i.e. they can easily give and withdraw a given consent).
Data minimization	Code of conduct (see Annex 6.2) and template service description data model	Data minimization is enforced through the code of conduct (there is a clause that requires service providers to carefully consider the data that they strictly need for their services) and through the template

	service description data model (the service provider has to pre-define the data elements it will request from the users of the service).

It should be noted that D3.7 look more detailed at the GDPR requirements and how they are exactly implemented in the set-up of the ACROSS platform.

2.3 Legal gap analysis in relation to the GDPR compliance work

It must be clear from the information above that the GDPR compliance work was of paramount importance during the course of the project. Nevertheless, the legal partner (Timelex) can identify some minor legal gaps (risks) that should be highlighted at the end of the project.

It should be noted that the ACROSS platform was indeed never used on real users during the course of the project, which necessarily meant that these risks could never occur, and which makes it more difficult to quantify them. However, after project end, there is a chance that the ACROSS platform (or components of it) are exploited and used on real users. This makes it highly relevant to do this exercise at the end of the project.

Table 4 Proposed Mitigating measures

Legal gap	Proposed mitigating measures
Although the ACROSS platform has already recognized the risk of service providers misusing the data provided through the ACROSS platform (i.e. using it for other purposes as the ones that were communicated).	As discussed above during the course of the project it was proposed to use the approach of a Code of Conduct to enforce the GDPR principles upon the service providers and to ensure the trustworthiness of the service provider. While beneficial, it should be recognized that this approach does have some downsides. One of the main downsides is the fact that you rely on a statement of compliance of the service providers (and therefore also mainly on the goodwill of that service provider). Therefore, it is important to evaluate this approach if the ACROSS platform would be exploited and used in real use cases. Another more stringent approach could be used such as implementing a prior risk assessment and compliance assessment of the service provider by using compliance questionnaires.

3 Legal considerations in relation to the Virtual Assistant

3.1 Data protection

3.1.1 Data protection considerations

One main aspect that was not investigated in detail in D3.6 and D3.7 is **the virtual assistant component,** since this component was still in a fairly early conceptual stage at that time. Therefore, in this Deliverable we will look into the main legal and regulatory considerations that have been taken into account regarding the virtual assistant tool in ACROSS.

Important to mention in this regard is the fact that the EDPB has published in 2021 a set of **guidelines on Virtual Voice Assistants (VVAs)** and the applicability of the GDPR to them.[2] The guidelines address key areas of concern and provide recommendations for VVA providers/designers, developers, and data controllers in general, and are therefore an important source of information for ACROSS.

The main requirements regarding VVAs that are stated in the guidelines are the following:

- **Data minimization**: the technology used should consider filtering unnecessary data, ensuring that only relevant user voice data is recorded;
- A formal **data protection impact assessment** is very likely required, due to the nature of the data processing involved;
- **Transparency and user consent**: privacy policies should clearly separate their information regarding VVA processing of personal data (i.e. present it in a manner that is clearly distinct from other processing activities). Consent, when used as a legal basis, must be specific and informed, particularly concerning the processing of voice data for various purposes;
- **Data retention and deletion**: personal data should be deleted after the execution of a user's request, unless there is a valid legal basis for retention.
- **Accountability and data protection measures**: VVA providers must document all data processing activities and ensure that users can effectively exercise their rights. Data protection by design and by default principles should guide the development and operation of VVAs.

[2] EDPB, Guidelines 02/2021 on virtual voice assistants, 7 July 2021, https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf.

3.1.2 Implementation in ACROSS

Specifically regarding the identified GDPR requirements for Virtual Assistants highlighted in the guidelines, the following considerations have been taken into account, with the corresponding identified compliance actions in ACROSS:

Table 5 GDPR requirements for Virtual Assistants

Legal requirement	Implementation in ACROSS VA
Data minimization	The voice recording has been limited to what is strictly necessary for using the VA-services in the ACROSS platform.
Performing a Data Protection Impact Assessment ("DPIA")	A DPIA has been performed and the data processing elements of the VA has been taken into account in the DPIA.
Transparency and user consent	The **voice recordings** take place based on the explicit consent of the citizen user who chooses to use the VA-services. When the user logs on to the ACROSS platform for the first time and attempts to use voice assistance, they will be asked to provide their consent for the access by ACROSS to their microphone by a pop-up in their browser. Even after this initial consent to access their device microphone, the user will need to actively switch on their microphone before being able to use the ACROSS virtual assistant (to introduce voice input into the ACROSS virtual assistant). The user is free to choose this service or not, and the ACROSS platform is entirely usable without the VA-services. Thus, the consent is informed, specific and freely given, thus satisfying the requirements of the GDPR. In order to provide the transparency information required by the GDPR, the privacy policy includes sections which contain specific information on the data processing by the ACROSS VA.
Data retention and deletion	**Retention**: The user's voice data is stored transiently (for at most a few seconds) within the browser (i.e. the user's device). This is a technical necessity, where the storage is

	needed for buffering before the data is transmitted to the VA backend, which will be done as soon as technically possible. The temporary storage is only used when the data cannot be immediately transmitted (e.g. due to short Wi-Fi connectivity dropouts on the user's device). **Deletion**: After the recording is delivered to the backend, the user's voice is processed by the ACROSS automatic speech recognition service immediately. After this processing, which includes a voice-to-speech transliteration of the spoken request, the audio data is destroyed.
Data protection measures and accountability	The data processing activities by the VA are sufficiently logged (documented).

3.2 AI Act

3.2.1 Applicability of the AI Act to the ACROSS Virtual Assistant

The ACROSS VA ultimately feeds into large language model (LLM), which are models that have been pre-trained on a vast and varied data set, giving them a varied diverse content knowledge. The ACROSS VA uses an LLM to allow users to provide written or voice instructions/questions (prompts), which the chatbot can reply to in written form.

The Artificial Intelligence Act[3] (hereinafter: "AIA") is a new Regulation on EU level that is designed to regulate some AI systems within the European Union, including Large Language Models (LLMs) and Virtual Assistants, by establishing harmonized rules that ensure AI systems are safe to use, and respect fundamental rights. The AIA has been approved by the European Parliament on 13 March 2024. Currently, the Regulation is still undergoing a final lawyer-linguist check and is expected to be adopted and published before the end of the legislature. Finally, the law also needs to be formally endorsed by the Council. It will enter into force twenty days after its publication in the official journal, and be fully applicable 24 months after its entry into force (with certain exceptions).

[3] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Act, EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu).

As a result, for the avoidance of doubt, the AIA was not applicable to the ACROSS project, and formal compliance with the requirements of the AIA is not possible, since it has not entered into force yet. Moreover, since language checking of the AIA is still ongoing and the text has not yet been published, verifying compliance with the final requirements is not possible at the time of submission of this deliverable. None the less, given the clear importance of the AIA for the future lawful use of VA models, the ACROSS legal team has assessed compliance with the draft Regulation, based on the most current version of the AIA, namely the draft that was adopted by the European Parliament in March 2024.[4]

It should first be noted that LLMs are classified as a type of "foundation model", which is defined in Article 3 (1) c) of the AI Act as "*an AI system model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks*".

The application of the AI Act to LLMs and Virtual Assistants can be understood through several key provisions and concepts outlined in the Act:

- **Definition of AI Systems**: The AI Act provides a broad definition of an AI systems[5], which includes machine-based systems that employ certain techniques and approaches that can generate outputs influencing the environments they interact with.[6] LLMs and Virtual Assistants fall under this definition as they are software systems capable of generating predictions, content, recommendations, or decisions based on certain data inputs (i.e. in the case of the ACROSS VA, this is text or voice input).
- **Risk-Based Approach**: The AI Act introduces a risk-based approach to regulation, categorizing AI systems into four levels of risk: unacceptable risk, high risk, limited risk, and minimal risk.[7] LLMs and Virtual Assistants could be categorized into one of these risk levels depending on their specific use cases and the potential impact on individuals' rights and safety.
    - AI systems that are considered forbidden can be found in Chapter II of the AI Act: it refers to AI systems that contradict European Union values of respect for human dignity, freedom, equality, democracy, and the rule of law and Union fundamental rights. Such

[4] European Parliament legislative resolution of 13 March 2024 on the Proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

[5] Article 3 (1) defines AI system as "*a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*."

[6] Recital 12 AI Act.

[7] Recital 27 AI Act.

prohibitions include systems that exploits vulnerabilities of a (group) of persons based on their age, disability or social or economic situations, systems that evaluate or classify persons based on their personal or personality characteristics, criminal behavior prediction systems, law enforcement 'real-time' biometric categorization systems, etc. It is clear that the ACROSS VA does not fall under one of these categories.

- AI systems that are considered high risk are spelled out in an Annex III to the AI Act, such as biometric AI systems used for identification or emotional recognition, AI systems used for the management and operation of critical digital infrastructure, AI systems used in education and employment, AI systems used in law enforcement, etc. The ACROSS VA does not fall under one of these categories.
- For the ACROSS use case, the LLM and VA would fall under the residual minimal risk category due to the intended use case (i.e. it is only intended to assist a user through a journey, it does not provide advice or interacts in another way with the users). As a result, the VA would need to satisfy certain transparency requirements, as will be explained below.

- **Requirements for High-Risk AI Systems**: If LLMs or Virtual Assistants are classified as high-risk AI systems, they would be subject to strict compliance requirements, including data and governance measures (i.e. requirements for the data sets that are used to train and validate the AI system), risk management systems, transparency obligations, human oversight and accuracy requirements.[8] Moreover, their compliance with these requirements will need to be certified by an independent third party, in line with the approach that is often used for European product safety legislation. Following such certification, the well-known CE-mark must be applied on the product. These requirements aim to ensure that high-risk AI systems are trustworthy and ethically sound, and the CE-mark allows users to determine that compliance with EU law has indeed been assessed.
- **Transparency Obligations for Certain AI Systems:** as noted above, the AI Act lays down transparency obligations for AI systems that interact with natural persons or generate content.[9] This means that LLMs and Virtual Assistants, especially those designed for direct interaction with users or content generation, must clearly inform users that they are interacting with an AI system.

[8] Ibid. The requirements for high risk AI systems can be found in Chapter III of the AI Act.
[9] Recital 132 and Chapter IV of the AI Act.

- **General-Purpose AI Models (GPAI)**: The AI Act also addresses general-purpose AI models[10], which includes many types of LLMs. It sets specific rules for these models, especially when they pose systemic risks, ensuring that their deployment is consistent with the Act's objectives to safeguard fundamental rights and public safety. The LLMs deployed in the ACROSS VA are not considered to pose a systemic risk as defined in the AI Act. However, all GPAI models, even those that do not present a systemic risk, must publicly disclose information about the consent used for training and put in place a policy to ensure that it respects EU copyright law.

Based on the overview above, it is clear that a distinction must be made between:

- **the LLM** as such. This is developed externally from the ACROSS project, and will likely face higher compliance burdens for **the providers that put the LLM on the EU market**, since it is a GPAI. This burden will have to be borne by the providers however, not by the users (in the same way that e.g. heavy machinery would have to undergo certification by the providers, but not by buyers of that machinery).
- **The VA services in ACROSS,** which constitute a use of that LLM. This makes ACROSS a so-called 'deployer' of an AI system in the model of the AIA (defined as "a natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity"). Deployers also face certain compliance obligations under the AIA, notably in terms of record keeping, monitoring, training, and transparency.

In summary, the AI Act would apply to Large Language Models and to Virtual Assistants (albeit affecting them differently), by classifying them according to the risk they pose, and by imposing specific obligations on providers and deployers, based on their risk level. Transparency and ethical use must at any rate be ensured, both by providers and by deployers, in their interactions with users. The Act aims to foster innovation while ensuring that AI systems, including LLMs and VAs, are developed and used in a manner that respects European values and fundamental rights.

