

DES HE data management plan

Deliverable ID:	D6.2
Project acronym:	U-AGREE
Grant :	101167187
Call :	HORIZON-SESAR-2023-DES-ER-02
Topic :	HORIZON-SESAR-2023-DES-ER2-WA1-4
Consortium coordinator:	UNIVERSITAT POLITECNICA DE VALENCIA
Edition date:	14 March 2025
Edition:	1.00
Status :	Final version
Classification:	PU

Abstract

The U-AGREE Data Management Plan (DMP) provides a structured framework for handling the data collected, generated, and analysed throughout the project lifecycle. In accordance with Horizon Europe and SESAR 3 JU requirements, this DMP ensures compliance with the FAIR (Findable, Accessible, Interoperable, and Reusable) principles, detailing how research data will be managed, stored, preserved, and shared both during and after the project.

The DMP includes a data summary, outlining the types of data used, their estimated size, and their sources, whether newly collected, re-used from existing datasets, or a combination of both. It also addresses data security, storage, and recovery provisions, as well as potential ethical or legal considerations that may impact data sharing.

The DMP is a living document that will be updated regularly. The DMP serves as both a practical management tool for the project team and a coordination instrument to facilitate alignment with other projects, ensuring effective data handling throughout U-AGREE.

Authoring & approval

Author(s) of the document

Organisation name	Date
EuroUSC Italia	14.03.2025

Reviewed by

Organisation name	Date
UPV	12.03.2025
DLR	13.03.2025
EUROCONTROL	13.03.2025

Approved for submission to the SESAR 3 JU by

Organisation name	Date
UPV	13.03.2025
DLR	13.03.2025
EUROCONTROL	13.03.2025

Rejected by¹

Organisation name	Date

Document history

Edition	Date	Status	Company author	Justification
00.01	15.01.2025	Draft	EuroUSC Italia	Table of content
00.02	28.01.2025	Draft	EuroUSC Italia	Editing and implementation
00.03	03.02.2025	Draft	UPV	Integration from the WP1 and WP4 leader
00.04	13.03.2025	Draft	DLR	Integration from the WP3 leader

¹ Representatives of the beneficiaries involved in the project.

00.05	04.03.2025	Draft	ENGage srl	Integration from the WP5 leader
00.10	12.03.2025	Draft	EuroUSC Italia	First complete draft
1.00	14.03.2025	Final version	EuroUSC Italia	Final editing and submission

Copyright statement © (2025) – (UPV, EUROCONTROL, EUROUSC ITALIA, ENGage srl, DLR, COLLINS, ENAIRE, CRIDA, INECO, CRA). All rights reserved. Licensed to SESAR 3 Joint Undertaking under conditions.

U-AGREE

U-SPACE AIR AND GROUND RISK MODELS ENHANCEMENT

U-AGREE

This document is part of a project that has received funding from the SESAR 3 Joint Undertaking under grant agreement No 101167187 under European Union's Horizon Europe research and innovation programme.



Table of content

Abstract	1
1 Data summary	6
2 FAIR data	10
2.1 Making data findable, including provisions for metadata	10
2.2 Making data accessible	10
2.2.1 Repository	10
2.2.2 Data	11
2.2.3 Metadata	11
2.3 Making data interoperable	12
2.4 Increase data re-use	12
3 Other research outputs	13
4 Allocation of resources	14
5 Data security	15
5.1 General policy on data security	15
5.2 Project policy on the protection of personal data	16
5.2.1 Principles for Data Protection	16
5.2.2 Purposes and legal basis for the processing of personal data	17
5.2.3 Rights of Data Subjects	18
5.2.4 Security Measures, Data Storage, Data Retention, Data Destruction, Data Breaches	21
5.2.5 Transfers of personal data to third countries or international organisations	23
6 Ethics	24
7 Other issues	25
8 Annex 1 – U-AGREE consent form (template)	26

