D1.5 Data management plan

Document Identification			
Status	Final	**Due Date**	30/06/2021
Version	1.0	**Submission Date**	30/06/2021

Related WP	WP1	**Document Reference**	D1.5
Related Deliverable(s)	-	**Dissemination Level (*)**	(PU) Public
Lead Participant	UPAT	**Lead Author**	George Domalis
Contributors	IMM, ENU, UNI GR, S5	**Reviewers**	FOKUS, TGS

Keywords:
Data management; List of Datasets; Types of data; FAIR; Data Sharing Policy; Data storing & Preservation; Data Security

Document Information

List of Contributors	
Name	Partner
George Domalis	University of Patras
Dimitris Tsakalidis	University of Patras
Nikos Karacapilidis	University of Patras
Dimitrios Tsolis	University of Patras
Anna Zoakou	Unisystems SA
Muhammet Veysel Beytur	Istanbul Metropolitan Municipality
Nikolaos Pitropakis	Edinburgh Napier University
Konstantinos Latanis	Suite 5 Data Intelligence Solutions Limited

Document History			
Version	Date	Change editors	Changes
0.1	22/02/2021	George Domalis (UPAT)	Initial version of document
0.1	01/05/2021	George Domalis; Dimitris Tsakalidis (UPAT)	First draft
0.2	15/05/2021	Nikos Karacapilidis; Dimitris Tsakalidis; Dimitrios Tsolis (UPAT)	First Draft Amended and Reviewed by UPAT members
0.3	26/05/2021	George Domalis (UPAT)	Second Draft
0.3	28/5/2021	Muhammet Veysel Beytur (IMM)	Review
0.3	28/5/2021	Nikos Pitropakis (ENU)	Review
0.3	4/6/2021	Anna Zoakou (Unis Gr)	Review with focused suggestions and comments
0.3	4/6/2021	Konstantinos Latanis (S5)	Review
0.4	7/6/2021	George Domalis (UPAT)	Third version of the first document based on the consortium review
0.5	14/06/2021	Anna Zoakou (Unis Gr)	Review of the document and update of Annex II
0.6	15/06/2021	George Domalis (UPAT)	Update of the document according to the comments provided
0.61	21/6/2021	Aslihan Kagnici (TGS)	Internal Review
0.62	21/6/2021	Fabian Kirstein (FOKUS)	Internal Review
0.7	22/6/2021	George Domalis (UPAT)	Comments from internal reviewers addressed and release

List of Contributors			
			of the deliverable
1.0	30 / 6/ 2021	Anna Zoakou (Unis Gr)	Final Check and Release
Quality Control			
Role		Name (Partner short name)	Approval Date
Deliverable leader		George Domalis (UPAT)	20. 06. 2021
Quality manager		Anna Zoakou (Unis Gr)	30. 06. 2021
Project Coordinator		Ilias Kontakos (Unis Gr)	30. 06. 2021

Table of Contents

List of Tables

List of Acronyms

Abbreviation / acronym	Description
API	Application Programming Interface
CA	Consortium Agreement
DMP	Data Management Plan
DMS	Data Management Strategy
DoA	Description of Action
DOs	Dissemination Objectives
Dx.y	Deliverable number y, belonging to WP number x
EAB	External Advisory Board
EC	European Commission
FAIR	Findable - Accessible - Interoperable - Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation 2016/679
IPR	Intellectual Property Rights
KPI	Key Performance Indicator
Mx	Month X
NDA	Non-Disclosure Agreement
ORDP	Open Research Data Pilot
PC	Project Coordinator
PM	Person-month
QA	Quality Assurance
QM	Quality Manager
RASCI	Responsible/Accountable/Supportive/Consulted/Informed
RP	Reporting Period
TL	Task Leader
UC	Use Case
WP	Work Package
WPL	Work Package Leader
YRx	Year X

Project Beneficiaries

No	Name	Short name	Country
1	UNI SYSTEMS SYSTIMATA PLIROFORIKIS MONOPROSOPIANONYMI EMPORIKI ETAIRIA	UNIS GR	Greece
2	FRAUNHOFER GESELLSCHAFT ZURFOERDERUNG DER ANGEWANDTENFORSCHUNG E.V.	FOKUS	Germany
3	EDINBURGH NAPIER UNIVERSITY	ENU	United Kingdom
4	PANEPISTIMIO PATRON	UPAT	Greece
5	UBITECH LIMITED	UBI	Cyprus
6	SUITE5 DATA INTELLIGENCESOLUTIONS LIMITED	S5	Cyprus
7	EUROPEAN ELECTRONIC MESSAGINGASSOCIATION AISBL	EEMA	Belgium
8	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAOFORMACAO E CONSULTADORIALDA	PDM	Portugal
9	TEKNOLOJI ARASTIRMA GELISTIRMEENDUSTRIYEL URUNLER BILISIM TEKNOLOJILERI SANAYI VE TICARET ANONIM TICARET	TGS	Turkey
10	Istanbul Metropolitan Municipality	IMM	Turkey
11	MINISTRY OF DIGITAL GOVERNANCE	MoDG	Greece
12	Ministério da Justiça	MoJ	Portugal
13	UNISYSTEMS LUXEMBOURG SARL	UNI	Luxembourg

1 Executive Summary

This deliverable introduces the initial data management action plan (DMP) and provides a general outline of the project policy for data management. GLASS DMP identifies the data types that will be used, collected and/or generated, and frames the overall guidelines regarding data collected and generated throughout the project implementation.

The DMP will describe the format and support the data management life cycle of all the data collected and generated following the FAIR (Findable, Accessible, Interoperable, Reusable) Data Principles, as defined in the "Guidelines to the Rules on Open Access to Scientific Publications [1] and Open Access to Research Data in Horizon 2020 [2]" and in the "Guidelines on FAIR Data Management in Horizon 2020 [3]". This document will present the methodology and standards to be followed, in cases where data will be shared and/or made open, and how it will be curated and stored.

The Data Management Strategy (DMS) identifies and classifies respectively the data generated and collected, along with their metadata to be used. Also, this document reports on the exploitation and availability of the aforementioned data/metadata, the required ethical and legal compliance issues, and the responsibilities in the implementation of the DMP.

The DMP is a living document that will be updated when important changes to the project occur, due to the inclusion of new data sets, changes in Consortium policies or any other external factors. At least two (2) updated versions are expected during the project lifetime; one in month 24 and the final one in month 36.

The next version of the GLASS DMP will emphasize on the definition of procedures to be implemented by the project to efficiently manage its research data in terms of storage and backup (backup provision, recovery procedure), selection and preservation (which data will be retained/shared/ preserved, length of time that data have to be preserved and preservation preparation time).