For the ACROSS VA the impact of the AI Act is currently of course non-existent, since the AIA has not entered into force. However, even when taking into account that the VA must already be provided in compliance with the AIA today to ensure that it is future proof later, compliance is relatively lightweight,

[10] General-purpose AI models are defined as "*an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are released on the market*."

since ACROSS would be considered a deployer of an LLM, rather than a provider, and that the VA would not be considered a high risk, nor a GPAI with a systemic risk. The ACROSS VA is relying on an already existent LLM, for which the developer will bear independent compliance burdens; and the European Parliament has expressed its desire to protect these type of AI providers, trying to ensure that such providers receive from the developers of the LLM all of the necessary information and support to ensure compliance of their downstream applications.[11]

Therefore, the main obligation under the AI Act for ACROSS will be the transparency obligation, where the user needs to be informed about the fact that they are interacting with an AI system, as well as certain monitoring duties. This is particularly important to ensure that the users understand the nature of the interaction and can respond appropriately, and to ensure that the system is functioning appropriately.

3.2.2 AI Act requirements for the ACROSS VA

The table below will provide an overview of the main requirements under the AI Act for the ACROSS VA:

Table 6 main requirements under the AI Act for the ACROSS VA

Identifier	Description
AI-01	Users need to be informed about the fact that they are interacting with an AI system (a chatbot, and not a human). The disclaimer needs to be made available in different modes of understanding, especially for users who are blind. Concretely, this means that disclaimers should not only be provided in writing, but also through aural and visual means.
AI-02	Users need to be provided with the possibility to cancel the interactions with the chatbot at all times. This is an important safeguard to ensure that the user remains in control of the interaction.
AI-03	Usage of the VA must be monitored, not in the sense that conversations themselves must be structurally monitored (which could pose data protection/privacy problems), but in the sense that logs must be kept of the frequency of use, and of any automatically detected errors. Moreover, the VA may only be used for its intended and documented purposes (i.e. for the VA support of the ACROSS services).

[11] Recitals 60 (f) and (g) of the AI Act.

3.2.3 How did the ACROSS VA take the AI Act into account?

Table 7 ACROSS VA/AI Act

Identifier	Description
AI-01	Not yet implemented at this stage.
AI-02	The VA can be closed and cancelled at any time, ending the interaction with the VA. The user can also at any later time decide to re-start the interaction, if he or she decides so later.
AI-03	Not yet implemented at this stage.

The fact that certain of the AI Act requirements are not yet fully implemented, can be justified as the legislation is still at the proposal phase, and therefore not yet applicable to the ACROSS VA.

Moreover, Generative AI is a new and fast-moving field, when the project initially started this integration was not at all foreseen. This resulted in a limited generative AI integration into the ACROSS platform which is more of a provisional nature and prototype than the rest of the ACROSS Implementation.

4 Conclusions

This deliverable provides an extensive overview of the legal and regulatory considerations that have been taken into account during the project with a special focus on GDPR compliance.

With regards to the GDPR compliance work in ACROSS, the Deliverable provides:

- A checklist with GDPR requirements that were taken into account during the research activities
- An overview of the GDPR requirements that were identified for the ACROSS platform, including the accompanying templates that were provided which can be found in the Annexes to this Deliverable.
- A legal gap analysis which highlights some of the minor GDPR risks which can still be identified. This Deliverable, nevertheless, proposes a solution to mitigate this risk.

Lastly, the Deliverable delved into the legal and regulatory considerations which were taken into account for the ACROSS Virtual assistant, focusing on the data protection aspects and the future impact of the AI Act.

The annexes below provide the actual templates which were drafted by the legal partner (Timelex) in this project.

5 References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural personas 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).

[2] EDPB, Guidelines 02/2021 on virtual voice assistants, 7 July 2021, https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf.

[3] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Act, EUR-Lex - 52021PC0206 - EN - EUR-Lex (europa.eu).

[4] European Parliament legislative resolution of 13 March 2024 on the Proposal for a regulation of the European Parliament and of the Council on laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

6 Annexes

6.1 Privacy policy for ACROSS platform

ACROSS platform
Privacy policy

We attach great importance to the security and confidentiality of your personal data. This privacy policy informs you about the processing of your personal data on the ACROSS platform.

1. **WHEN DOES THIS PRIVACY POLICY APPLY?**

1.1. You are of course free to use the ACROSS platform or not. If you do decide to use it, we will need to process and collect some of your personal data. In such instances, this privacy policy will apply. If you disagree with any part of the privacy policy, please refrain from using the platform.

1.2. This privacy policy may be amended as set forth in Article 8. We will inform you of any significant changes that come up.

2. **WHO ARE WE?**

2.1. "We" in this privacy policy refers to the ACROSS Platform operator.

Name platform operator:	Athens Technology Centre (ATC)
Address:	Rizareiou 10, Athens 152 33, Greece
Company number:	EL094360380

2.2. We are responsible for the collection and use of your personal data in the manner explained in this privacy policy. If you have any questions about this, please contact the platform's data protection officer by e-mail (hans.graux@timelex.eu).

2.3. Please note that this privacy policy can only apply to the platform itself. Any service providers that receive your personal data through the ACROSS platform are responsible for their own processing of your personal data, and must be regarded as independent data controllers, who will apply their own privacy policies. These are outside of our control. Therefore, we also recommend you to consult the privacy policies of the service providers directly via their website prior to making your data available to them.

3. WHICH PERSONAL DATA DO WE PROCESS AND WHY?

We will only process your personal data for a specific purpose and to the extent permitted by law. We further explain below in which cases we collect and use your personal data. If we do not receive your personal data directly from you, we will also inform you of this below.

3.1. WHEN YOU USE THE ACROSS PLATFORM

When you use the ACROSS platform, we will collect and process the following information:

What personal data?	Why?	Legal basis?
Basic identification information (username, (email) address, phone number, et cetera) you provide us while registering to the platform and other information you decide to provide freely to us (by filling in specific forms on the platform). Most of your personal identity data and your sensitive information (for example university application documents, documents for job application, et cetera) will be stored in your personal wallet, or by the external electronic identity service provider that you've chosen to use outside of this platform, and therefore not directly on the ACROSS Platform. Some personal data that is required by the public administration/ third party service provider, but which is not part of your personal wallet or your eID, will be collected through forms on the platform. We will make sure that the data collected will be limited to what is strictly necessary for the provision of the cross-border service.	Sharing (if you consent to it) of your personal data with public administrations and third party service providers (university, banks, health and liability insurers, real-estate agencies, et cetera) to enable cross-border services in the field of citizens mobility. To facilitate at your request the exercising of data subject rights on the ACROSS platform (for example obtaining a copy of your personal data, requesting the service provider to delete your personal data, et cetera).	Your specific and informed consent as an end user of the ACROSS platform.

Any information you publish on the public website in comments or experiences.	To share your user experience on the website and to improve the user experience of the ACROSS platform.	Your specific and informed consent.
Metadata such as data on your activity, profile and/or behaviour on the platform. In this case your IP address, date and time of access, browser used, , operating system, etcetera may be processed.	Enabling the use of the ACROSS platform and to make the Platform user-friendly and optimize its functioning.	Our legitimate interest in ensuring the proper functioning of our platform.
Voice recordings and any information you provide to the ACROSS Virtual Assistant (either by using the voice assistant or by using the chat bot assistant). Please note that when using the ACROSS virtual Assistant your voice will be recorded including any characteristics (emotions, accents, etc.). This voice recording will only happen when you explicitly consent to it.	In order to give you a user-friendly experience of the platform and to assist you through the different functionalities on the platform.	Your specific and informed consent. Your explicit consent for the recording of your voice via your audio devices on your PC, laptop, tablet or smartphone, will be asked when first accessing the ACROSS website. Additionally, you will need to switch on the microphone each time you want to use the voice assistant.
Where applicable: URLs or other technical reference techniques that can connect you to the status of your individual application procedure, which will be linked to your user profile	To enable you to consult your application procedure status and (if you choose to do so), to take additional steps in your application process in a user-friendly way.	Our legitimate interest in ensuring a user-friendly platform.

The processing will be limited to these purposes. We will not use your data for tracking, profiling or data selling/trading, surveillance or direct marketing purposes, unless you explicitly consent to this.

3.2. ADDITIONAL USE OF YOUR DATA

3.2.1. For all personal data that we collect in the above circumstances, we may also need to process your personal data in the following cases.

What personal data?	Why?	Legal basis?
Above-mentioned personal data.	To comply with our legal obligations or to comply with any reasonable request from competent police authorities, judicial authorities, government institutions or bodies, including competent data protection authorities.	Our legal obligation.
Above-mentioned personal data.	To prevent, detect and combat fraud or other illegal or unauthorized activities.	Our legal obligation.
Above-mentioned personal data.	To ensure the security of the platform, for example to prevent unauthorized access to the platform.	Our legitimate interest in ensuring a safe and secure platform.
Above-mentioned personal data.	To defend ourselves in legal proceedings.	Our legitimate interest in using your personal data in these proceedings.

4. WITH WHOM DO WE SHARE YOUR PERSONAL DATA?

4.1. In principle, we do not share your personal data with anyone other than the persons who work for us, as well as with the service providers you explicitly gave your consent for. Anyone who has access to your personal data will always be bound by strict legal or contractual obligations to keep your personal data safe and confidential. This means that only the following categories of recipients will receive your personal data:

- You;
- Our employees and suppliers;

- The service provider connected to the platform (to the extent you consented to share your data with them); and
- Government or judicial authorities to the extent that we are obliged to share your personal data with them (e.g. tax authorities, police or judicial authorities).

4.2. We do not transfer your personal data outside the European Economic Area (EEA) (the European Economic Area consists of the EU, Liechtenstein, Norway and Iceland) in principle, except if you explicitly request us to do so, i.e. when you consent to data sharing with a service provider outside the EEA or if you would move to a country outside the EEA. If a transfer were to take place, we will take sufficient safeguards to protect your personal data during the transfer, either on the basis of an adequacy decision of the European Commission or if not yet in place, by entering into an agreement based on standard data protection clauses approved by the European Commission.

5. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

5.1. You can use the user interface on the platform to define the retention period for which we can share your personal data with any of the service providers you consented to. At any moment, you can decide to modify this pre-set retention period by using the user interface.

5.2. We will also stop processing your personal data when you decide to withdraw your consent for the processing. Note that we cannot technically oblige the service provider that has received your personal data based on your consent and has stored a copy of your personal data, to delete that copy. You can request the service provider to delete the copy of your personal data, by using the e-mail link that will allow you to directly communicate with the DPO of the service provider. Your request will be further handled according to the procedure of the service provider.

5.3. As a general rule, we will delete or de-identify your personal data when it is no longer needed for the purposes described above or when the retention period, as explained in this Article 5, has expired. This includes the termination of the ACROSS platform's operation, of which we would inform you in advance. However, we cannot delete your personal data if there is a legal or regulatory obligation or a court or administrative order preventing us from doing so.

6. HOW DO WE KEEP YOUR PERSONAL DATA SECURE?

6.1. The security and confidentiality of the personal data we process is very important to us. That is why we have taken technical and organizational measures to ensure that all personal data processed is kept secure. These measures include:

- Access controls: your personal data on the ACROSS Platform will only be accessible to third party service providers you consented to. The access to the ACROSS Platform will be controlled using a login and a secure password;
- Transfer controls: your personal data will be protected against unlawful interception through effective encryption (SSL encryption);
- Logging and audit trails: the exchanges of personal data on the ACROSS platform is logged in a way that allows all the interactions to be identified and examined. The logs only comprise metadata.

7. YOUR RIGHTS REGARDING YOUR PERSONAL DATA

7.1. The personal data the ACROSS platform stores about you, e.g. user name, password, etc. can be accessed, changed, corrected and deleted by you in the profile setting. You therefore do not need to send us a formal request for exercising these rights (although you of course are free to do so). If you want to exercise your rights against the service providers, you can use the e-mail link that is provided on the Platform, and which will allow you to directly contact the DPO of the Service Provider. The rights you can exercise against the service providers on the platform will be described in more detail below.

7.2. You can use the e-mail link to request from the service provider to give you access to your personal data. Additionally, you may also ask the service provider to provide you a copy of your personal data. Please be aware that the service provider may require some additional information to verify your identity. The reason for this is to prevent a data breach, by giving unlawful access to your personal data.

7.3. You have the right to request to request the service provider to correct your personal data if you can demonstrate that the personal data the service provider process about you is inaccurate, incomplete, or out of date. You can exercise your request by using the e-mail link that will allow you to communicate with the DPO of the Service Provider. We highly recommend that you to indicate in your e-mail the context in which the service provider uses your personal information (e.g., to respond to a request), so that they can review your request quickly and accurately.