List of tables

Table 1: list of acronyms	5
Table 2 WP1 Data summary	6
Table 3 WP2 Data summary	7
Table 4 WP3 Data summary	8
Table 5 WP4 Data Summary	8

Table 6 WP5 Data summary	9
Table 7 WP6 Data summary	9

Acronym	Description
CDE	Communication, Dissemination and Exploitation
DMP	Data Management Plan
DOI	Digital Object Identifier
EDPB	European Data Protection Board
EU	European
FAIR	Findability, Accessibility, Interoperability, and Reusability
GA	Grant Agreement
GB	Gigabyte
GDPR	General Data Protection Regulation
KB	Kilobyte
n/a	not applicable
SESAR JU	SESAR Joint Undertaking
SORA	Specific Operations Risk Assessment
TB	Terabytes
UAS	Unmanned Aviation System
UPV	Universitat Politècnica de València
WAN	Wide Area Network
WP	Work Package

Table 1: list of acronyms

1 Data summary

Throughout the U-AGREE project, various types of technical and research data will be generated, gathered, and processed across all Work Packages (WPs). Suitable methodologies and tools must be identified for data collection and analysis, along with a structured system for storing, managing, and safeguarding the data throughout the project's duration. Additionally, an essential aspect of U-AGREE's data management strategy is ensuring proper consent procedures for collecting and handling certain personal data, particularly in cases where individuals voluntarily participate in project activities such as events or feedback requests.

The tables below outline the research requirements related to data collection, generation, and processing for each WP. It specifies the types and sources of data, the purpose of processing, estimated dataset sizes, and the potential benefits for both project partners and external stakeholders. This information will be regularly updated as the project progresses.

WP1 - Project management and coordination	
Data	- Personal data (image data, audio data, contact data, contract data, connection data, location data) - Technical data
Origin(s)	Data generated within the U-AGREE project (e.g., deliverables, datasets, communication materials) or provided directly by the Consortium team (e.g., contact data, location data).
Purpose(s)	To manage the project team, coordinate at all levels, and set up and organize meetings. The collected data will be primarily used for the preparation of Technical and Financial reports, among other project-related activities. In accordance with the Grant Agreement (GA), beneficiaries must process personal data under the Agreement in compliance with applicable European (EU), international, and national data protection laws, particularly Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR).
Size(s)	The estimated size of the data expected to be generated is projected to be up to 1 gigabyte (GB).
Data utility(s)	The generated data in this WP might be useful to: - Consortium of the project - SESAR JU - Commision European (CE)

Table 2 WP1 Data summary

WP2 – Concept formulation	
Data	• Technical data • Reused data
Origin(s)	Sector based datasets coming out from other SESAR JU projects previously performed. The collection is carried out through appropriate standards.
Purpose(s)	Research, validation and Communication, Dissemination, and Exploitation (CDE) activities.
Size(s)	The estimated size of the data expected to be generated or reused is in kilobytes (KB).
Data utility(s)	The dataset might be useful to: • project beneficiaries • sector-based networks • EU and international institutions

Table 3 WP2 Data summary

WP3 – Risk models	
Data	• Technical data generated by the project. ○ Deliverable D3.1 Initial Air Risk Model ○ Deliverable D3.2 Initial Ground Risk Model ○ Deliverable D3.3 Initial Collision Risk Model ○ Deliverable D3.4 Final Air Risk Model ○ Deliverable D3.5 Final Ground Risk Model ○ Deliverable D3.6 Final Collision Risk Model ○ Associated algorithms, statistics, formulas, schematics, etc. • Reused data ○ Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 ○ Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 ○ Commission Implementing Regulation No. 2021/664 of 22 April 2021. ○ Deliverables and datasets produced by other SESAR projects (e.g., CORUS-XUAM, BUBBLES, etc.) ○ Openly accessible wildlife research data and bird strike research results ○ Openly accessible data on accidents/ incidents
Origin(s)	• Regulation by European Commission (EC). • Deliverables by other SESAR projects.
Purpose(s)	Research and risk modelling activities related to the project objective.
Size(s)	The estimated size of the data expected to be generated or reused is projected to be up to 1 GB.