2 Introduction

This deliverable constitutes the first version of the DMP document of the GLASS project. It provides the baseline of the policy that will be followed by the GLASS consortium with respect to the data management related activities and covers the following aspects:

- What types of data will be collected and/or generated (Section 2.4)?
- What standards will be used (Section 2.4.1)?
- How will this data be exploited, shared, processed and made accessible (Section 3)?
- How will this data be curated, stored and preserved (Section 5)?
- Which tools and methodologies will be used to store this data and for how long (Section 3)?
- How are data restriction levels managed (Section 5)?
- What is the structure of the consent forms (Annex 1)?

This DMP outlines how research data, either **synthetic** or **real**, will be handled throughout the life cycle of the project, as well as after its completion, contributing to the following issues:

- Ensuring that project research data and records are accurate, complete, authentic, interoperable and reliable.
- Saving time and resources in the long run.
- Enhancing data security and thereby minimizing the risk of data loss.
- Ensuring research integrity and reproducibility by others.
- Preventing duplication of effort by enabling others to use the GLASS project's data.

Synthetic data refers to information that's artificially manufactured rather than generated by real-world events. Synthetic data can be created algorithmically, and it is used mostly for evaluation purposes as testing dataset of production or operational data towards validating and train machine learning models.

The described policy herein reflects the current state of consortium agreements regarding data management and is in accordance with those referring to exploitation and protection of results. It is a living document that is expected to mature during the project lifetime and will be updated accordingly.

2.1 Definitions

Open Access Data: Open access refers to unrestricted access to research results. Commonly, the open access characterization is given to open-source peer-reviewed publications, datasets, tools and source code. Open access focuses on building a community and enables scientists, researchers, individuals and enthusiasts to:

- Build and enhance existing research results.
- Avoid redundancy.
- Participate in Open Innovation activities.
- Get in contact with high-ranking results of the GLASS project.

Open Research Data: Open research data refers to the disclosure of the linked research data which are needed to assess, validate and replicate the results presented in research publications. Complementary to the concept of open access, open research data enables the online availability of data resources towards promoting research.

The open research data concept focuses on enabling researchers and individuals to:

- understand, assess, reconstruct and further expand scientific publications;
- build innovative concepts on top of existing research data;
- establish a continuous improvement mechanism of research.

2.2 Approach

The general strategy for data management, according to the Guidelines on Data Management in Horizon 2020 [3] will be based on the identification and classification of data generated and collected, standards and metadata to be used, exploitation and availability of data, data sharing and archiving, the preservation of the information, as well as on the ethical and legal compliance and the responsibilities in the implementation of the DMP.

Each participating organization will examine whether open access can be granted without affecting any legal and ethical requirements, including the Intellectual Property Rights as per the dissemination access level of each dataset produced (Annex 2).

Such information consists of:

- A general data summary, including origin, types and formats of files, purpose, size, and utility;
- FAIR Data:
    - **Findable:** discoverability, naming convention, search keywords, version numbers, metadata;
    - **Accessible:** availability, software tools, repositories, restriction and/or conditions for access;
    - **Interoperable:** description of interoperability, metadata vocabularies, standards and/or methodologies;
    - **Re-Usable:** license, data quality, time frames for availability and storage.
- Allocation of resources (by Consortium agreement, each partner has to individually identify and allocate resources for data storage and management);
- Data security;
- Ethical aspects, with reference to the dedicated deliverables of WP9, if needed;
- Other issues.

Towards formulating an effective DMP, and ensuring to effectively keeping track of the varieties of data generated and/or collected by the project, it is of significant importance to categorize the datasets according to their form, source and type. For this reason, the GLASS partnership classifies the numerous data collections according to their origins and purpose, as described in detail below. An initial breakdown of the project datasets in five (5) categories is as follows:

- **Dataset Category 1:** Consortium Information
- **Dataset Category 2:** Project files
- **Dataset Category 3:** Research activities
- **Dataset Category 4:** Development data, packages and source code
- **Dataset Category 5:** Demonstration activities

2.3 List of Datasets

The data that will be collected, extracted and generated throughout the activities of the GLASS project are classified in five (5) datasets, as follows:

Dataset Category 1 - Consortium Information (A): This dataset category includes personal and sensitive information of the consortium partners, such as emails and online accounts. This information will be treated with confidentiality and only for internal communication for the purposes of the project.

All the information will be stored in a private and secure storage area (NextCloud [4]). Access will be restricted only to the members of the consortium and the External Advisory Board (EAB) members, which are also considered as members of the GLASS partnership.

Dataset Category 2 - Project files (B): It includes all the gathered information from internal plenary, technical and review meetings as well as workshops. It will be securely stored within the private cloud area (NextCloud) and will be only restricted to consortium members.

The project outcomes that do not contain any personal or sensitive information will be publicly disseminated through the relevant channels of the project (social media, website, etc.).

Confidential outcomes along with any linked files and documents will be encrypted and stored in the internal cloud area of the project (NextCloud). The encrypted data will only be accessible by the data owners and specific consortium partners. For example, in a meeting between a public authority (e.g., a Ministry) and a technical partner that outlines the interoperability requirements, if confidentiality is required, any relevant outcome (documentation, report, etc.) will be restricted only to authorized consortium members that will be able to participate.

Dataset Category 3 - Research activities (C): It refers to the project's research related outputs such as deliverables, white papers, publications, etc. This dataset category will adopt an open access approach. State-of-the-art methods will be utilized, if and where necessary, to carry out the project's research and development activities. In specific research tasks that involve sensitive information (personal data, confidential information from public authorities, etc.), all relevant documentation, files and any other type of source will be stored and protected locally by the corresponding organization.

If any material related to the project needs to be shared, proper anonymisation and encryption tools will ensure the integrity of personal and sensitive information. These procedures will comply with the ethics deliverables, reported in D9.1, D9.3, D9.4.

Dataset Category 4 - Development data, packages and source code (D): This dataset category concerns data generated throughout the life cycle of the project's implementation process, from research prototypes to development codes and deployment scripts. The aforementioned material will be stored and preserved in a private repository of version control tools, such as GitHub [5] or GitLab [6]. Backup versions of each module will be extracted periodically and stored in the NextCloud platform.

Dataset Category 5 - Demonstration activities (E): It includes the data generated in the pilot activities of the three (3) project demonstrators including data generated and collected from stakeholder workshops and trainings (WP2, WP8). All the synthetic information, evidence, data and metadata that will be produced along with the processes data will be managed and preserved locally by each organization. Other types of data, as well as users and participants that might be considered during the project lifetime, as set and updated by the user/ system requirements, will be included in the second version of this deliverable.

2.4 Data types and format

2.4.1 Types of data

- **No personal data:** such as information which is not affected by Data Protection legislation.
- **Personal data:** Information that is clearly about a particular person such as email address, telephone number, passwords, etc.
- **Sensitive information:** A specific set of "special categories" information that must be treated with extra security. This includes information pertaining to:
    - Racial or ethnic origin;
    - Political opinions;
    - Religious or philosophical beliefs;
    - Trade union membership;
    - Genetic data; and
    - Biometric data (where processed to uniquely identify someone).