7.4. If you have granted your consent to collect, use and share your personal data, you have the right to withdraw this consent at any time. The withdrawal of your consent will stop the data sharing with third parties in the ACROSS platform immediately. Note that, in this case, we will not require the third party service providers to delete your personal data which they had accessed before the withdrawal of your consent. You can use e-mail link within the ACROSS platform to communicate with the DPO of the service provider to delete your stored personal data by that service provider.

7.5. You may ask the service provider via the e-mail link on the ACROSS Platform to erase your personal data if these personal data are no longer necessary for the purposes for which they received them through the ACROSS platform, if their collection was unlawful or if you have successfully exercised your right to withdraw your consent or your right to object to the processing of your personal data by the service provider. When either of these circumstances applies, the service provider will be obliged to erase your personal data immediately, unless legal obligations or administrative or judicial orders prohibit them from deleting your personal data.

7.6. You may ask the service provider to restrict the processing of your personal data using the e-mail link:

- during the time needed to review your request for correction of your personal data;
- during the time needed to review your objection to the processing of your personal data;
- when such processing was unlawful, but you prefer a restriction to erasure; and
- when the service provider no longer needs your personal data, but you need them for the establishment, exercise, or defence of any legal action.

7.7. If we have collected your personal data on the basis of your consent, you have the right to obtain a copy from us in a structured, widely used and machine-readable format. .

7.8. If you wish to exercise any of these rights, you can use the e-mail link on the ACROSS Platform. By using the e-mail link, you can directly send your request to the DPO of the of the service provider. The service provider will further handle your request in accordance with their own internal procedures; please note that we cannot and will not intervene in this interaction, since we cannot monitor your communications with the service provider under applicable law.

7.9. If you have a complaint about the processing of your personal data by us, you can always contact us at hans.graux@timelex.eu. If you are not satisfied with our response, you may lodge a complaint with the competent data protection authority, you can find a list of the competent data protection authorities in the different European Member States and their contact information on this website (https://edpb.europa.eu/about-edpb/about-edpb/members_en).

8. CHANGES TO THIS PRIVACY POLICY

8.1. We can change this privacy policy on our own initiative at any time. If material changes to this privacy policy may affect the processing of your personal data, we will communicate these changes to you in a way that we normally communicate with you (e.g. via e-mail).

8.2. We invite you to read the latest version of this privacy policy on our website ([domain-name]).

9. DO YOU HAVE ANY QUESTIONS?

9.1. Should you have any further questions about the processing of your personal data, please do not hesitate to contact our data protection officer. You can contact our data protection officer by e-mail: hans.graux@timelex.eu.

6.2 Code of Conduct for Service Providers

ACROSS platform
Code of Conduct for Service Providers

1. INTRODUCTION

1.1. The ACROSS platform is a user-centric platform/gateway for European citizens to find and interact with trustworthy national governmental services and private sector Service Providers (hereinafter referred to as "Service Providers") in cross-border scenarios (i.e. "studying abroad" and "moving abroad"). Through the ACROSS platform public administrations and/or private sector Service Providers can gain access to personal data of Citizen Users, based on the consent of that user.

1.2. The ACROSS platform aims to enable data sharing with a potentially unlimited range of Service Providers, including public sector and private sector Service Providers. Public sector Service Providers are typically considered trustworthy to a significant extent, based on the fact that they must operate within the limits of a legally defined mandate. Private sector Service Providers are however not subject to the same constraints with regards to the processing of personal data of citizens. For that reason, the ACROSS operator has identified the need to implement additional measures in place, particularly to ensure the privacy of the data shared by users through the ACROSS Platform. This Code of Conduct is one such measure.

1.3. Service Providers are independent data controllers (distinct from the ACROSS operator) in relation to the data they receive through the ACROSS platform. In simpler terms, the ACROSS operator ensures the proper operation of the platform, including by technically supporting any connections to the Service Providers; and the Service Providers use the data they receive for the purposes they've communicated to the user. In that sense, the Service Providers have their own responsibilities under data protection legislation. However, as a part of the ethics requirements in developing the ACROSS platform, the project partners have identified a need to set a minimum level of data protection that must be respected by every user of the ACROSS platform. This is done in practice by requiring Service Providers (whether public or private) to agree to respect the provisions of this Code of Conduct. In this way, ethical behaviour is more likely to occur at the Service Providers' side, since they are contractually bound by the provisions of this Code, both towards the ACROSS operator and towards the ACROSS platform users.

1.4. The ACROSS platform is designed with privacy and data protection in mind, in accordance with the privacy by design and the privacy by default principles set out in the General Data Protection Regulation (hereinafter referred to as the GDPR). This Code of Conduct has been developed with these principles in mind: it provides an effective tool to ensure that Service Providers process personal data of Citizen Users in compliance with data protection legislation, and that they are following the general ACROSS data protection framework.

2. THE PURPOSE AND SCOPE OF APPLICATION OF THIS CODE

2.1. The purpose of this Code is to foster justified trust among the Citizen Users (i.e. any natural persons using the platform, irrespective of their nationality or place of establishment) of the ACROSS Platform, by ensuring an appropriately high standard of data protection for any data processing activities that occur by Service Providers, even outside of the perimeter of the Platform. The Code aims to fulfil this goal by providing guarantees to ensure the proper application of the GDPR principles and general good conduct principles.

2.2. Crucially, this Code of Conduct and its principles apply to data processing activities not only in direct interaction with the Platform (i.e. when Service Providers request data via the Platform, or receive it via the Platform), but also to processing activities outside of the Platform (i.e. for processing activities undertaken after the Service Provider has received the data, including processing activities on its own infrastructure). In all instances, the provisions of the Code are binding, except where applicable and binding legislation requires the Service Provider to disregard the terms of the Code (i.e. if a Service Provider, whether public or private sector, is required by applicable laws to engage in processing activities or other behaviours that are not permissible under this Code, applicable laws will take precedence).

2.3. This Code applies to any Service Providers that are using the ACROSS platform to provide their services. Adherence to the Code by these Service Providers is a condition to use the ACROSS platform. Every Service Provider must submit a legally binding declaration of compliance to the ACROSS platform operator before registering to the platform. Annex I provides a template for a self-declaration of compliance to this Code of Conduct, which must be accepted by the Service Provider.

3. GENERAL RULES OF CONDUCT

3.1. The present section will define behaviours that are considered unacceptable when using the ACROSS platform.

3.2. The following behaviours are forbidden:

- Service Providers may not directly or indirectly discriminate citizens based on their nationality, race or ethnicity, background, family status, gender identity or expression, marital status, sex or sexual orientation, age, (dis)ability, socioeconomic status, religion, geographic location, experience, etc.
- Service Providers may not use the ACROSS platform to enable the spread of false information and/or hate speech towards people or other organizations;
- Service Providers may not hack the ACROSS platform and will not use the ACROSS platform for acts that may result in illegal access to data from linked sources, which would impair the proper functioning of the ACROSS platform or the jeopardizing the use of available functionalities to other Citizen Users;
- Service Providers cannot use the ACROSS name, logo, work or other images in an inappropriate way, which includes any misleading use (such as suggesting any partnership or support of the ACROSS operator) and any violation of any applicable intellectual property laws.
- It goes without saying that, in addition to this Code, any action or inaction that is unlawful under EU law or under any national law that applies to the Service Provider is also forbidden, even if the terms of this Code of Conduct might suggest otherwise.

3.3. Service Providers must also ensure the accuracy of the information provided by them on the ACROSS platform, e.g. when providing URLs on the ACROSS platform where citizens can check their application for services, the Service Provider must ensure that this URL is valid, and that it is update as needed. They must periodically check the URL on any suspicion of phishing or hacking.

3.4. Service Providers must notify any identified improper or unlawful use of the ACROSS platform of which they become aware, e.g. hacking, presence of illegal content on the ACROSS platform, presence of discrimination by other Service Providers on the ACROSS platform, etc. by sending an e-mail to […] so that ACROSS can take necessary and appropriate action if necessary.

4. DATA PROTECTION PRINCIPLES

4.1. Principle of purpose limitation: Service Providers using the ACROSS platform must respect the principle of purpose limitation. This means that the personal data of the Citizen User that is shared via the ACROSS platform can only be used for the purposes of providing the services that the Citizen User has selected on the platform and which have been clearly communicated to the citizen in the service description on the ACROSS platform.

Service Providers may only use the data provided by the Citizen User for purposes compatible with those for which the personal data have been initially collected or for which the Citizen User has decided to make them available to the Service Provider. The Service Provider must in this case that into account the following:

- The possible link between the purposes;
- The context in which the personal data have been collected, in particular taking into account the relationship with the data subjects and the usage disclosed to the Citizen User;
- The nature of the personal data (specifically its sensitivity under EU or national law, but also more generally its privacy sensitivity to a reasonably diligent person);
- The possible consequences of the intended further processing for data subjects; and
- The existence of appropriate safeguards.

4.2. Principle of data minimisation: Service Providers that are using the ACROSS platform must carefully consider what data is strictly necessary for the provision of the services. Only the personal data that is strictly necessary for the provision of the service can be requested as mandatory data by the Service Provider through the ACROSS platform. Service Providers may not collect or process more data or use the data for a longer duration than is strictly necessary to achieve this purpose.

4.3. Principle of transparency: Service Providers must provide the Citizen Users with clear information about the personal data they are processing, the purposes of this data processing, the legal basis and any third parties with whom they will share the personal data. The Citizen Users must also be provided with information about their data subject rights and the way in which they can exercise those rights. The Service Provider shall make sure that the information that is provided to the Citizen Users is sufficiently understandable and clear.

4.4. Principle of storage limitation: the Service Provider shall ensure that the personal data of Citizen Users is processed no longer than is necessary for the provision of the services and in any case in accordance with mandatory retention periods set forth in applicable legislations. Service Providers must establish time limits for erasure or for a period review of the personal data they store or process. Wherever this is technically, operationally and legally feasible, the Service Provider shall retain the Citizen User's data only for a minimal amount of time as needed to provide the services communicated to the user, without storing that Citizen User's data after the service has been provided. In other words, the Service Provider acknowledges that they are legally required under this Code to attempt to use the ACROSS Platform to access the Citizen User's data dynamically during each use of the data, without storing

it outside of the ACROSS Platform whenever this is feasible. The ACROSS Platform endeavours to be a dynamic data sharing platform from which data can be accessed when needed, not a source from which data is copied permanently.

5. RULES ON INTERNATIONAL TRANSFERS OF THE CITIZENS PERSONAL DATA

5.1. In the case of transfers of citizens personal data to countries outside the European Economic Area (EEA, i.e. the EU Member States, Norway, Iceland and Liechtenstein), the Service Provider shall be responsible for ensuring the existence of any safeguards according to Chapter V of the GDPR, and shall take into account applicable judgements (such as the Schrems II Court of Justice Judgement) and EDPB guidelines, notably Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. If the Service Provider is unable to do so for whatever reason, it must refrain from using the ACROSS Platform as a source to access personal data.

5.2. Transfers to third countries shall only take place when strictly necessary for the provision of the service. When a Service Provider would rely on sub-processors that are established outside the EEA, the Service Provider shall take reasonable steps to search for an EU alternative. If no alternative is available, the Service Provider shall make sure that the international transfer takes place only if the conditions in Chapter V GDPR are met. This means that one or more of the following conditions must be satisfied:

- The locations are countries which are covered by an adequacy decision of the European Commission ;
- The third party has provided appropriate contractual guarantees through the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries, or through the conclusion of Binding Corporate Rules (BCRs);
- Transfers are permissible if the Service Provider has obtained the Citizen User's unambiguous consent to the proposed transfer. However, transfer is only a valid ground for occasional and clearly identified transfers, not for repeated or structural transfers. If the Service Provider intents to systematically and frequently transfer data to a location outside of the EU/EEA, one of the two aforementioned conditions should be satisfied.

6. RIGHTS OF THE DATA SUBJECT

6.1. Service Providers using the ACROSS platform acknowledge that the Citizen Users have the following data subject rights under the GDPR:

- The right to access the personal data relating to them that the Service Provider is processing, including the right to receive a copy of the personal data;

- The right to obtain corrections of the personal data if it is incorrect or outdated;
- The right to object to any further processing of the personal data by the Service Provider;
- The right to request a restriction of the processing;
- The right to demand a deletion of the personal data;
- The right to request data portability;
- The right not to be subject to automated decision-making; and
- The right to submit a complaint to a competent supervisory authority

6.2. Service Providers shall ensure that Citizen Users can exercise such rights towards the Service Providers, even if European data protection laws do not formally apply to them. Service Providers shall take any actions reasonably necessary, and shall act in good faith, to ensure that the exercise of rights by Citizen Users towards them is practically feasible in the same manner and under the same conditions as is required under EU data protection law.