Data utility(s)	The dataset might be useful to: • project beneficiaries • the academic community • national /EU /international institutions
-----------------	--

Table 4 WP3 Data summary

WP4 – U-space mitigation barriers characterisation	
Data	• Technical data generated by the project. ○ Deliverable D4.1 Initial barriers characterisation ○ Deliverable D4.2 Final barriers characterisation ○ Simulated trajectories. ○ Simulated flight plan. ○ Algorithms, diagrams, schematics, etc. • Reused data ○ Commission Implementing Regulation No. 2021/664 of 22 April 2021. ○ Deliverables and datasets produced by other SESAR projects (e.g., CORUS-XUAM, BUBBLES, etc.) ○ Manned aircraft trajectories. ○ Statistical data of UAS trajectories.
Origin(s)	• Regulation by European Commission (EC). • Deliverables by other SESAR projects. • Flight aware trajectories of manned aircraft provided by COLLINS. • Statistical parameters from UAS trajectories provided by EUROCONTROL based on data recorded in ACCUTE project. • Synthetic trajectories previously generated/recorded in other SESAR projects (e.g., BUBBLES, SPATIO). • Simulated trajectories generated using tools developed by UPV, Engage s.l.r., and CRA.
Purpose(s)	Research and validation activities related to the project objective.
Size(s)	The estimated size of the data expected to be generated or reused is in less than 1 Terabytes (TB).
Data utility(s)	The dataset might be useful to: • project beneficiaries • the academic community • sector-based networks • national /EU /international institutions.

Table 5 WP4 Data Summary

WP5 – Concept evaluation	
Data	• Technical data • Reused data
Origin(s)	• Flyzones from D-Flight • Obstacles from OpenStreetMap • Synthetic flight plan generated within the simulators • Synthetic trajectories generated within the simulators
Purpose(s)	Research and validation activities related to the project objective
Size(s)	The estimated size of the data expected to be generated or reused is in gigabytes (GB).
Data utility(s)	The dataset might be useful to: • project beneficiaries • the academic community • national /EU /international institutions.

Table 6 WP5 Data summary

WP6 – Communication, dissemination and exploitation	
Data	• Personal data (image, audio, contact data) • Re-used data
Origin(s)	Surveys, interviews, and registration forms for workshops and events. The collection is carried out through appropriate standards.
Purpose(s)	Research and communication, dissemination and exploitation activities.
Size(s)	The estimated size of the data expected to be generated or reused is in gigabytes (GB).
Data utility(s)	The dataset might be useful to: • project beneficiaries • the academic community • sector-based networks • national /EU /international institutions

Table 7 WP6 Data summary

2 FAIR data

U-AGREE is dedicated to implementing FAIR data management principles throughout the project, ensuring that research data is handled in a way that enhances its accessibility, usability, and long-term value. FAIR, standing for Findability, Accessibility, Interoperability, and Reusability, defines the essential qualities that data should possess to support effective discovery and broad dissemination.

All research publications within the project will also align with FAIR principles. While efforts will be made to promote open access, some data and findings may remain restricted due to confidentiality agreements or licensing constraints, particularly within the aviation sectors.

2.1 Making data findable, including provisions for metadata

To improve the discoverability of data within the U-AGREE project, a structured metadata framework will be implemented. This framework will facilitate the organisation, identification, and tracking of both existing and newly generated data assets, ensuring they can be efficiently located and utilised. Keywords will be incorporated to optimise data discovery and encourage potential reuse. As part of this effort, the Consortium will take specific steps to enhance data findability, including the assignment of persistent identifiers such as Digital Object Identifier (DOIs), provided by established repositories like Zenodo.