According to EU directives, personal/ sensitive information refers to the information that might lead to the identification of an individual, either:

a) directly from this data, or
b) indirectly, through information that is in the possession, or is likely to come into the possession, of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Since GLASS follows the European directives, any personal data that might be included in the research and the implementation activities will be anonymised, according to the Community's guidelines, to ensure that no ethical or privacy issues with either the EU or any National legislation arise. Such activities are carried out as part of WP7 and WP9, namely demonstrators' activities and ethics requirements, respectively.

In the project's demonstration and pilot activities, along with the workshops and stakeholders' engagement activities planned to be carried out (WP2, WP8), each participant, including members of GLASS consortium, will be informed prior to the data collection process. In particular, to ensure the application of the ethics principles and avoid any ethics related implications, all participants will be invited to sign a consent form[1].

Synthetic data: Data that will simulate individuals' personal and sensitive information, according to the EU definitions [7]. Synthetic datasets will include a set of actions that will be applied to design, synthesise and extract data that simulates individuals' personal/sensitive information. To ensure a high-quality simulation of personal and sensitive information, all the generated datasets within GLASS will be handled as personal/sensitive information.

[1] The generic template of GLASS informed consent is available in Annex 1.

2.4.2 Data formats

The aforementioned identified datasets can include different data formats. A manually gathered dataset concerning impact assessment and user acceptance of the demonstrators can consist of interview notes, pictures from pilot sites, as well as questionnaires' responses. Both the collected and generated data will be delivered anonymous as open research data. GLASS will use widely accepted data formats, such as:

Documents/Reports/Publications (.PDF/A, .txt, .doc/.docx): A TXT file is a standard text document that contains unformatted, plain text. It is recognized by any text editing or word processing program such as Microsoft Notepad or Apple TextEdit. TXT files are encoded in numerous non-proprietary encodings such as ASCII and UTF-8.

JavaScript Object Notation (.json): JavaScript Object Notation is a lightweight data interchange format. JSON files store simple data structures in an organized and easy-to-access approach. It is a collection of name/value pairs, while it is also completely language independent. JSON is built on two structures: (a) a collection of name/value pairs, (b) an ordered list of values. JSON is a text-based format accessed via any text editor, or command line editor (e.g., Vim) on other than Windows operating systems.

Comma - Separated Values (.csv): CSV text files use commas to separate values. Typically, they store tabular data (numbers and text) in plain text. They can be opened with any text editor, such as Notepad++ [8]. The CSV file format is not fully standardized, albeit there are some specific rules and recommendations. In cases where field data also contains commas or embedded line breaks, it is a common approach to use quotation marks to surround the field.

Spreadsheets (.xls/. xslx): Spreadsheets is a program application that enables analysis and storage of data in tabular form. Spreadsheet is a file that consists of cells in rows and columns. In spreadsheets, data formats vary from numeric values to text, formulas, references and functions. Aside from storing tabular data and performing basic arithmetic and mathematical functions, spreadsheets such as Excel [9], WPS [10] provide built-in functions for statistical operations.

Extensible Markup Language (.xml): Markup Language defines a set of rules for encoding textual data such as documents. XML is widely acceptable and is used for the representation of arbitrary data structures. XML files are accessible with any web browser, editable via any text editor or website that offers a view, edit, and convert to other formats capacity. An XML file is encoded with the ASCII text standard.

Pictures (.jpg, .png): The abbreviation JPEG stands for "Joint Photographic Experts Group". It is a universal- standard image format for compressed image data. JPEG files are accessed via an image viewer or image editor, such as Paint, Windows Photos, Apple Preview. Various web browsers such as Google Chrome, Firefox and Microsoft Edge can be utilized to access images. JPEG standard specifies the codec that defines how an image is compressed into a stream of bytes and decompressed back into an image.

2.5 Data Generation, Testing and Validation

Towards designing, building and updating all individual modular prototypes to final components, a synthetic data generation pipeline will ensure the production of artificial data that simulate the structure, schema and format of the actual personal/sensitive evidence. Therefore, the GDPR and other EU-National restrictions will not be applicable. However, to test, assess and validate the final integrated solution in a near operational environment, and ensure the integrity and security of the data processing modules, GLASS will incorporate all the appropriate security, anonymisation measures.

All data will be generated and processed only for the scope of the project. Even though data will be synthetic, the main purpose is to validate the GLASS technologies and GLASS modular components with a focus on being delivered as a holistic EU based solution that is fully aligned and compatible with different use case scenarios, to be defined in T3.1 and validated in WP7.

Regarding the volume of the datasets, at this stage of the project we foresee the incorporation of synthetic users, in the magnitude of thousands, for the training of the submodules (WP7, T6.5) that will probably scale to millions.

A breakdown list of the data to be synthesised and generated is as follows (WP3):

- Citizen ID
- Birth Extract
- Passport
- Health Insurance (public or private)
- Medical History
- Valid Stay Authorisation
- Proof of Income
- School Records
- Criminal Record
- Past employment experience
- Nationality Certificate (Nationality Extract)
- Birth Certificate
- Disability Report/ Proof
- Contact details (username, email, phone numbers, etc.),
- Time stamp and hashes of the data.

Concerning the final integrated version of the GLASS platform to be deployed at the end of the project, it must be emphasised that the project will only provide the means towards a trusted and interoperable European framework, but it will not connect directly to any external repository. This will require further steps and ad-hoc configurations with the local authorities and their external systems, managed by each corresponding end user. A full communication with external systems is out of scope of the GLASS project.

3 FAIR Data

3.1 Making data findable, including provisions for metadata

Special emphasis is placed on enhancing the discoverability of the collected and generated data. GLASS follows a metadata-driven approach so as to increase the searchability and the discoverability of the data, while also facilitating its understanding and re-use. Metadata refers to information about the data collected and/or generated. It is usually structured in textual information that describes the creation, content, or context of a digital resource. The most notably known types of metadata are names, dates, location, data types, relations and interdependencies to other data sets. Metadata links information and data across the web and constitutes a powerful tool that helps individuals (researchers, developers, citizens, etc.) to discover, identify, and manage digital resources.

To further increase data discoverability, all data produced and categorised as open for sharing and re-use, will be accessible via open data repositories such as Zenodo [11]. Open access repositories like Zenodo accept any file format and offer various functionalities, such as the creation of their own collections. Open access repositories are free of charge for both the project to upload their data and individuals searching for datasets to download and re-use.

Datasets that will be uploaded to open access repositories will be deposited in a searchable resource (the cloud web storage service of the project) and will be accessible via dedicated Application Programming Interfaces (APIs).

The naming conventions in the development of the project's data files can significantly increase their searchability. Towards this, GLASS will design consistent data file names that properly describe their content, status and versioning, with a view on increasing their discoverability.