6.3. The ACROSS platform provides means for the Citizen User to exercise his or her data subject rights, specifically by providing contact information (an email address) of the data protection officer (DPO) or data protection contact point of the Service Provider. This means that each Service Provider that uses the ACROSS platform must nominate a data protection officer, when required under the GDPR or under other applicable law. When the Service Provider is not obliged to nominate a data protection officer, the Service Provider shall instead designate a point of contact for data protection related issues, meeting the requirements of chapter IV, section 4 GDPR.

6.4. The Service Provider is responsible for responding to the data subject request within the mandatory timeframe. The Service Provider shall not refuse to respond to a data subject request except when its not in the position to identify the data subject and it has taken reasonable steps to identify the data subject (e.g. by asking proof of identity documentation such as a passport or a drivers license).

6.5. The Service Provider must have documented procedures in place for fulfilling data subject requests, and must ensure that these procedures are adhered to in practice, and that they are effective in responding to Citizen User rights request.

7. TECHNICAL AND ORGANISATIONAL MEASURES

7.1. Service Providers are required to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, disclosure, access and other unlawful forms of processing.

7.2. The appropriateness of the implemented security measures will be highly dependent on the nature of the data that is processed (sensitivity) and its potential impact on the user. At minimum, the Service Provider must have the following security measures in place:

Technical measures:

- Equipment Access Control: deny unauthorised persons access to processing equipment used for processing;
- Data Media Control: prevent the unauthorised reading, copying, modification or removal of data media;
- Storage Control: prevent the unauthorised input of personal data to unauthorised inspection, modification or deletion of stored data;
- User Control: prevent the use of automated processing systems by unauthorised persons using data communication equipment;
- Communication Control: ensure that it is possible to verify and establish the bodies to which personal data have been or may be transmitted or made available using data communication equipment;
- Input Control: ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input;
- Transport Control: prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (by implementing encryption controls for any transit of data);
- Recovery: ensure that installed systems may, in the case of interruption, be restored;
- Ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Organizational measures:

- Sub-contracting: the Service Provider must conclude data processing agreements with all the sub-processors it contracts with to process the personal data of the Citizen Users. Prior to contracting with a sub-processor, the Service Provider must also assess whether their level of compliance with data protection legislation is considered appropriate.
- Data protection officer or data protection contact point: the Service Provider must nominate a data protection officer, when required under the GDPR. When the Service

Provider is not obliged to nominate a data protection officer the Service Provider shall have a point of contact for data protection related issues, meeting the requirements of chapter IV, section 4 GDPR;

- Privacy notices/policies: the Service Provider must have the required privacy notices and general privacy policies in place informing the Citizen Users about the processing of their personal data. The privacy policy and notices must fulfil the requirements as set forth in Article 13 and 14 of the GDPR.
- Incident response and data breach procedure: the Service Provider must have a incident response and data breach procedure in place which explains in detail the steps that need to be taken when a data breach occurs and which assigns responsibilities. More information on the data breach procedure can be found under clause 7.

7.3. The Service Provider must duly document its technical and organisational measures and must keep them up-to-date taking into account any changes in legislation, guidance by supervisory authorities or any lessons-learned from data breaches that may have occurred. The Service Provider must ensure that in case of new or updated technical and organisational measures, the level of protection remains equal as to the measures set forth in clause 6.2., and that no less protective measures shall be implemented.

8. DATA BREACHES

8.1. A data breach occurs when any Citizen User's personal data is subjected to an incident leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, that personal data.

8.2. The Service Provider must have a clear process in place in case (suspected) data breaches occur. The data breach procedure must include at least the following steps:

1. The Service Provider must consider whether citizen's data that has been provided through the ACROSS platform is impacted by the data breach, and if yes, which personal data has been impacted.
2. The Service Provider shall duly consider whether there is a duty to notify the data breach to any supervisory authority in a specific country or countries. The Service Provider shall respect the time frames set forth in the GDPR, meaning that it shall make the notification (if mandatory) without undue delay and, in any case, no later than 72 hours after having become aware of the breach. The Service Provider shall also notify the data breach to the impacted data subjects, if it considers that the breach has a high impact on the rights and freedoms of those data subjects.

3. The Service Provider must perform a root cause analysis of the data breach and implement as soon as possible any mitigating measures to address the data breach and to avoid any further breaches. The lessons learned should be used to assess the appropriateness of the implemented security measures.

9. ENFORCEMENT OF THIS CODE OF CONDUCT

9.1. Any non-compliance with the general conduct rules and the GDPR principles listed above will not be tolerated. Any user of the ACROSS Platform who becomes aware of a non-compliance by any Service Provider using the ACROSS platform (including the Service Provider itself) must notify this non-compliance via: [...].

9.2. Any identified non-compliance with the rules of this Code of Conduct will be assessed and investigated by the ACROSS platform operator, and appropriate measures will be taken to address the situation. These measures will be dependent on the nature, severity and duration of the infringement and the intentional or negligent character of the infringement.

9.3. The following measures (non-exhaustively) can be taken by the ACROSS operator at its sole discretion:

- Warning;
- Request to bring activities in compliance with this Code of Conduct;
- Temporarily suspension from the ACROSS platform;
- Expulsion from the ACROSS platform;

ANNEX I: SELF-DECLARATION OF COMPLIANCE FORM

By signing this self-declaration of compliance form, I declare, on behalf of the entity that I lawfully represent, that I have read and understood this Code of Conduct. I also declare that I will comply with the obligations and measures set forth in this Code of Conduct, and that I shall ensure that these obligations and measures shall also be respected within the entity that I lawfully represent.

Name: […]

Function: […]

Signature: […]

Note: this form may also be implemented in the form of a checkbox declaration during the onboarding of Service Providers, e.g.:

☐ I confirm that I have read and understood the terms of the Code of Conduct of the ACROSS Platform, and agree to be bound by them, both personally and on behalf of the organisation that I represent.

6.3 Data Protection Impact Assessment on ACROSS platform

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

Data protection impact Assessment ACROSS Platform

Project Reference No	959157 — ACROSS — H2020-SC6-GOVERNANCE-2018-2019-2020
Deliverable	Data Protection Impact Assessment (DPIA)
Work package	WP8: ethics requirements
Nature	Report
Dissemination Level	Confidential, only for members of the consortium (including the Commission Services)
Contributor(s)	Jolien Clemens, Timelex Hans Graux, Timelex
Document description	This document is the documented result of the Data Protection Impact Assessment that was performed on the ACROSS platform during the final year of the project. Information was collected through the technical deliverables and through interviews with relevant stakeholders.

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
V1.0	23/08/2023	Initial draft	TLX
V1.1	04/10/2023	Revised draft for release within the consortium	TLX
V.2.1	17/04/2024	Revised draft based on feedback of the partners	TLX

Executive Summary

This Data Protection Impact Assessment (DPIA) was drafted in the context of the EU funded ACROSS project. It aims to assess data protection compliance risks in relation to the ACROSS Platform (the Platform), which is being developed in that project.

At a high level, the Platform allows individual persons to make their data available in a secure way towards service providers, for specifically defined use cases, on the basis of their consent. The users are capable of managing their consents at any time, and of exercising their data subject rights towards the service providers.

This DPIA aims to comply with the requirement under applicable EU data protection law, notably the General Data Protection Regulation (GDPR), to establish a DPIA and implement appropriate mitigation measures to ensure that data processing activities within the scope of the DPIA are acceptably secure, and compliant with EU data protection law.

As with any other DPIA, this is a living document that will be maintained over time, specifically until the termination of the ACROSS project.

Table of Contents

1 INTRODUCTION 7

1.1 PURPOSE AND SCOPE 7

1.2 METHODOLOGY AND STRUCTURE OF THE DELIVERABLE 8

2 GDPR CONSIDERATIONS IN ACROSS 9

2.1 GDPR REQUIREMENTS FOR THE RESEARCH ACTIVITIES (CO-CREATION AND CO-DELIVERY SESSIONS) 9

2.1.1 Introduction 9

2.1.2 The concept of personal data in research activities 9

2.1.3 The Consortium's partners responsibilities under the GDPR 10

2.1.4 Checklist of the main GDPR requirements for the research activities 11

2.1.5 GDPR requirements for the ACROSS platform 16

2.2 DESCRIPTION OF THE DELIVERED COMPLIANCE WORK 16

2.2.1 GDPR compliance work in relation to the co-creation sessions and co-delivery sessions 16

2.2.2 GDPR compliance work in relation to the ACROSS platform 18

2.3 LEGAL GAP ANALYSIS IN RELATION TO THE GDPR COMPLIANCE WORK 21

3 LEGAL CONSIDERATIONS IN RELATION TO THE VIRTUAL ASSISTANT 22

3.1 DATA PROTECTION 22

3.1.1 Data protection considerations 22

3.1.2 Implementation in ACROSS 23

3.2 AI ACT 24

3.2.1 Applicability of the AI Act to the ACROSS Virtual Assistant 24

3.2.2 AI Act requirements for the ACROSS VA 28

3.2.3 How did the ACROSS VA take the AI Act into account? 29

4 CONCLUSIONS 30

5 REFERENCES 31

6 ANNEXES 32

6.1 PRIVACY POLICY FOR ACROSS PLATFORM 32

6.2 CODE OF CONDUCT FOR SERVICE PROVIDERS 41

6.3 DATA PROTECTION IMPACT ASSESSMENT ON ACROSS PLATFORM 51

1 INTRODUCTION 1

1.1 PURPOSE AND SCOPE 1
1.1.1 What is a Data Protection Impact Assessment (DPIA)? *1*
1.1.2 Terminology *2*
1.1.3 Why is a DPIA necessary for the ACROSS Platform? *3*
1.2 METHODOLOGY AND STRUCTURE OF THE DELIVERABLE 4
2 DESCRIPTIVE ANALYSIS 6
2.1 MAIN COMPONENTS OF THE ACROSS PLATFORM 6
2.2 DESCRIPTION OF THE PROCESSING ACTIVITIES IN THE ACROSS PLATFORM 9
2.2.1 The purposes for processing *9*
2.2.2 The data subjects *10*
2.3 IDENTIFICATION OF THE DIFFERENT STAKEHOLDERS (OTHER THAN THE DATA SUBJECTS DESCRIBED ABOVE) 11
2.4 CATEGORIES OF PERSONAL DATA PROCESSED 12
2.4.1 Use case: data shared when moving for work *13*
2.4.2 Use case: data shared when moving for studies *14*
2.4.3 Personal data stored on the ACROSS infrastructure *15*
2.5 SUPPORTING ASSETS 17
3 APPRECIATIVE ANALYSIS 19
3.1 FUNDAMENTAL DATA PROTECTION PRINCIPLES ANALYSIS 19
3.2 DATA SUBJECT RIGHTS ANALYSIS 26
3.3 TECHNICAL SECURITY CONTROLS 30
3.4 ORGANIZATIONAL SECURITY CONTROLS 33
4 RISK ASSESSMENT AND THEIR MITIGATING MEASURES 35
4.1 ILLEGAL ACCESS TO PERSONAL DATA 36
4.2 UNAUTHORIZED MODIFICATION OF PERSONAL DATA 37
4.3 LOSS OF PERSONAL DATA 38
5 ACTION POINTS 40
5.1 HIGH PRIORITY 40
5.2 MEDIUM PRIORITY 40
5.3 LOW PRIORITY 40

List of Terms and Abbreviations

Abbreviation	Definition
DPIA	Data Protection Impact Assessment
FDM	FISA Dialog Manager
GDPR	General Data Protection Regulation
PIA	Privacy Impact Assessment

1 Introduction

1.1 Purpose and Scope

1.1.1 What is a Data Protection Impact Assessment (DPIA)?

A Data Protection Impact Assessment (DPIA) is a concept introduced by the General Data Protection Regulation (hereinafter GDPR).[1] A DPIA is a structured process for managing data protection risks of certain processing operations causing 'high risks' to data subjects and are therefore not necessary for all kinds of processing activities.