The responsibility for completing metadata records will lie with data owners and providers, ensuring accurate and comprehensive documentation. These records will be securely stored within the U-AGREE repository, and metadata summaries for each dataset will be made publicly accessible through trusted repositories.

Further details on metadata provisions can be found in § 2.2.3.

2.2 Making data accessible

2.2.1 Repository

For the U-AGREE project, the consortium and its partners will ensure that data is stored exclusively in trusted repositories, following specific conditions outlined in appropriate agreements. The selection of these repositories will be determined as the project progresses and will be documented in the second release of the DMP.

For internal operational needs, the consortium will utilise the collaborative workspace provided by Universitat Politècnica de València (UPV) on Microsoft SharePoint. This private, project-specific platform will enable all beneficiaries to share working documents and temporarily store master copies of raw data for processing and analysis. However, local drives, company cloud storage, and external portable devices are not considered within the scope of this data management plan and will not be used for official data storage.

For long-term storing of data and to guarantee the findability, accessibility, interoperability, and reusability of data generated by, U-AGREE has the option to create a Zenodo community.

2.2.2 Data

The U-AGREE consortium adheres to a set of open data policies aimed at ensuring transparency and accessibility while safeguarding necessary confidentiality constraints.

- **Open access to scientific publications:** All beneficiaries will guarantee free access to peer-reviewed scientific publications related to the project's findings, in line with Article 17 of the GA. The consortium is committed to open-access publishing and will prioritise dissemination through platforms that support open access.
- **Open access to research data:** Digital research data, along with the necessary metadata to validate published findings, will be stored in research data repositories. Whenever feasible, beneficiaries will enable third parties to access, analyse, use, reproduce, and share these datasets free of charge. However, some data may be restricted under the principle of "as open as possible, as closed as necessary." In cases where open access would compromise the project's objectives, certain data may remain confidential.

In case of embargo due to the need to allow time for publication or to seek protection of intellectual property (e.g., patents), the duration of the embargo and the underlying reasons will be determined on a case-by-case basis, taking into account the specific circumstances of each situation. The consortium will work to balance the protection of intellectual property rights with the goal of ensuring open access to data and research outputs, while adhering to relevant legal and ethical considerations.

Within U-AGREE, project data will be classified into three categories, as follows and each with different access conditions:

- **Open data** can be freely accessed, used, and cited without requiring permission from the original researcher.
- **Sensitive (confidential/restricted) data** may be accessible under specific conditions, such as the removal of identifying information or ethical clearance. In some cases, researcher approval may be required, and access might be granted under restrictions (e.g., through a Non-Disclosure Agreement). This applies particularly to datasets collected from experts feedback, where confidentiality and security considerations must be observed. Regardless of restrictions, processed data results will be shared within the consortium.
- **Closed data** will not be made available for sharing. Some U-AGREE datasets may remain closed if their disclosure conflicts with the legitimate interests of beneficiaries, such as commercial considerations, patent applications, or proprietary developments.

2.2.3 Metadata

For the purposes of the U-AGREE project, the following types of metadata will be generated: Preservation metadata, which refers to the information used by repositories to support the long-term digital preservation of data. In addition to this, the Consortium and its partners will create and provide

metadata that ensures data findability and accessibility. This metadata will be structured in a way that allows it to be harvested and indexed by external systems, ensuring that it can be easily discovered and accessed.

2.3 Making data interoperable

U-AGREE will aim to ensure that the project datasets can be effectively shared, integrated, and used across different systems and disciplines. For the purposes of data interoperability, the Consortium and its partners will follow the interoperability best practices endorsed by their professional communities for all the data generated and used within the project.

2.4 Increase data re-use

To promote and increase the re-use of data, the Consortium and its partner will promote adequate data validation and qualified references to other data. More details will be provided about data reuse in the final release of U-AGREE DMP. Details concerning the ownership, transfer and dissemination of projects results are defined in U-AGREE Consortium Agreement and shall be followed accordingly. The relevant rules of the Grant Agreement, in specific Article 13, Article 15, Article 16 and Annex 5, are also relevant and apply accordingly.