3.2 Making data openly accessible

FAIR open access to the data guide refers to making data accessible to all project partners, researchers and the public, following the privacy and anonymity guidelines of the EU and National regulations. Horizon 2020 Open Research Data Pilot [12] states that all data generated and used, if possible, are publicly open and available. The GLASS partnership will ensure the integrity of personal data and sensitive information prior to the dissemination of the datasets.

The partners of GLASS will utilize state-of-the-art methodologies towards ensuring the secure storage, delivery and access of all kinds of data and project related material, managing at the same time the clearance levels and access rights among the users.

During the execution of the project, each partner will provide detailed information on privacy/confidentiality and the procedures that will be implemented for data collection, storage, access, sharing policies (especially when third party countries are concerned), protection, retention and destruction. The consortium will confirm that the project complies with national and EU legislation throughout its lifetime and after its completion.

Personal data, if any, will be treated confidentially and carefully, taking proper technical means of information protection (e.g., storing general and personal data separately, using encryption for personal data and identities, deleting personal data when it becomes unnecessary). Some examples include public-key encryption and symmetric encryption with session keys negotiation over HTTPS. Considering that some transmitted data may be regarded as highly sensitive, the highest security standards will be used (i.e., asymmetric cryptography with at least 1024-bit keys). Where necessary

(e.g., sensitive and evidence information collected by public authorities and/or consortium members), data will be stored in a locked server, while all identification data will be stored separately. Moreover, no one outside the research team will have access to this information. The access to the database will be restricted to authorised personnel only, set by each consortium member. Moreover, an access log will be maintained to ensure the proper use of the accessed data.

For all data, especially those used in the Demonstrators (generated in WP2, WP7, WP8), the names of the participants are not pointing to real persons. All the direct and indirect (according to the EU legislation - GDPR) information of an individual will be fully masked in any printed materials, project reports or dissemination activities.

All identified dataset categories will be stored and backed up regularly through existing back-up mechanisms in place at NextCloud. Qualitative data will be backed up and secured by the coordinator on a regular basis; metadata will include clear labelling of versions and dates. The data produced and generated in the context of the research and development activities of the project, from research prototypes to development codes and deployment scripts, will be stored and preserved in a private repository in version control tools such as Github or GitLab. Accordingly, backup versions of each module will be extracted periodically and stored in the NextCloud platform. All data containing private information will be destroyed upon completion of the respective study/research task. In any case, all personal data will be destroyed at the end of the project and only anonymous or non-identifiable data will be retained after the completion of the final report.

3.3 Making data interoperable

Data interoperability refers to the ability of systems and services to access readable and editable data, in terms of their content, context and meaning. To achieve it, GLASS will incorporate suitable standards and vocabularies for data and metadata creation.

The interoperability of the aforementioned publicly available data will be achieved, since the data and its respective metadata will be stored in JSON format according to a defined JSON schema (see Section *2.3 Data types & format*). The JSON schema provides a collection of shared vocabularies that can be used to mark-up pages in ways that can be understood by the major search engines.

The interoperability of the data that will not be publicly shared will be facilitated through the use of the Dublin Core Metadata [13] standard that contains fifteen elements (Table 1) and provides a vocabulary of concepts with natural-language definitions (e.g., title, creator, author, etc.) that are instantly converted into open machine-readable formats (such as XML, HTML, etc.), thus enabling machine- processability. Alongside, data interoperability will be facilitated through the DCAT RDF vocabulary [14]. DCAT gives the ability publishers to describe datasets and data services in a catalogue using a standard model and vocabulary that facilitates the consumption and aggregation of metadata from multiple catalogues.

#	Element	Element definition
1	Title	A name given to the resource.
2	Subject	The topic of the resource.
3	Description	An account of the resource.
4	Creator	An entity primarily responsible for making the resource.
5	Publisher	An entity responsible for making the resource available.
6	Contributor	An entity responsible for making contributions to the content of the resource.
7	Date	A date associated with an event in the life cycle of the resource.
8	Type	The nature or genre of the resource.
9	Format	The file format, physical medium, or dimensions of the resource.
10	Identifier	An unambiguous reference to the resource within a given context.
11	Source	A reference to a resource from which the present resource is derived.
12	Language	A language of the resource.
13	Relation	A related resource.
14	Coverage	The spatial or temporal topic of the resource, the spatial applicability of the resource, or the jurisdiction under which the resource is relevant.
15	Rights	Information about rights held in and over the resource.

Table 0-1 Dublin Core Metadata Vocabulary [15]

3.4 Increase data re-use (through clarifying licences)

To ensure that interested third parties can re-use the GLASS research datasets, all produced data will be released under the Creative Commons Licensing scheme. Licences are the means that enable a third-party to copy, display, edit and build upon for the purposes set by a specific licence.

Data availability after the end of the project depends highly on the type and content of data, taking into account sensitivity and anonymisation status. Data should be available for public reusability after being granted permission from their respective contributors, following the proposed legal and ethics requirements.

Rich metadata will enable proper discovery and identification of the data along with the appropriate licensing schemes facilitating their re-usability. In principle, it is expected that data will become available after the publication of the respective deliverables and will remain available after the completion of the project.

To safeguard the transparency, consistency, quality, completeness and accuracy of the data, GLASS adopts a data quality assurance procedure. Peer-reviews of the data generation methods and/or data summaries will be applied to assess the quality of the dataset and identify any need for improvement.

4 Allocation of resources

The costs required for making the data collected/generated FAIR have been included in the budget of the project. Unisystems (UNIS Gr), as project coordinator and leader of WP1 and University of Patras (UPAT) as primarily responsible for the delivery of the data management strategy, have a particular responsibility in creating and updating the Data Management Plan. The relevant deliverables elaborated in WP1 and WP9 are also useful for this task.

5 Data security

The GLASS partnership pays a strong emphasis on ensuring the security of all the produced datasets, safeguarding them from unauthorized access and loss. To achieve so, dedicated technical and organization measures will be designed and applied, following the guidelines produced in the risk assessment plan formulated within *T1.3: Risk management & Quality Assurance*. More specifically, the project's data security plan will focus on minimizing the risks of a data breach during the implementation of the project, as well as after its completion. Both human, machine and hardware errors will be considered to cover a wide spectrum of potential failures.

All the information will be stored in a private and secure storage area, namely NextCloud. The data will be backed up on a regular basis and access will be restricted only to the members of the consortium. The External Advisory Board (EAB) members, who have signed an NDA, are also considered as members of the GLASS partnership, therefore full disclosure to the project files will be given to them.

To ensure that data are protected and secure, all project partners will incorporate the appropriate means in terms of both processing data as well as storing and preserving them, in private servers or cloud providers, according to the relevant legal data protection requirements (e.g., GDPR). In case of personal data collections, it is crucial that this data can only be accessible by those authorised to do so. To make the data publicly accessible in dedicated public repositories, storage environments will investigate in depth options such as Zenodo. Any personal data and sensitive information are stored after applying pseudo-anonymisation techniques and methodologies.