A DPIA is only mandatory if the processing "*is likely to present a high risk to the rights and freedoms of natural persons*" (Article 35(1) GDPR). The GDPR provides a number of examples of when processing is "*likely to present a high risk*":

- *"(a) A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;*
- *(b) Processing on a large scale of special categories of personal data referred to in Article 9(1) or of personal data relating to criminal convictions and offences referred to in Article 10; or*
- *(c) A systematic monitoring of publicly accessible areas on a large scale.*[12]

The ethics advisor in the ACROSS project had initially determined that a DPIA is not mandatory based on the legal criteria mentioned above and the guidelines by the European Data Protection Board.[13] Nonetheless, DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the GDPR.

Therefore, project partners agreed that performing a DPIA is desirable in order to manage and enhance compliance with applicable data protection laws later on.

Lastly, it is important to mention that any DPIA is inherently a living document, which must be continuously maintained, re-assessed and if necessary updated over time, as processing activities, risks and mitigating measures evolve. It is intended to maintain this DPIA until the termination of the ACROSS project.

[12] Article 35 (3) GDPR.
[13] The EDPB guidelines can be found via the following link: .

1.1.2 Terminology

1.1.2.1 Processing of personal data

As described above, a DPIA is mandatory when the processing of personal data is likely to present a high risk to the rights and freedoms of natural persons. Two elements of this definition need to be described more precisely: personal data and processing.

"**Personal data**" is defined in the GDPR as "any information relating to an identified or identifiable natural person ('data subject')".[14] It is obvious that personal details of a person are personal data for example their name, address, et cetera. Randomly chosen identifiers such as alphanumeric strings can also be considered personal data, insofar an individual can be singled out from all other individuals on the basis of this identifier. The qualification as "personal data" is not dependent on whether or not the randomly chosen identifier can ultimately be linked with someone's name, the capacity to "single out" suffices.

Important to note is that data may be personal whenever someone is able to link the data to an individual, insofar it can be done with "reasonable means". Hence, the personal character of the data should not only be assessed from the perspective of the organization engaging in its processing, but also from the perspective of others who may have other data or information which allows data to be linked to an individual.

"**Processing**" is defined in the GDPR as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[15]

1.1.2.2 Roles and responsibilities of the controller

According to Article 34 GDPR, the responsibility to carry out a DPIA lies with the "controller". The controller is the entity that determines the purpose and the means of the processing (the "why" and the "how" of a processing activity).[16] A controller can be a natural or legal person, public authority, agency or other body.

In some cases, more than one entity will play a role in determining the purpose and the means of the processing. They can act together either as joint controllers (where they jointly determine the purpose

[14] Article 4 (1) GDPR.
[15] Article 4 (2) GDPR.
[16] Article 4 (7) GDPR.

and the means) or as multiple separate controllers (where, for instance, they each separately have their own purpose for the same processing).

Sometimes a controller relies on the services of a third party for whole or part of the data processing activities. The third party processes the personal data only at the instruction(s) of the controller and is therefore, in the language of the GDPR, a processor.[17]

1.1.3 Why is a DPIA necessary for the ACROSS Platform?

It is important to note that the ACROSS platform will not be used/tested during the project on real end users (i.e.) data subjects, but rather 'personas', using a test bed designed to emulate operational services they are using or intend to use through the ACROSS platform. Personas are in effect fictitious persons, which are credible and realistic, but not directly or indirectly based on identifiable real persons. Therefore, **personas are not humans** (or data subjects in the sense of the GDPR), **nor are they research participants** in the sense of this deliverable. Reliance on personas allows in-depth emulation, analysis and research, without triggering any data protection or privacy concerns.

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, 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.

Performing a DPIA would also help with implementing **data protection by design** (Article 25 GDPR) as a principle for the ACROSS platform, as it is an important tool for data controllers to show that appropriate measures have been taken to ensure compliance with the GDPR. This is also strongly connected to **the accountability obligations** (Article 5.2 GDPR) of the controller. A DPIA could be used as documentary evidence to provide proof of compliance to Supervisory authorities, public and private service providers wanting to use the platform, end-users, et cetera.

[17] Article 4 (8) GDPR.

1.2 Methodology and Structure of the Deliverable

There is no fixed methodology for performing a DPIA correctly. The GDPR leaves a lot of personal appreciation and responsibility to the person performing the assessment. Nevertheless, the GDPR18 does provide a list of minimum requirements that must be included in a DPIA:

- A systematic description of the intended processing operations and the purposes of the processing, including, where applicable, the legitimate interests pursued by the controller;
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of the data subjects; and
- The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

From these four (4) mandatory requirements it is possible to distil the two-step approach to performing a DPIA that will be followed in this template. It consists of (i) a descriptive part and (ii) an appreciative part.

The **descriptive part** will give a detailed overview of the processing activities conducted by The elements that will be discussed are the following:

- A functional description (incl. nature, scope, context and purposes) of the processing activity;
- A list of the personal data processed, categories of recipients of the data, the period for which the data are stored;
- The supportive assets of the processing activities.

The **appreciative part** will discuss the following elements:

- Fundamental principles analysis
- A data subject right analysis
- Technical and organizational security controls
- Risk assessment

[18] Article 35 GDPR.

For the appreciative part, which necessarily includes a risk assessment model, this DPIA relies on the PIA (Privacy Impact Assessment) methodology proposed by the French data protection authority (CNIL).19 This PIA methodology was developed under the old data protection framework of Directive 95/46/EC, and has since been updated to be applied also under the GDPR.

The risk assessment model has two dimensions (risk severity and likelihood of occurrence) and four levels for each dimension:

Severity	Level	Likelihood of occurrence
Data subjects either will *not be affected* or may encounter *a few inconveniences*, which they will overcome *without any problem*.	**Negligible (Low)**	It does *not seem possible* for the selected risk sources to materialize the threat by exploiting the properties of supporting assets.
Data subjects may encounter *significant inconveniences*, which they will be able to overcome despite a *few difficulties*.	**Limited (Low)**	It seems *difficult* for the selected risk sources to materialize the threat by exploiting the properties of supporting assets.
Data subjects may encounter *significant consequences*, which they should be able to overcome albeit with *real and serious difficulties*.	**Significant (High)**	It seems *possible* for the selected risk sources to make the threat materialize by exploiting the properties of supporting assets.
Data subjects may encounter *significant, or even irreversible, consequences*, which they may not overcome.	**Maximum (High)**	It seems *extremely easy* for the selected risk sources to make the threat materialize by exploiting the properties of supporting assets.

Table 1 – Risk Assessment Model

[19] Available in English: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf.

2 Descriptive analysis

2.1 Main components of the ACROSS platform

The following section relies on inputs from D5.1 System Architecture & Implementation Plan; it will be updated and revised as needed during the project's further execution.

Back end components:

- **The User Journey Modelling Tool**: the Modelling Expert is responsible for modelling the identified cross-border services as User Journey Models in the User Journey Modelling Tool. This Tool will create from each User Journey a machine-readable User Journey Workflow description (using a open-source drawing software Draw.io) for the service orchestration which is provided to the User Journey Service Engine.
- **The User Journey Service Engine:** The machine-readable User Journey Workflows Descriptions will be provided and initiated towards the citizens through the User Journey Service Engine, which will transform the machine-readable workflows into concrete User Journey Service Workflows. The citizen can access the workflows and select services through the Web Application, or through the Virtual Assistant (see more information below).
- **The Service Catalogue:** this component has three modules:
    - Service registry of all the available services in the ACROSS platform. The Service Provider will be responsible for the registration of their service (this includes information on the purpose, the personal data needed for the service and a general (technical) description of the service, based on standard models (e.g. ISA2, W3C DPV, etc.). Each service will be identifiable in the Platform via a Service ID.
    - Metadata and Vocabulary catalogue: this module provides metadata references for service data mapping.
    - Data connectors dashboards: this module provides a visual dashboard to manage the status of services connected to the platform by means of a specific data connector instance. The data connectors allow the citizens to receive updates on the status of their applications to certain services.
- **Citizen Data Ownership component**: this component allows citizens to manage their personal data usage by public and private service providers. It provides several interfaces for the Transparency Dashboard, where users can grant and withdraw their consents and receive

notifications on how their data is being used. Other interfaces will inform service providers about the user's consent and allows them to send notifications on the data usage to users.

- **Usage control component**: this component allows the enforcement of usage control policies.

Citizen Front End components:

- **A Multi-lingual Virtual Assistant (VA)**: the user-interfacing ACROSS applications will be able to connect to the VA, which will benefit the User Experience. The VA enables a conversational interaction mode through natural language (text) and speech. The user can interact with the VA which will navigate them through the different steps in the process defined by the User Journey. The VA will consist out of the following functionalities:
    - Textual chat-bot user interface
    - Conversational user interaction navigation support
    - Conversational support for executing individual interactions
    - Q&A functionality for obtaining additional information conversationally
    - Support for multi-lingual operation, for selected languages corresponding to the use-cases (Greek, Latvian and German)
    - For selected languages: acoustic speech user interfaces, which can convert speech-to-text (STT) and text-to-speech (TTS)
- **The Web Application:** the web application will provide a one-stop-shop service for the citizen. The application enables the process of cross-border digital service and tackles the difficulty of finding the correct digital public service and the different steps that need to be taken. Through the web application the citizen will be able to access their personal User Journey Services, a visualization of the services orchestration of their User Journey for moving, and virtual assistance in the User Journey Experience.
    - The web application will make use of the overall JavaScript framework. The web application will be implemented by following the guidelines of material design.
    - The application will be developed with the official SDKs and tools provided by Apple and Google for iOS and Android respectively.
- **Transparency Dashboard**: this is a web-application that uses a human centric approach to liberate the potential of personal data and to facilitate its controlled flow from multiple data sources to applications and services. It enables data control by the citizens and allows easy opt-in and opt-outs from the use of their personal data by third party service providers (grant and withdraw

consents). Through the transparency dashboard the citizen receives notifications on how their data is used and processed by the third-party service providers.

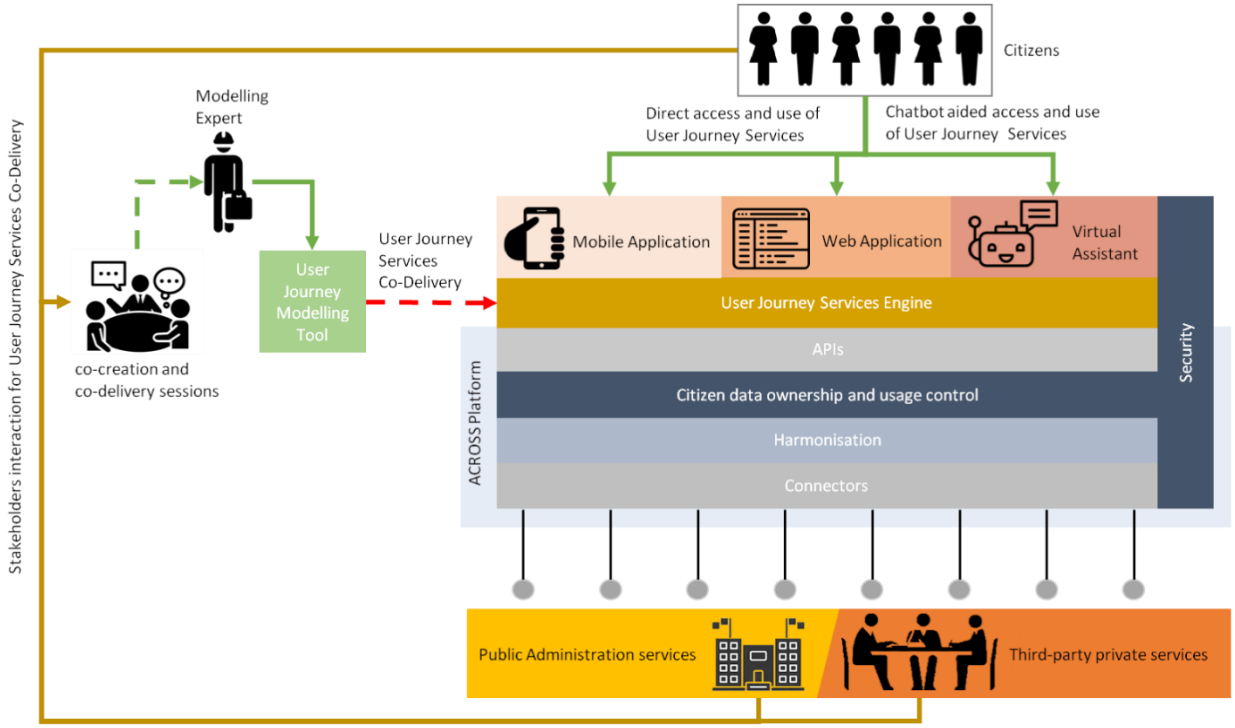

Figure 1 – ACROSS conceptual architecture (Figure copied from D. 5.1)

The following components/functionalities are outside the scope of the ACROSS project (and thus also outside the scope of this DPIA) as they are being developed in other projects/initiatives:

- Data wallet component
- Secure data transfers technologies
- External identification services (such as national identification schemes and the eIDAS nodes through which authentication can take place)

2.2 Description of the processing activities in the ACROSS Platform

2.2.1 The purposes for processing

The main purpose for processing data in the ACROSS Platform is **to enable data sharing in cross-border services with a user-centric approach**, meaning that the citizen will be able to control the access and use of their personal data and documents by private and public service providers. The citizen can choose freely to share its data through the ACROSS platform with both public and private service providers, in accordance with the once-only-principle.