3 Other research outputs

The U-AGREE project will not generate any additional research outputs beyond those already planned and delivered.

4 Allocation of resources

The effective distribution of resources plays a critical role in ensuring the successful execution of data management within the project. Adequate allocation of both financial and human resources guarantees that the project will meet its data objectives while remaining within the specified budget and timeline. The responsibilities for making the data accessible have been allocated to the WP leads coordinated by the Project Manager.

The project budget, already allocated among the partners, will cover the costs necessary to make the data FAIR. No additional costs are expected for storing open results in the project's designated repository (Zenodo).

Data will be maintained for a minimum of 5 years after the completion of the project. As per Zenodo's general policies (<http://about.zenodo.org/policies/>), data items will be preserved for as long as the repository exists.

5 Data security

5.1 General policy on data security

Measures are established to ensure the security of project data, protecting its confidentiality, integrity, and availability. These safeguards are implemented in compliance with applicable data protection regulations and to preserve sensitive or confidential information.

In addition to software and hardware security standards, data will be protected by applying strict data protection procedures. Any personal data will be processed legally and fairly: collection of data will be adequate, relevant and not excessive in relation to the purposes of the project; data that identifies individuals (personal data) will not be kept any longer than necessary. Any personal data will be destroyed two years past the termination of the project. The Consortium will comply with European (i.e., GDPR) and national legislation relevant to the countries where data collection is taking place.

Data collected for research purposes (including questionnaires, interviews, field observations, audio/screen recordings where applicable), as well as promotional materials gathered during data collection activities and project events that may be video recorded or photographed, will be subjected to current European regulations on matters of data handling and privacy (GDPR, Regulation (EU) 2016/679). The research outcomes will always be reported without contravening the right to privacy and data protection.

- **Secure Storage Policy:** Any partner is accountable for the processing activities performed within its research and administrative activities. All the processing activities shall be compliant with the applicable legislation and with the consortium policies. Storage practices shall be compliant with minimisation and confidentiality principles. All personal data will be stored on digital hard disks on computers that are not connected to Wide Area Network (WAN) Internet. Removable storage will include large-capacity hard drives that will be kept in locked cabinets.
- **Anonymisation Policy:** According to the minimisation principle (reg. EU 2016/679, Article 5(1)(c)), partners will ensure the processing of «personal data shall be [...] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed» and «if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject» (ibidem, Article 11(1)). Against this background, the consortium adopts a specific anonymisation policy that prescribes the anonymisation of all personal data that does not explicitly require processing in an identifiable format. Any partner is accountable for the anonymisation techniques adopted by its team. Generally, the main reference for anonymisation is the Working Party Article 29 Opinion 5/2014 on Anonymisation Techniques.
- **Secure Access Policy:** Data will be encrypted, and password protected. Only members of the team directly working with the data (“need to know”) will have authorisation to access the data. Each Data Controller will be responsible for de-identification of the data or establishing a procedure to be followed by other partners in charge of personal data.

- **Secure Sharing Policy:** If data might be transferred for further processing to other project members, sharing needs to have an adequate legal basis. The admitted legal basis includes the consent of the data subject; and the legitimate interests of the controller(s) if justified by documented interrelation among task(s) and/or WPs.
- **Monitoring of Data Transfer:** The data will not be transferred outside the Consortium without prior authorisation

5.2 Project policy on the protection of personal data

The Consortium and its partners may need the processing of personal data. The following table provides an overview of the categories of personal data processed in the project and the related purpose(s).