In case of data breach, the respective project partner is obliged to urgently notify (not later than 72 hours), the relevant national data protection authority and the subjects (partners, participants, citizens, etc.) that might be affected. The partner will develop a thorough report of the data breach. It will document the personal data breaches, including any information leaked, its effects and the remedial action(s) taken.

5.1 Archiving and preservation

The GLASS partners will utilize state-of-the-art methodologies towards ensuring the secure storage, delivery and access of all kinds of project's data and related material, managing and setting clearly the access rights among the various user types.

All partners will contribute to the later versions of this document (D1.5), by describing their privacy-confidentiality issues as well as the procedures to be implemented in terms of data collection, storage, sharing policies (especially when third party countries are concerned), protection, retention and destruction.

All the relevant EU legislation, such as GDPR and relevant national legislation, will be applied on information of an individual and any reference to personal data or sensitive information will be fully masked in any printed materials, project reports or dissemination activities.

Personal data, such as personal information from project partners members, will be treated confidentially, taking into consideration all the proper technical means. General and personal data will be stored separately. Where deemed necessary, encryption such as public-key encryption and symmetric encryption with session keys negotiation over HTTPS, will be applied on personal data. In cases of sensitive evidence and information collected by public authorities and/or consortium members the data will be stored in a locked server. Access to this information will be restricted to authorised personnel only and an access log will be maintained to record access to data.

All data containing private information will be destroyed upon completion of the respective study/research task. In any case, all personal data will be destroyed automatically at the end of the project and only anonymous or non-identifiable data will be retained after the completion of the final report.

6 Ethical aspects

All details about ethics and legal compliance in terms of current EU legislative initiatives, anonymisation procedures, consent needed, restrictions on third parties, procedures for handling sensitive data and data owners will be included in the corresponding deliverables of WP1 (D1.2, D1.3) and WP9 (D9.1- D9.1, D9.3, D9.4). Procedures and clear protocols for collection and management of research data (gathering, processing and disseminating) will be defined and implemented with the support of the consortium, the EAB members as well as the Ethics Manager. Meanwhile, information about the expected future updates of this document will be thoroughly described in the next versions of the DMP, in months 24 and 36. Additionally, the Grant Agreement and the GLASS Consortium Agreement are to be referred to for further details on the ownership and management of intellectual property and access.

7 Conclusion

This deliverable provides the first iteration on the description of the data that GLASS will generate, process and manage during its lifetime together with challenges and constraints that need to be considered to (i) ensure that the project's research data and records will be accurate, complete, interoperable and reliable, (ii) enhance data security and minimize the data loss risks, and (iii) prevent duplication of efforts allowing others to use some of the data managed by the project.

The next version of the GLASS DPM will provide an elaborated description of data management policies and a log of actions performed to sensitive data collected (if any), which will follow the guidelines described in WP1 and WP9. Moreover, the GLASS Consortium will ensure that all generated datasets do not infringe either partner IPR rules or regulations related to personal data protection. A clear and complete mechanism for systematic anonymisation of personal data will be defined and is planned to be in place before the first stage of pilots that will start in month 21.

References

[1] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf

[2] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

[3] https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

[4] https://nextcloud.com/

[5] https://github.com/

[6] https://about.gitlab.com/

[7] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[8] https://notepad-plus-plus.org/downloads/

[9] https://www.microsoft.com/en-us/microsoft-365/excel

[10] https://www.wps.com/

[11] www.zenodo.org

[12] https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm

[13] https://dublincore.org/

[14] https://www.w3.org/TR/vocab-dcat-2/#introduction

[15] https://guides.library.ucsc.edu/c.php?g=618773&p=4306386

Annexes

Annex 1 – Informed Consent

Part A – Information Sheet

The following information is provided to inform you about the "GLASS" project and help you to decide about your participation or not. The informed consent explains the purpose of the project in detail and how you can participate to provide feedback on the following aspects: **[add by project partners as needed**].

Please read this consent form carefully and ask as many questions as you wish before you decide whether you want to participate in this research. Feel free to ask questions at any time before, during, and/or after your participation. You should be aware that even if you agree to participate, you are free to withdraw at any time without saying the reason and with no repercussions for you.

Project title: 'SinGLe Sign-on eGovernAnce paradigm based on a distributed file exchange network for Security, transparency, cost effectiveness and truSt' (GLASS)

Project partners:

1. UNIS GR, Greece

2. FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (FOKUS), Germany

3. EDINBURGH NAPIER UNIVERSITY (ENU), UK

4. PANEPISTIMIO PATRON (UPAT), Greece

5. UBITECH LIMITED (UBITECH), Cyprus

6. SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED (S5), Cyprus

7. EUROPEAN ELECTRONIC MESSAGING ASSOCIATION AISBL (EEMA), Belgium

8. PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA (PDM), Portugal

9. TEKNOLOJI ARASTIRMA GELISTIRME ENDUSTRIYEL URUNLER BILISIM TEKNOLOJILERI SANAYI VE TICARET ANONIM TICARET (TGS), Turkey

10. Istanbul Metropolitan Municipality (IMM), Turkey

11. MINISTRY OF DIGITAL GOVERNANCE (MoDG), Greece

12. Ministério da Justiça (MoJ), Portugal

13. UNISYSTEMS LUXEMBOURG SARL (UNI) Luxembourg

Project-Coordinator: Ilias Kontakos - Unis Gr

Technical-Coordinator: Danai Vergeti- Ubitech
Local coordinator(s): [to be filled by the name of partner(s) in charge] Contact Information**:** [email and phone number]

1. Purpose of the research **[to filled in by partners, adapted according to the objectives of data collection]**

2. Description of GLASS **[what is the project about]**

The rapid growth of Information and Communication Technology (ICT) and its ubiquitous presence in our everyday life has significantly affected the way government services are delivered today. This poses constant challenges to safeguard the data confidentiality and integrity of e-government services, while increasing its adoption and usage by citizens and businesses. GLASS caters for a 'European Common Services Web', bringing closer together citizens, businesses and European governments. The project introduces a citizen-centric e-governance model that enables beneficiaries to participate in a network for big data exchange and service delivery, which is by design digital, efficient, cost-effective, interoperable, cross-border, secure and promotes the once-only priority. The GLASS solution comprises (i) a distributed file storage system, capable of addressing the complexity of the processes and their high demand on resources; (ii) a distributed ledger, which records every transaction among users to increase the overall transparency and trustworthiness; (iii) a distributed application (dapp) ecosystem for delivering mobile services tailored to the needs of its users; (iv) a single sign-on Wallet as a Service (WaaS) platform responsible for managing multiple services provided by each dapp; and (v) a Middleware Gateway Framework, responsible for the establishment of secure communication pathways among operational stakeholders and the integration of already existing e-governance systems with newly developed ones.

3. Participant selection **[to filled in by partners, indicating why these people have been chosen to participate in the research with reference to the objectives of data collection]**

4. Explanation of the procedure to be followed **[description of the structure of the research and flow to be followed]**

5. Reimbursement [**State clearly, what you will provide the participants with as a result of their participation.]**

Participation is voluntary and no remuneration is foreseen.