Next, the following purposes have been identified:

- The personal data of the citizen may also be used when **a data subject exercises their rights on the ACROSS platform** (e.g. when they ask for a copy of their personal data on the platform). In that case the platform operator will solely use the personal data of the citizen to respond to the data subject request.
- The platform operator will process metadata on user usage of the platform (such as activity, behaviour, profile, etc.) to **enable a user-friendly functioning of the platform and for optimization of the components of the platform**.
- **To comply with legal obligations or to comply with any reasonable request from competent police authorities, judicial authorities, government institutions or bodies, including competent data protection authorities**.
- **To prevent, detect or combat fraud or other illegal or unauthorized activities on the platform**, for example to prevent unauthorized access s to the platform and to personal data of citizens.
- **Data may be processed in order to use as defence in legal proceedings**.

2.2.2 The data subjects

The **citizen** or **the end-user** are the main data subjects under the GDPR, since their personal data will be processed in the ACROSS platform. For completeness, the second category of data subject that needs to be mentioned here are the natural **contact persons (employees or staff) of the public and private service providers**.

Personal data of other data subjects may also be processed indirectly (including, but not limited to):

- **Parents:** underage children that want to travel for studies may also submit information about their parents through the ACROSS platform e.g. certain authorizations may be required.
- **Children**: when a parent is moving for work together with their child, data of the child will also be collected for applying to education institutions.
- **Family members**
- **Professors and other academics (such as Erasmus coordinators)**: when a student wants to travel for studies it may be possible that information about professors will be shared through the ACROSS platform (e.g. in case of a reference letter). In case of an Erasmus exchange, information about the Erasmus coordinator of the student will be processed.
- **Health care providers**: this information may potentially be shared through the ACROSS platform in case the citizen wants to apply for health care insurance or when the citizen is looking for a general practitioner (GP) when moving to another member state.

These 'indirect data subjects' are not ACROSS platform users themselves (since they do not interact with the ACROSS platform personally), but their information may be included as a 'payload' within any data being shared with a service provider. For that reason, their interests and rights must be considered as well.

2.3 Identification of the different stakeholders (other than the data subjects described above)

Stakeholder	Role	Justification
The platform operator	Data controller	The platform operator is the entity that hosts the citizen's personal data. They determine the purpose and the means of the platform, and should therefore be considered as a data controller under the GDPR for the processing operations that are inherent to the platform's functionality (and thus explicitly excluding processing activities by the service providers).
The public/private service provider	Data controller	The service providers (i.e. the organisations with whom the user chooses to share its data via ACROSS) are independent data controllers. They determine the purposes and means for their own use cases. For example, a university decides independently on which information it needs from a student applying for a study program, and how that information is further used within its administration.
Infrastructural IT service providers (e.g. Red Hat: provider of Keycloak**)**	Data processor	If any other IT service providers are used, e.g. hosting service providers, identity management service provider, etc. they must be considered as data processors under the GDPR. These service providers will solely process the personal data in the ACROSS platform on the basis of instructions of the platform operator. The platform operator must enter into data processing agreements with these IT service providers which must comply with the requirements of Article 28 of the GDPR.

Table 2 – Identification of the different stakeholders

2.4 Categories of personal data processed

A potentially vast amount of personal data and documents can be processed through the ACROSS platform (although, as noted above, during the project's duration, processing activities are limited in scope and focus on fictitious personas rather than real persons).

For reasons of harmonization, the ACROSS Personal Data Framework will use a personal data model defined on DPV-PD: Extended Personal Data Categories for DPV Taxonomy and Classes.[20] This is the model that will describe the categories of personal data.

Based on an assessment of the main use cases[21], the tables below will provide a non-exhaustive overview of the categories of personal data that is collected and shared when a citizen wants to move for work or for studies to another Member State. It is important to highlight that this list will not be exhaustive as the data asked by service providers will differ for each of the requested services and on the country to where the citizen will be moving. Conceptually, any kind of personal data can fall within the scope of the platform. User control and reliability of the service providers are thus critical to the security of the platform, since the operator will not constrain the categories of personal data as such.

It is important to note that the personal data and documents mentioned below **will not be stored on the ACROSS platform** itself, ACROSS will rather work as an **intermediary service** to allow for the citizen to easily access the public and/or private services. It must be clear that ACROSS provides the functionalities for users to connect and access public/private services that are offered by public administrations and private providers. The data is accessed through heterogeneous sources, such as repositories, systems managed and owned by public administrations, etc.

[20] https://w3c.github.io/cg-reports/dpvcg/CG-FINAL-dpv-pd-20221205/.
[21] Information was derived from D6.1 Use Case scenarios & roadmap.

2.4.1 Use case: data shared when moving for work

Category of personal data	Description
Common identifying data	This data includes name, age, place and date of birth, place of residence, address (street, house number, ZIP code, city or community), etc.
National identification number	The national identification number will also be on official documents. Other identification numbers may include: social security number, tax identification number, etc.
Contact information	Telephone number, email address (personal and/or work).
Data concerning family	Family composition, marital status, etc.
Data concerning employment	Employment history, experience, information about previous income, proof of payroll, etc. Self-employed may be required to provided proof of their self-employed status.
Data concerning insurances	Social security number, health insurance number, information regarding pension plan and other benefits, information about previous health insurance company, proof of insurance coverage, etc.
Financial data	This data includes bank account, financial account number, financial status, tax declaration, tax return, etc.
Official documents	Certificate of birth, residency permit, certificate of marital status, tax declaration, official diploma's, residence permit, identification documents, rental agreement, etc.
Data concerning vehicle	This data includes vehicle license number and registration number, type of vehicle, etc.
Data concerning health	Information regarding someone's medical history, health records, medication and prescriptions, disabilities, diagnosis, treatment, hospitalizations, etc.

Data related to criminal convictions	Criminal charges, convictions, certificate of conduct or copy of criminal record (this is sometimes requested by employers), etc.

Table 3 – Data shared when moving for work

2.4.2 Use case: data shared when moving for studies

Category of personal data	Description
Common identifying data	This data includes name, age, date of birth and place, etc.
National identification number	The national identification number will also be on official documents. Other identification numbers may include: social security number, tax identification number, etc.
Contact information	This data includes telephone number, email address (school and/or personal).
Data concerning education	Education level and experience, field of education, diploma type, information related to university/high school of origin, proof of acquired language level, mobility type (semester or short-term), details about study program at the receiving institution, a proof of the gained ECTS, learning agreement (which includes details about the learning outcome), student ID number, etc.
Financial information	This information will be asked when applying for funding (information regarding parent's financial situation, income, etc.). The following information will often be asked when opening a new bank account: bank account number, financial account number, etc.
Official documents	Certificate of birth, residence permit, marriage or tax declaration, official diploma's, identification

	documents (ID-card or passport), Certificate of family composition, rental agreement, etc.
Data concerning family	Family composition, marital status, etc
Data concerning health	Information regarding someone's medical history, health records, medication and prescriptions, disabilities, diagnosis, treatment, hospitalizations, etc.
Data concerning insurances	Social security number, health insurance number, information on the type of insurances.

Table 4 – Data shared when moving for studies

2.4.3 Personal data stored on the ACROSS infrastructure

The personal data items listed above, will as already mentioned, not be stored on the ACROSS infrastructure; ACROSS acts as a pure intermediary that accesses and transfers the data upon request.

However, some personal data items are stored on the platform in order to enable user control and user interaction. These will in most cases not directly identify the citizen, but may identify the citizen when linked to, or combined with, other personal data (e.g. stored by the public administration or private service providers).

Category of personal data	Description
Name of the user	The ACROSS platform will store the (login) name of the citizen user, a credential that will in principle be pseudonymous.
Status of services (submitted, rejected, finished)	A user journey of a citizen will be different for each user, as it depends on the country of origin, the purpose (moving for work or studies) and the country of destination. The updates of the services are different depending on the type of service. ACROSS recognizes two different type of services. • Asynchronous REST Services: the status is automatically updated by the service provider. The citizen can see the status update when logging onto the Citizen Web Application.

	• Synchronous REST Services: the status of the service will be accessible via an output URL, which will redirect the citizen to their application with the service provider. This URL will be stored in the service engine database. Due to the broad concept of personal data in the GDPR, this URL will be considered personal data, even if the Across Platform operator could not identify the citizen by just storing and looking at the link, it is sufficient that, through collaboration with a third party (i.e., the service provider), it would be possible to identify the citizen. Moreover, the URL will be "linked" to the User profile of the citizen, so that also makes it personal data of that user.
Voice recordings	When the citizen user chooses to use the Virtual Assistant, the system will record, store and process the user's voice (audio data, textual input, voice characteristics, etc.).
Comments, reviews, testimonials	Citizens will be able to post comments, reviews and testimonials on the ACROSS platform, which will be linked to their username and will therefore also be considered personal data.

Table 5 – personal data stored on the ACROSS platform

2.5 Supporting assets

Supporting assets are the components of information systems which are used for the processing of personal data (from collection to erasure). The table below will identify those supporting assets and will provide a short description.

Process	Description	Supporting asset
Collection	The Citizens can **register** via an external system (**KeyCloak**) to the ACROSS Personal Data Governance Framework. The system supports the Once-only-principle (OOP), meaning that the user will only need to provide their data for registering to the system once, with their respective national ID providers, allowing them to access other services in the ACROSS platform. It is important to note that personal data will not be stored on the ACROSS platform, but will rather be stored on external personal data wallets or repositories held by public administrations.	• Registration to the ACROSS platform using **KeyCloak**; • **The eIDAS SAML v2.0 IdP Brokering extension** will be used to connect eIDAS nodes, allowing the citizen to authenticate in his/her country of origin. After successful registration on the country of origin's IdP, the citizen will be redirected to Keycloak and will need to create his/her account during the first login.
	VIRTUAL ASSISTANT: the voice recordings will be collected using the audio devices (microphone, speaker or headphones) connected to the user's device (PC, laptop or smartphone), and more specifically, to the web browser used to access the ACROSS web app.	• This works based on normal web technology APIs standardized by the W3C and associated bodies, which have been implemented by browser operators, such as Google Chrome, Microsoft Edge and Mozilla Firefox.
Retention	Official documents, including ID-document, driving license, diploma's, bank account documents, will be retained in **digital wallets**	• **Digital wallets**: as from now the ACROSS platform has not been able to integrate a third party

	provided by public authorities or private entities. The personal data of users will not be stored on the ACROSS platform. When initiating a service on the ACROSS platform, the user will be asked to provide certain personal data to the service provider (some will be marked as mandatory), which he/she will need to provide through fill-in forms.	digital wallet. The personal documents of the citizen user (i.e. driver license, diploma's, etc.) will have to stored on the personal device of the user and can be uploaded using the forms when initiating a service. However, this data will not be stored on the platform, but will solely be transferred to the service providers using secure APIs (see below).
	VIRTUAL ASSITANT: The user's voice data is stored transiently (for at most a few seconds) within the browser (i.e. the user's device). This storage is just for buffering before the data is transmitted to the VA backend, which will be done as soon as technically possible. The temporarily storage is only used when the data cannot be immediately transmitted (e.g. due to short Wi-Fi connectivity dropouts on the user's device).	• **Temporarily storage in user device (browser)** • **Backend VA storage:** ACROSS Kubernetes infrastructure.
Transfer	The ACROSS platform will be able to connect to **public administration service providers** and **private service providers** to support cross border services. Data transfers in the ACROSS Platform between Citizen and Service provider (public administrations and private services) are logged. The event logs can be viewed by the Citizen (via the Transparency Dashboard) and	• Data is accessed using **uniform APIs fp** • **secure data connectors** will allow ACROSS to access proprietary systems of public or private service providers. The data connectors will enable the receiving and sending of

	by the Service Provider (via the Service Catalogue user interface).	data to other proprietary systems. • **Audit loggers** will log all operations executed by the API adapter • Logging of the transfers is done in the ACROSS **Data Governance Framework** (event logs) and in **the data connectors dashboard**;
	VIRTUAL ASSISTANT: the user's voice data is transmitted from the user's web browser to the FDM (FISA Dialog Manager).	• Transfer through a secure websocket connection (i.e. a state-of-the-art end-to-end encrypted channel adhering to all relevant W3C standards).
Destruction/ erasure	Data erasure in the **ACROSS Platform** is supported.	
	VIRTUAL ASSISTANT: the user's voice is processed by an automatic speech recognition service immediately when it arrives at the FDM backend. After this processing, the audio data will be destroyed.	