6. Duration and requirements **[how much time participants will have to allocate to the research and whether any specific requirement is needed, e.g., ICT literacy, etc.**]

7. Risks **[Explain and describe any risks that you anticipate or that are possible.]**

8. Benefits **[mention the individual benefits, the benefits to the community in which the individual resides, and benefits to society as a whole, as a result of finding an answer to the research questions.]**

9. Confidentiality **[Explain how the research team will maintain the confidentiality of data with respect to both information about the participant and information that the participant shares. If the research is sensitive and/or involves participants who are highly vulnerable, explain to the participant any extra precautions you will take to ensure safety and anonymity and avoidance of stigmatization. In case of focus groups: Focus groups provide a particular challenge to confidentiality because once something is said in the group it becomes common knowledge. Explain to the participant that you will encourage group participants to respect confidentiality, but that you cannot guarantee it.**

We will not be sharing information about you with anyone outside of the research team. The information that we collect from this research project will be kept private.

10. Participants' right to the termination of research study

You are free to choose whether or not to participate in this study. There will be no penalty or loss of benefits to which you are otherwise entitled if you choose not to participate. In the event you decide to discontinue your participation in the study, there will not be any disadvantages for you. You can decide to discontinue your participation at any time and without saying the reason! In this case, please inform us by contacting **[add the name, the affiliation, and the contact details, email, phone number of the local partner in charge]** and we will take care of all necessary steps to remove your data!

11. Data processing

[add the name and affiliation of the person in charge of data processing and contact details]

12. During the research the following personal data will be processed **[list all personal data, indicate whether video or audio recording will take place]**

13. How will your data be stored and transferred during the project?

[1. Identify all locations where data will be stored, indicating for each location whether it will be used to store identifying information or de-identified research data, and providing details of access controls that will be applied.
2. Describe any administrative measures that you will take to control the risks of inappropriate disclosure, e.g., pseudonymization, and procedures for secure transfer between locations, e.g., using file encryption and encrypted channels.
3. Specify who will be able to access the identifying information and how you will ensure they process the information securely, e.g., through training, supervision and adherence to secure data handling procedure.
4. Confirm that all data requested are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in accordance with Article 5 of GDPR]

14. How will research data be preserved and shared on completion of the project?

[1. Identify the research data that will be preserved and shared at the end of the project by deposit in a public data repository or other archiving solution.

2. Describe the measures that will be taken to ensure data are suitable for sharing, e.g., securing consent, anonymizing data prior to deposit/sharing, sharing confidential or high-risk information under a controlled access policy.
3. Identify data repositories or other solutions that will be used to preserve and share data]

15. How will retention and disposal of personal data and confidential information after project completion be managed?

[State how long you plan to retain personal data/confidential information after the end of the project. Specify under whose authority this information will be maintained and disposed of after the project]

16. Publications

Results of this study can be publicized with anonymized data only. This ensures that it will not be possible to identify you in any way. Your personal data will never be published!

The Ethics Manager, Ms. Georgia Livieri, Unisystems Luxemburg, LivieriG@unisystems.gr, will oversee that the procedures run smoothly; in case of any non-compliance, the Ethics Manager in collaboration with the Ethics Committee will decide the timeline and mitigation measures, so as to take all the necessary actions in a timely manner and ensure full compliance with the legal and ethical requirements of the project. In all cases, all non-compliant actions will be immediately suppressed or suspended, and the partners will implement a mitigation action within 5 working days.

Part b- Consent Form

Project title: 'SinGLe Sign-on eGovernAnce paradigm based on a distributed file exchange network for Security, transparency, cost effectiveness and truSt' (GLASS)

Participant name: _____
Gender: _____ [plus the option I prefer not to say]
Age range: 18-25, 26- 35, 36-45, 46-55, 56+
Stakeholder role: [select the one(s) that apply: public servant, citizen, user of the service, case study participant, NGO representative, other (pls specify_____)]
Which is your highest degree in education:
Email address: _____

I have read very carefully and completely understood this consent form, and I volunteer to participate in this research study, as a choice under free will. I understand that I will receive a copy of this form. I have had the opportunity to ask, and I have received answers to, any questions I had regarding the study.
I was thoroughly informed about the aim and course of the study, my rights and obligations, and the voluntary nature of participation.

I agree with the processing of my personal data as part of the research project as described in the Participant Information Form. I was informed about my privacy rights, especially my right to cancel my participation.

Place, date _____ Place, date _____

Participants' signature Signature of the partner in charge

Annex 2 – Available Datasets

Annex 2 includes an extensive list of the datasets (rows), already delivered and to be developed in the context of the project's research and implementation activities. The list is comprised of nine (9) columns each of which present the key aspects of each dataset:

1. The corresponding work package (WP)
2. The relevant deliverable (Del)
3. The related task (Task)
4. A description of each dataset, as described in the GA (Description)
5. The lead beneficiary (Lead)
6. The type of each dataset (Type) (Section 2.3)
7. The means of archiving (Archiving)
8. The dissemination level (Diss level)
9. The estimated due date (Due date)

Aside from the expected deliverables, Annex 2 also includes all the supportive and complementary datasets (documents, excel, contacts, etc) structured towards delivering the goals of the project.

WP	Del	Task	Description	Lead	Type	Archiving	Diss. Level	Est. Due Date
WP1	-	T1.1	Information about the consortium and legal documents (Grant Agreement, Consortium Agreement)	UNIS GR	Project files	NextCloud	Private	-
WP1	-	T1.1	Meetings minutes & Recorded Teleconferences	UNIS GR	Project files	NextCloud	Private	-
WP1	D1.1	T1.1	A management plan that will consist of a list with all the responsibilities of each partner, templates and set of documentation for the management process, quality checks and procedures for all deliverables and the internal and external review processes.	UNIS GR	Project files	Local/ NextCloud	Public	31 Mar 2021
WP1	D1.2	T1.4	An initial draft a (before the kickoff of the GLASS demonstration) of the Legal and Ethics Manual will be prepared and issued to assure the ethical assurance, the gender equality and the compliance with national and EU legislation.	UNI	Research activities	Local/ NextCloud	Public	28 Feb 2021
WP1	D1.3	T1.4	A final revised version of the Legal and Ethics Manual will be prepared and issued to assure the ethical assurance, the gender equality and the compliance with national and EU legislation.	UNI	Research activities	Local/ NextCloud	Public	31 Dec 2022
WP1	D1.4	T1.1, T1.3	The report will include current progress versus objectives, results achieved and planned actions per WP, dissemination activities, as well as potential deviations in relation to the original work plan and corrective measures. The report will also include methods related to risk analysis, monitoring and mitigation and report on the results and conclusions of the risk management and quality assurance methods used.	TGS	Research activities	Local/ NextCloud	Public	31 Dec 2022
WP1	D1.5	T1.5	This deliverable will provide the plan for managing the data generated and collected during the project.	UPAT	Research activities	Local/ NextCloud	Public	30 Jun 2021
WP2	D2.1	T2.1	D2.1 | Draft Document	UPAT	Project files	Local/ NextCloud	Public	30 Sep 2021