Table 6 – supporting assets

3 Appreciative analysis

3.1 Fundamental data protection principles analysis

The fundamental principles of the GDPR have been described in detail in **D3.6 Legal Requirements**. The table below will assess the current compliance status of these fundamental principles in the ACROSS platform.

Check point	Description	Status?
Purpose definition	The purposes are clearly defined in the ACROSS platform in two ways: • The citizen user of the platform will be informed about the purpose of the processing of personal data by the operator of the Platform in **the privacy policy** which is accessible on the Platform and which is provided to the User before registering. • The citizen will be able to consult information on the purposes for the processing of their data by the service providers in the **Transparency Dashboard** and in **the service description.**	Implemented
Legal basis for processing	• For the **ACROSS platform operator**, **consent** (Article 6.1 a) GDPR) will be the main legal basis for operating the platform and for sharing user data with specific service providers (at least when the platform is an independent service). Some processing operations on the platform may also be performed on the basis of a separate legal basis, such as the processing of meta-data of the citizen using the platform to determine the user-friendliness and functionality of the platform, which will be based on the **legitimate interest** of the platform operator (Article 6.1 f) GDPR). • It is important to mention that the citizen's data is not held by ACROSS itself, but rather that the ACROSS architecture is implemented as a range of modules or tools that are integrated by existing data holders. In that case, the data holders still act as data controllers, but another legal basis for holding and processing their data would apply, such as notably a specific legislation (at the EU or national level) that obliges an organisation to run such a platform. This is however out of the scope of this DPIA. • For the **service providers**, the legal basis will generally also be **consent** (Article 6.1 a) GDPR) for the transfer of the citizen's data from the platform to their own systems. After receiving the data, a completely new legal basis could apply,	Fully implemented; but only partially verifiable (see third party data subjects)

	e.g. for public sector service providers, the legal basis may also be that they have a legal mandate under national legislation to provide a public service. In that case their legal basis will be the necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6.1 e) GDPR). For private sector service providers, their legal basis for the further processing of the data will mainly be consent, but they may also rely on 'performance of a contract' to which the data subject is party (Article 6.1 b) GDPR), e.g. in the situation of a rental agency, when they would process data and/or documents to conclude a rental agreement with a citizen. In this case, the data processing must be necessary to conclude the agreement with the data subject. Again, this is processing activity outside the eIDAS context, and thus out of scope of this DPIA. • The **voice recordings** can take place based on the explicit consent of the citizen user. When the user logs in to the ACROSS platform for the first time and attempts to use voice assistance, they will be asked to provide their consent for the access by ACROSS to their microphone by a pop-up in their browser. Even after this initial consent to access their device microphone, the user will need to actively switch on their microphone before being able to use the ACROSS virtual assistant (to insert voice input into the ACROSS virtual assistant). The user is free to choose this service or not; the consent satisfies the requirements of the GDPR. • The data processing of any **third party data subjects** as identified under 2.2.2 (e.g. the children or spouse of an ACROSS user, whose information could also be mentioned in exchanged information) cannot be based on their consent (as they will not be using the platform themselves, and may not even have any knowledge that their data is shared via the	

	ACROSS platform). The processing of their data will be based on: ○ For private service providers: their legitimate interest to provide the services. Details about family members and other people may be required to provide the service in an appropriate way. ○ For public service providers: the performance of a task carried out in the public interest or in the exercise of official authority vested in them. The citizen end-users are informed about the legal basis of the platform operator in the privacy policy on the platform. However, the other data subjects i.e. the third parties about whom the citizen may share data on the platform, are not clearly informed as they are not using the platform themselves. The legal risk can be reduced by explicitly requesting that citizen users notify any third party data subjects beforehand; while this does not create a consent as such for those third party data subjects, it does create transparency towards them that strengthens notably the appeal to a legitimate interest justification. This is presently not yet implemented. With regards to the information about the legal basis of the service providers, this information will also be provided in the platform in the transparency dashboard, under the component 'available services' where they can find more information on the legal basis for that specific processing activity by the service provider.	
Purpose limitation	The platform operator should only use the data for the purposes to which the citizen explicitly consented. Furthermore, the data should not be processed in a manner that is incompatible with the initial purpose. For the platform operator, this includes a prohibition on tracking, profiling, data selling or trading, surveillance, or direct marketing – except where a user consented to these processing activities.	Implemented

	With regards to the data processing by service providers, the platform operator cannot fully control what the service provider might do with the data when they receive it through the platform. The contractual approach between the ACROSS platform and the service providers, and between the service provider and the end user, does mitigate this risk significantly. The ACROSS platform takes an extra step in this regard by also enforcing a code of conduct which specifically obliges the 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.	
Transparency	The principle of transparency means that the controller (i.e. both the platform operator and the service provider) has an obligation to inform data subjects about which personal data they collect and the purpose of this data collection. The ACROSS platform is designed with the transparency principle in mind. The **transparency dashboard** enables the citizen to control the usage of their data by service providers and to manage their consents (grant, withdraw, etc.). The users are also informed about the purpose, legal basis and the personal data needed for a service through the service description in the service catalogue. Moreover, citizens are informed about their personal data processing via the **privacy policy** on the ACROSS platform. Which provides information on the personal data, purposes, retention periods, security measures, data subject rights, etc.	Implemented
Data minimization	The principle of data minimization means that the data should be adequate, relevant and limited to what is necessary in relation to the purpose. With regards to the data sharing with the Service Providers, the Operator of the ACROSS platform should maintain a clear oversight of the data that is asked by the service provider to deliver the services. This is ensured by providing a **template Service Description**	Implemented

	Data Model for the Service provider which must be used to create new services in the platform. Service providers must also clearly define within the service description model which data is mandatory for the provision of the service, and which data is optional. Next, when registering new service providers they also must adhere to the aforementioned **code of conduct**, which attaches great importance to the principle of data minimization, and requires service providers to define their data requests in accordance with their actual minimal need.	
Data accuracy	The principle of data accuracy means that a controller must have processes and procedures in place to ensure that the personal data is accurate and kept up to date. In ACROSS, this principle is implemented in a reasonable manner: the information is in principle not stored on the platform itself, but obtained via external sources, which are presumed to be authoritative. In some instances (such as the eIDAS nodes), the authenticity of this information has a clear legal basis; in other cases it will not. Accuracy is however universally strengthened through transparency, in the sense that the user can identify which data sources are used, which data is obtained from them, and which data is shared. The user has the ability (and duty, on the basis of the terms of use) to verify that this information is accurate before sharing it with service providers. Accuracy is thus appropriately embedded in the infrastructure.	Implemented
Storage limitation	The principle of storage limitation means that a controller must ensure that personal data is kept no longer than necessary for the purposes for which the personal data is processed. Within the ACROSS platform itself, this principle is technically enforced, since data is obtained from third party sources, shared with service providers, and then deleted as soon as technically feasible. Substantive data is thus not stored (excepting of course	Implemented

	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 be legally required to retain data under nationally applicable law, e.g. by entering it 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 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.	

Table 7 – Fundamental principles controls

3.2 Data subject rights analysis

Under the GDPR, data subjects receive certain data subject rights which they can exercise against data controllers processing their personal data. The table below will provide a short description of the different data subject rights and will assess the status of compliance by the ACROSS platform in ensuring the facilitation of those data subject rights.

Check point	Description	Status?
Transparency	See information provided in table 6 – Transparency.	
Right to revoke consent	The GDPR requires that the consent of the data subject is revokable (Article 7.3 of the GDPR). This means in essence that the citizen should be able to choose to stop using the ACROSS platform, and to stop any additional data sharing with service providers, since both of these are based on the consent of the citizen, as described under 3.1. The **consent management module** 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 authorities and private actors is immediately ceased. Note that in this case, the ACROSS platform operator will not require the third party who has received your 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 is accessible in the ACROSS Platform to directly contact the DPO of the service provider. It goes without saying that users can also always opt to stop using the ACROSS platform altogether, removing the legal basis for processing via the ACROSS platform, and resulting in data deletion	Implemented

	of any personal data stored on the platform (which is designed to be minimal, as explained elsewhere).	
Right of access	The right of access means that the data subject should be able to obtain information about his/her data that are being processed by the controller and that he/she can receive a copy of the personal data undergoing processing. As discussed above, ACROSS is an intermediate service that enables data sharing with third party service providers, and therefore does not store any substantive personal data on the platform (other than account information). ACROSS does enforce the data subject rights of the citizen users by providing e-mail links to the DPO of the relevant service providers. The citizen can use the link to request access to his/her data held by that service provider. By using the ACROSS platform the citizen will also know which data will be processed by each service provider.	Implemented
Right of rectification	When exercising his/her right to rectification, a data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. The citizen can use the e-mail link provided on the ACROSS platform to request a rectification of his/her personal data directly to the service provider. Additionally, the ACROSS platform in principle will use third parties to provide the users' data (rather than storing it itself). Rectification of data at the source is thus also possible (and preferable), although this cannot be effected via the ACROSS platform, and rectifications of data at the source will only affect service providers after the data is requested anew (which is an additional reason why service providers should rely on live requests of personal data, rather than storing data locally – live access ensures that the data is as correct as possible).	Implemented
Right to erasure	The right to erasure means that the data subject has the right to obtain an erasure of his/her personal data without undue delay in	Implemented

	certain circumstances. E.g. when a citizen would withdraw its consent for the processing of his/her personal data by the service provider and that service provider does not have another lawful ground to further process the data, the data should be erased. The citizen can use the e-mail link provided on the ACROSS platform to request an erasure of his/her personal data directly to the service provider. The outcome of this process is not guaranteed, since the service provider may have a legal duty to retain the data (e.g. in case of public sector service providers that are legally required to maintain official records). This is in line however with the GDPR.	
Right to restriction of processing	The right to restriction of processing means that the data subject shall have the right to obtain from the controller restriction of processing in certain circumstances. The citizen can use the e-mail link provided on the ACROSS platform to request a restriction of the processing of his/her personal data. Moreover of course, the consent management dashboard inherently allows the user to restrict processing, at least in the sense that the service provider will no longer be capable of retrieving new personal data.	Implemented
Right to object	The GDPR provides the data subject with a right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her, when the processing is based on legitimate interest or public interest. The citizen can use the e-mail link provided on the ACROSS platform to object to the processing of his/her personal data. Again, the consent management dashboard inherently allows the user to object to processing by withdrawing their consent to data sharing.	Implemented

Right to data portability	In case the processing is based on the consent of the data subject or on a contract concluded with that data subject, the data subject can request to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit that data to another controller. The citizen can exercise his/her right to data portability directly against the service provider by using the e-mail link.	Implemented
Right to not be subject to automated decision making	N/A – no automated decision making occurs, or is enabled via ACROSS.	N/A

Table 8 – data subject rights controls

3.3 Technical security controls

The technical security controls have been derived from the information provided in D.5.4 Platform Prototype and Applications and D.5.2 System Architecture and Implementation.