WP2	D2.2	T2.2	Draft Document D2.2: GLASS EU legal framework	EEMA	Project files	Local/ NextCloud	Public	30 Sep 2021
WP2	D2.3	T2.3	Draft Document D2.3: Government to ALL Specification list	S5	Project files	Local/ NextCloud	Public	31 Dec 2021
WP2	D2.5	T2.5	Use of e-Wallets: Citizen Perception Survey I Survey Launch	TGS	Project files	Local/ NextCloud	Public	28 Feb 2022
WP2	D2.1	T2.1	This deliverable includes a thorough analysis on the solutions, best practices and best of breed technological methodologies for eGovernment and eGovernance models at an international level.	FOKUS	Research activities	Local/ NextCloud	Public	30 Sep 2021
WP2	D2.2	T2.2	The law and policy framework to be considered for the establishment of the eGovernance model, based on the finding of the analysis of T2.2.	EEMA	Research activities	Local/ NextCloud	Public	30 Sep 2021
WP2	D2.3	T2.3	This deliverable provides the full registry with the identified digital interactions, their dependencies and their specification for the digitization of public services.	S5	Research activities	Local/ NextCloud	Public	31 Dec 2021
WP2	D2.4	T2.4	The deliverable will present the operational eGovernance related whitepaper of the proposed framework, in technical and operational aspects.	UPAT	Research activities	Local/ NextCloud	Public	28 Feb 2022
WP2	D2.5	T2.5	This deliverable will provide the GLASS business model. It will also provide the guidelines, the actions to be done towards the adoption of the GLASS eGovernance model from private and public organizations.	TGS	Research activities	Local/ NextCloud	Confidential	28 Feb 2022
WP3	D3.1	T3.1	Consolidated Demonstrator policies; Consolidated Evidences; Activity diagrams; Consolidated Use Case Pilot Integration Scenarios	TGS	Project files	NextCloud	Public	30 Jun 2021
WP3	D3.2	T3.2	Technical requirements; activity diagrams	UBI	Project files	Local/ NextCloud	Public	30 Sep 2021
WP3	D3.1	T3.1	This deliverable will document the use-case and user requirements of GLASS.	TGS	Research activities	Local/ NextCloud	Public	30 Jun 2021
WP3	D3.2	T3.2	This deliverable presents the system specifications for all different components/modules of the GLASS overall solution, including also the interoperability specifications. These specifications	UBI	Research activities	Local/ NextCloud	Public	30 Sep 2021

			will be refined after the first evaluation.					
WP3	D3.3	T3.3	This deliverable will provide the data sharing model to protect the data integrity from exchanges among untrusted entities, distributed systems, modules and centralized databases.	ENU	Dev. package	Github/ NextCloud	Confidential	30 Sep 2021
WP3	D3.4	T3.4	This deliverable gives an overview and upgraded version of the general architecture of GLASS. Interfaces and hybrid integration methodologies will also be defined.	FOKUS	Research activities	Local/ NextCloud	Public	31 Dec 2021
WP3	D3.5	T3.4	This deliverable gives an overview and upgraded version of the general architecture of GLASS. Interfaces and hybrid integration methodologies will also be defined.	FOKUS	Research activities	Local/ NextCloud	Public	30 Sep 2022
WP4	D4.1	T4.1	This deliverable will outline the challenges, the research problems and the scientific directions addressed in WP4, along with the SotA report that will be the baseline for the design and development of the first prototypes.	PDM	Research activities	Local/ NextCloud	Public	30 Sep 2021
WP4	D4.2	T4.1	This deliverable will outline the challenges, the research problems and the scientific directions addressed in WP4, along with the SotA report that will be the baseline for the design and development of the first prototypes.	PDM	Research activities	Local/ NextCloud	Public	30 Jun 2023
WP4	D4.3	T4.2	This deliverable will produce the initial and the final version of the UDID prototypes	PDM	Dev. package	Github/ NextCloud	Confidential	30 Jun 2023
WP4	D4.4	T4.3	This output focuses on the delivery of the first and final version of the back-end mechanisms of the WaaS functionalities.	PDM	Dev. package	Github/ NextCloud	Confidential	30 Jun 2023
WP4	D4.5	T4.4	This deliverable will provide the user-interfaces of the WaaS.	UBI	Dev. package	Github/ NextCloud	Confidential	30 Jun 2023
WP4	D4.6	T4.5	The deliverable will provide the single sign-on distributed APIs to support the IAS and enable the utilization of multi-factor authentication in the secure identity management ecosystem.	ENU	Dev. package	Github/ NextCloud	Confidential	30 Jun 2023
WP5	D5.1	T5.1	This deliverable will be responsible for the architecture and the development of the public	ENU	Dev. package	Github/ NextCloud	Confidential	30 Jun 2022

			distributed ledger, the ledger's API as well as the configuration of the IPFS architecture, deployment and its integration within the network along and the ledger.					
WP5	D5.2	T5.3, T5.4	This deliverable will provide an extended SotA report along with the developed consensus function that will operate to ensure the consensus on GLASS ledger. Alongside, it delivers the GLASS seamless and secure multi-sided identity and data management module and the compliance control mechanics.	S5	Dev. package	Github/ NextCloud	Public	30 Jun 2022
WP5	D5.3	T5.5	This deliverable will record the requirements and the framework that developers will need to create compatible dapps with the GLASS infrastructure.	ENU	Research activities	Local/ NextCloud	Public	31 Aug 2022
WP5	D5.4	T5.5	This deliverable will design, develop and deploy into the ecosystem, the dapps which will support the cross-border documentation exchange, data sharing, communication establishment among cross-sector entities.	UBI	Dev. package	Github/ NextCloud	Confidential	31 Mar 2023
WP6	D6.1	T6.1	This deliverable aims to produce the secure gateway channel to support ad hoc intercommunication functionalities among users, alongside with the documents which list the technical specification as well as the operational functionalities of the module.	UBI	Dev. package	Github/ NextCloud	Confidential	30 Jun 2023
WP6	D6.2	T6.2	This will provide the browser that runs on the distributed environment, enabling the searching capabilities of content, libraries, reusable smart contracts, code, among others.	S5	Dev. package	Github/ NextCloud	Confidential	30 Jun 2023
WP6	D6.3	T6.3	This deliverable will deliver the transaction analytics module alongside with its technical documentation to enable and support its maintenance and operation from end users.	S5	Dev. package	Github/ NextCloud	Confidential	31 Aug 2022
WP6	D6.4	T6.4	This deliverable comprises the data and documents collected to feed the neural network and initiate the	UPAT	Dev. package	Github/ NextCloud	Public	31 Aug 2022