Check point	Description	Status?
Encryption	• All components support **SSL/TLS 1.0 (and up)** for a secured communication; • The user's voice data is transmitted through a secure websocket connection (end-to-end encrypted channel). • All service providers users of the platform must support **https.** • The information about an authenticated citizen or system will be transferred through a **generated bearer token**. The bearer token will include an Object in **JSON-format encoded as JWT (JSON Web Token).** All service providers must be able to decode this token.	Implemented
Anonymization / pseudonymization	N/A (The core functionality of ACROSS is to disclose personal data of the user, conditional upon their consent).	N/A
Partitioning	• Data is stored on different databases	Implemented
Logical access control	• For citizens and service providers users using the ACROSS platform, **Keycloak identity management server** will be deployed for authentication and authorization. This allows the user to authenticate for using a national service by using their country's eIDAS node. • The ACROSS Platform provides a **identity and access management (IAM) component**, this module will provide authentication against the eIDAS node for citizen and will authorize the citizen to use the	Implemented

	services provided by public administrations or private service providers. • A **data access control component** ensures authorization enforcement restricting unauthorized access to data resources, by relying on Role Based models. Within the Kubernetes cluster, Role-Based Access Control (RBAC) is deployed that defines and assigns roles to users, thus minimizing the risk of unauthorized access and ensuring a principle of least privilege.	
Traceability	• **Audit logs** are in place to track the data usage, exchange and the restrictions. The component will work either with event-based (centralized) or flow-interception (distributed) way of logging. The logged events will be timestamped. • The logged events can be viewed by both the Data Subject (via the transparency dashboard – event log window: this shows the statistics to the end user of how work flows they have initiated) and by the Service provider (via the Service Catalogue user interface).	Implemented
Data integrity	• Through ACROSS, personal data is carried via a secure connection from the data source to the service provider; tampering is thus not possible (unless the ACROSS platform is compromised in a manner that allows the data to be corrupted during transit – abusing ACROSS to conduct a man-in-the-middle attack)	Implemented
Archiving	N/A – ACROSS is not intended to archive any personal data; this would contradict the data minimisation principle.	N/A
Paper document security	N/A – no paper documents involved	N/A

Operating security	• The operational environment of the ACROSS ecosystem is set up in a dedicated Kubernetes cluster v.1.21.9. • The cluster is hosted on Digital Ocean and consists of 3 Linux server nodes that act as cluster workers. • Each cluster node consists of 4 VCPUs and 8 GB of RAM. • Nginx-ingress, wildcard domain and cert manager have been configurated to enable external encrypted access. • A network file storage servicer has been configured to act as a persistent volume storage.	Implemented
Anti-malware	• The Kubernetes Nodes operate on the latest version of Ubuntu Server, benefitting from the latest features, optimizations and security updates. • To enhance network security, we have implemented a UFW firewall, meticulously configured to block all ports except the one designated for the ingress service, reducing the attack surface. Each service is encapsulated within a pod, leveraging the inherent security benefits of containerization through isolation. • As part of our commitment to maintaining secure container images, we employ vulnerability scanning tools provided by DockerHub to thoroughly assess and mitigate potential risks associated with our Docker images	Implemented
Workstation management	N/A – no workstations involved that interact with personal data	N/A
Website security	• **SSL/TLS 1.0 (and up)** for a secured communication; • All service providers users of the platform must support **https.**	Implemented

Backups	• No backups are performed at deployment level, backups are performed at deployment level (in Kubernetes). • Weekly backups of data are performed and stored on cloud storage provided by digital ocean.	Implemented
Maintenance	• Maintained by security testing (all components) and all components are compatible with OWASP top 10 standards. • Automated tools are used to scan for known vulnerabilities within the Kubernetes nodes.	Implemented
Network security and monitoring	• Grafana and Prometheus instance is deployed to monitor the performance of each ACROSS component and to report incidents. • Security posture in Kubernetes includes the proactive monitoring of network activities and resource usage, allowing us to promptly detect and respond to any potential security treats.	Implemented
Physical access controls	N/A	N/A
Physical distancing from risk sources	N/A	N/A

Table 9 – technical security measures controls

3.4 Organizational security controls

Check point	Description	Status?
Data processing agreements	As there will be no collection of real user data during the development of the ACROSS platform, it is not yet necessary to conclude any data processing agreements between the platform operator and the identified processors (such as Keycloak). The data processing agreements must contain the elements as required by Article 28 of the GDPR.	N.A.

Data transfer arrangement with third parties	As there will be no collection of real user data during the development of the ACROSS platform, it is not yet necessary to conclude any data transfer arrangements with third parties (such as private and public service providers).	N.A.
Intra-group arrangements	Data sharing within the context of the project is arranged in the Consortium agreement.	Implemented
Description of roles related to data protection	A Data Protection Officer (DPO) has been appointed for the duration of the project. If the ACROSS platform would be used after the project, the operator of the platform would need to appoint a DPO (if they have not yet appointed one).	Implemented
General data protection policy	There is a general privacy policy for the ACROSS platform.	Implemented
General risk management	Service providers wanting to use the ACROSS platform will need to adhere to a code of conduct, this is done to ensure a level of compliance from the service providers with regards to data protection and security.	Implemented
Information security policy	There is no general information security policy for the ACROSS platform.	Not implemented
Testing of security measures	• Vulnerability testing tools provided by DockerHub are used to thoroughly assess and mitigate potential risks associated with our Docker images; • security posture includes the proactive monitoring of network activities and resource usage, allowing us to promptly detect and respond to any potential security threats.	Implemented
Incident response and data breach procedure	There is a data breach procedure in place via the Code of Conduct.	Implemented
Staff management	Each partner in the ACROSS project bears its own responsibility for the training of its employees in data protection and cyber security.	Implemented

Table 10 – Organizational security measures controls

4 Risk assessment and their mitigating measures

Supervisory authorities typically recognize three main types of risks:

- Illegal access to personal data;
- Unauthorized modification of data;
- Loss of data;

Each of these main types of risks will be analysed for the ACROSS platform. It should be stressed that the risk assessment is forward looking – i.e. it assesses the risk under a scenario where actual personal data would be processed (as opposed to the personas actually used during the project, which by definition pose no actual risk).

The source of the risks can be either **internal** (e.g. a staff member) or **external** (e.g. a third-party attacker). Furthermore, the risk can come from an accidental or a deliberate action of such an internal or external actor. In the table below each threat is described for each type of risk, taking into account the possible risk sources.

For each threat the relevant check points as described above are listed. Depending on the status of the check point, each threat can then be scored using the scoring mechanism described above.

4.1 Illegal access to personal data

Risk source	Threat description	Mitigating measures	Scoring
Internal, accidental	The platform operator could accidentally grant access to the wrong service provider.	• Consent management platform • Audit logs • Access controls	This risk is highly unlikely as the citizen user is fully in control of the data sharing. The platform operator cannot grant access without the consent of the user.
Internal deliberate	The platform operator uses the data provided by the citizen through the ACROSS platform for different purposes than those that were communicated to the data subject.	• Purpose limitation • Transparency (dashboard) • Privacy policy • Audit logs	The scoring of this risk will depend on the reliability of the platform operator.
External, accidental	A service provider using the ACROSS platform could unintentionally disclose the personal data it receives through the ACROSS platform to unauthorized third parties.	• Access controls • Code of conduct • Audit logs	It is difficult to fully control the processing of personal data by the service providers using the ACROSS platform. ACROSS has measures in place to ensure that only trusted third parties are able to use the platform.
External, deliberate	A service provider could maliciously use the personal data illegally e.g. by selling it to other unauthorized third parties.	• Code of conduct	It is difficult to fully control the processing of personal data by the service providers using the ACROSS platform. However, ACROSS has implemented additional measures to limit misuse.
	There is a risk of identity fraud, meaning a hacker could hack the eID of a citizen user and access confidential information.	• Access controls • Audit logs • Encryption	The risk is mitigated by using secure user authentication logins. The Keycloak system also has fraud and anomalies detection feature (device recognition and attempts recognition).

			This risk is also mitigated by the fact that the ACROSS platform does not hold the data itself. The hacker could potentially access the status of the citizen's request for services by accessing the URL (for Asynchronous REST services).

Table 11 – Illegal access to personal data

4.2 Unauthorized modification of personal data

Risk source	Threat description	Mitigating measures	Scoring
Internal, accidental	Due to a configuration issue the personal wallets of users get mixed-up.	• Identification and authentication • Access control • Audit logs • Network security	The occurrence of this risk is very unlikely, however if the risk would materialize, the severity would be enormous (as the data shared through the ACROSS platform is highly personal).
Internal, deliberate	The ACROSS platform operator uses the platform to create a man-in-the-middle attack, modifying the user's personal data during the transfer from source to service provider.	• Audit logs • Network security	The occurrence of this risk is unlikely, however if the risk would materialize, the severity would be enormous (as the data shared through the ACROSS platform is highly personal).
External, accidental	Due to an ill-configuration or updates of the ACROSS platform the user journeys could get mixed up, i.e. a citizen user could end up seeing a user journey from someone else.	• Audit logs • Backups	Although the risk of occurrence is mitigated due to the implemented security measures, the risk severity would be high as a user journey can reveal sensitive information about a citizen (namely that they are moving for work or studies to a specific other country).

External, deliberate	A hacker could change statuses in user journeys or grant consent to data sharing.	• Access control • Identification and authentication • Audit logs	The occurrence of the risk is mitigated due to the secure identity management system (Keycloak). However, in the unlikely event that the risk would occur, the damage would be severe as the citizen could get the impression that his/her application is approved or denied.

Table 12 – unauthorized modification of personal data

4.3 Loss of personal data

Risk source	Threat description	Mitigating measures	Scoring
Internal, accidental	Due to ill configuration of the platform, data shared through the platform gets lost.	• Network security	The risk is low because the data is not stored on the platform. When data would get lost in transmission, the data can still be found in personal wallet or PA databases.
Internal, deliberate	Since only account data is stored on the platform, only that data could be lost.	• General security measures of the platform	No significant risk; accounts can be recreated at will, and no substantive data can be lost.
External, accidental	Errors could occur during updates, configuration or maintenance of the ACROSS Platform which could lead to user journeys getting lost.	• Audit logs • Backups	Risk occurrence and severity is low as no personal data would get lost. The citizen would however lose the overview on the status of his/her applications for different services, which would interfere with the purpose of easing the administrative burden for cross-border services.
External, deliberate	A hacker could deliberately remove users journeys from the ACROSS platform.	• Audit logs • backups	Risk occurrence and severity is low as no personal data would get lost. The citizen would however lose the overview on the status of his/her

			applications for different services, which would interfere with the purpose of easing the administrative burden for cross-border services.

Table 13 – loss of personal data

5 Action points

The analysis above shows that the platform is already in a satisfactory state of compliance (even with a forward looking perspective, i.e. under the assumption that it would be used for real-life personal data, rather than personas). None the less, several action points can be identified; these will be followed up during the closing months of the project.

5.1 High priority

- Declarations of adherence to the Code of Conduct during the onboarding of Service Providers should be enabled.
- The documentary gaps in section 3.3 above (Technical security controls) should be addressed, notably with respect to logging, anti-malware, back-ups and maintenance. Note that this is likely an information gap only; there is no indication of a substantive problem at this time.
- The risk of an internal attack against the integrity of personal data should be assessed and (if needed) addressed, i.e. the possibility of someone within the ACROSS platform capturing and modifying personal data before sharing it with a service provider.

5.2 Medium priority

- While the trustworthiness of the service provider is strengthened by the Code of Conduct, it should be assessed whether/how the trustworthiness of third party data sources can be ensured. For official data sources (such as the eIDAS nodes), this is not necessary since they have an established legal value; but there are no generic rules for non-official data sources.

5.3 Low priority

- The documentary gaps in section 3.4 above (Organizational security controls) should be addressed, notably with respect to testing of security measures, and incident response mechanisms. Note that this is likely an information gap only; there is no indication of a substantive problem at this time.

Update on the action point in April 2024:

The documentary gaps that have been identified in this DPIA have been updated in the table, no action points related to the technical and organisational measures that had been identified are still present.