			learning process of the artificial neurons.					
WP6	D6.5	T6.4	This deliverable deploys the AI Data Schema Transformer module, that will enable the interoperability among various types of systems.	UPAT	Dev. package	Github/ NextCloud	Confidential	31 Aug 2022
WP7	D7.1	T7.1	This deliverable will provide an integration plan, that documents all technical and operational aspects and the APIs to be developed, to guide the integration process and ensure the quality of the results.	UNIS GR	Research activities	Local/ NextCloud	Confidential	30 Jun 2022
WP7	D7.2	T7.3	D7.2 will provide a detailed demonstration plan for the demonstrators, the timelines and testing protocols based on the results presented on D3.1.	PDM	Demonstration activities	Local/ NextCloud	Public	30 Sep 2022
WP7	D7.3	T7.3	This deliverable provides the details on the operational functionalities giving the guidelines that support the technical maintenance of each individual module alongside with the technical and operational evaluation guidelines.	UNI	Demonstration activities	Local/ NextCloud	Public	30 Sep 2022
WP7	D7.4	T7.4	This deliverable aims to report the findings from the questionnaires, interviews and all the interactive procedures of T7.4 which targets to gather information related to users' acceptance and adoption rates.	IMM	Demonstration activities	Local/ NextCloud	Public	31 Dec 2023
WP7	D7.5	T7.2	This deliverable provides the first prototype and the final release of the integrated GLASS framework.	UNIS GR	Dev. package	Local/ NextCloud	Confidential	30 Jun 2023
WP7	D7.6	T7.5	The policy recommendation report will supplement the GLASS governance model (D2.4) and present the findings and results of the research and operational tested demonstrators to promote the advantages of such distributed governance modeling, towards its full adaptation.	MoDG	Research activities	Local/ NextCloud	Public	30 Nov 2023
WP8		T8.1	Final Document D8.1: Dissemination and Communication Plan & Website	EEMA	Project Files	Local/ NextCloud	Public	30 June 2021
WP8	-	-	Conference Paper: A trustable and interoperable decentralized solution for citizen-centric and cross-border eGovernance: A conceptual approach (https://arxiv.org/abs/2103.15458)	UPAT	Research activities	-	Public	-

WP8	D8.1	T8.1, T8.2	This deliverable will describe the detailed plan for the project dissemination and exploitation strategy to be adopted throughout the project's lifetime, and it will define the plan with which the different stakeholder communities will be targeted, as well as the establishment of the project website along with the social media which will be used. This will include management procedures for interacting with the Advisory Board.	EEMA	Dev. package	Github/ NextCloud	Public	30 Jun 2021
WP8	D8.2	T8.1, T8.2	This deliverable will describe the dissemination and communication activities up to M12 and highlight updates and modifications to the initial plan (including plans for workshops). This will include KPI monitoring.	EEMA	Research activities	Local/ NextCloud	Public	31 Dec 2021
WP8	D8.3	T8.1, T8.2, T8.3	This deliverable will describe the dissemination and communication activities from M13 to M36, including workshops. It will also compare actual performance to expected KPIs. The training programs and workshops will be detailed, and the outcomes, attendees and content will be reported. This final report will include a summary of contributions of the Advisory Board and complete minutes of any Advisory Board meetings during the project lifetime.	EEMA	Research activities	Local/ NextCloud	Public	31 Dec 2023
WP8	D8.4	T8.4	This deliverable will summarize the activities towards ongoing commercialization, including measures taken to protect IPR and future opportunities.	TGS	Research activities	Local/ NextCloud	Confidential	31 Dec 2023
WP8	D8.5	T8.5	This deliverable describes and summarizes the project activities in standard development and engagement.	FOKUS	Research activities	Local/ NextCloud	Public	31 Dec 2023
WP9	D9.1	T1.4	The procedures and criteria that will be used to identify/recruit research participants must be submitted as part of a deliverable. The informed consent procedures that will be implemented for the	UNIS GR	Research activities	Local/ NextCloud	Confidential	30 Jun 2021

			participation of humans and in regard to data processing must be submitted as part of a deliverable. Templates of the informed consent/assent forms and information sheets covering the voluntary participation (humans) and data protection issues (in language and terms intelligible to the participants) must be submitted as part of a deliverable. Details on incidental findings policy must be submitted as part of a deliverable. The applicant must clarify whether vulnerable individuals/groups will be involved, and the measures to protect them and minimize the risk of their stigmatization must be submitted as part of a deliverable.					
WP9	D9.2	T1.4	Copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans must be obtained before the start of the relevant activities, and submitted as a deliverable	UNIS GR	Research activities	Local/ NextCloud	Confidential	31 Oct 2021
WP9	D9.3	T1.4	In case activities undertaken in non-EU countries raise ethics issues, the applicants must ensure that the research conducted outside the EU is legal in at least one EU Member State. This must be submitted as part of a deliverable. Details on the materials which will be imported to/exported from the EU must be submitted as part of a deliverable. In case personal data are transferred from the EU to a non-EU country or international organisation, confirmation that such transfers are in accordance with Chapter V of the General Data Protection Regulation 2016/679, must be submitted as part of a deliverable.	UNIS GR	Research activities	Local/ NextCloud	Confidential	30 Jun 2021

			In case personal data are transferred from a non-EU country to the EU (or another third state), confirmation that such transfers comply with the laws of the country in which the data was collected must be submitted as part of a deliverable.					
WP9	D9.4	T1.4	In case sensitive personal data will be collected, processed and stored, the beneficiary must check if special derogations pertaining to the rights of data subjects or the processing of genetic, biometric and/or health data have been established under the national legislation of the country where the research takes place and submit a declaration of compliance with respective national legal framework(s) as part of a deliverable. In case sensitive personal data will be collected, processed and stored, justification for the processing of sensitive personal data must be submitted as part of a deliverable. The beneficiary must explain how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle). This must be submitted as part of a deliverable. A description of the technical and organizational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as part of a deliverable. Description of the anonymization/pseudonymization techniques that will be implemented must be submitted as part of a deliverable.	UNIS GR	Research activities	Local/ NextCloud	Confidential	30 Jun 2021

			An explicit confirmation that the data used in the project is publicly available and can be freely used for the purposes of the project must be submitted as part of a deliverable. The beneficiary must evaluate the ethics risks related to the data processing activities of the project. This includes also an opinion if data protection impact assessment should be conducted under art.35 General Data Protection Regulation 2016/679. The risk evaluation and the opinion must be submitted as a deliverable.					
WP9	D9.5	T1.4	The host institution must confirm that it has appointed a Data Protection Officer (DPO) and the contact details of the DPO are made available to all data subjects involved in the research. For host institutions not required to appoint a DPO under the GDPR a detailed data protection policy for the project must be submitted as a deliverable.	UNIS GR	Research activities	Local/ NextCloud	Confidential	31 Jan 2021