Category of data	Data	Purposes
Personal data	Name, date and place of birth, organisation	Communication, dissemination, exploitation activities.
Image data	Pictures, photos, videos, or other identifiable illustrations of face, body and/or parts of body	Communication, dissemination, exploitation activities.
Audio data	Audio records concerning voice, processed in an identifiable way	Communication, dissemination, exploitation activities.
Contact data	Home address, email address, phone number	Communication, dissemination, exploitation activities. Validation activities. Administration activities.

Table 6: Processing of personal data

5.2.1 Principles for Data Protection

Research and administrative activities will be compliant with the principles relating to the processing of Personal Data, according to Article 5 of the GDPR:

- Lawfulness, fairness and transparency in relation to the data subject;
- Purpose limitation: Personal data were collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- Data minimisation: Personal data were adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accuracy: Personal data were accurate and, where necessary, kept up to date; data were not modified or falsified.
- Storage limitation: Personal data were 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;
- Integrity and confidentiality: Personal data were processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- Data protection by design and by default: The controller implemented appropriate technical and organisational measures which are designed to implement data-protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to protect the rights of data subjects. The controller implemented appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed;
- Accountability: The controller is responsible for and is able to demonstrate compliance with the above-mentioned principles.

5.2.2 Purposes and legal basis for the processing of personal data

Personal data are processed on a lawful basis, as provided by reg. EU 2016/679, Articles 6 and 9. Notably, the processing of personal data is based on consent (for common personal data) and explicit consent (for special categories of personal data).

Consent of the data subject has to be freely given, specific and informed. As anticipated, for the sake of conciseness, the data subject's consent is given in the context of a written declaration which also concerns other matters. Nonetheless, the request for consent to the processing of personal data is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

As requested in Article 7 of the GDPR, the responsible parties are able to demonstrate that all data subjects have consented to the processing of their personal data.

Explicit consent is obtained before processing special categories of personal data, such as neurophysiological data.

According to the Working Party Article 29 Guidelines on Consent, consent of the data subject means any:

- freely given,
- specific,

- informed and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

The responsible parties will also ensure the so-called “granularity” of consent, intended as follows: «a service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes» (Working Party Article 29 and European Data Protection Board (EDPB) Guidelines, p. 3.1.3).

Prior to obtaining their consent, participants to project activities will be always provided with information listed in Article 13, reg. EU 2016/679, and with any communication under Articles 15 to 22 and 34, reg. EU 2016/679 relating to processing the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

In all the activities, no personal data will be processed without informed, specific, explicit consent of the data subjects.

The main user groups targeted are professionals working in the aviation and technology development domain (e.g., members of industry and government, academics, researchers, etc.). Engaged stakeholders had the competence to understand written and oral informed consent information.

For the sake of clarity, it is relevant to remark that the research at issue does NOT include children, adults unable to give informed consent, nor vulnerable individuals/groups.

5.2.3 Rights of Data Subjects

The General Data Protection Regulation provides a set of rules for the protection of the fundamental rights of the data subjects, listed in Chapter III of the GDPR. This section contains a selection of the provisions of the law applicable to the case and peculiarities of research activities.

- **Right to information** (Articles 13 and 14)

According to the Reg. EU 2016/679, the controller has to take appropriate measures to provide any information relating to processing the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

With regard to the project activities, the data subject has the right to be informed at least about:

- the identity and the contact details of the controller;
- the contact details of the data protection officer;
- the purposes of the processing and the legal basis for the processing;
- the recipients or categories of recipients of the personal data;
- the intention of the controller to transfer personal data to a third country or international organisation;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject as well as the right to data portability;
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Right of access (Article 15)

The data subject has the right to obtain from the controller confirmation as to whether or not his/her personal data are being processed and access to the personal data and the basic information about the processing, such as the purposes, the categories of personal data processed, the possible recipients of data, even in third countries, the retention period, the existence of data subject's rights, the right to lodge a complaint to the supervisory authority, the existence of automated decision-making, including profiling, the source of data, when they have not been collected from the data subject.

Article 13 states that the controller has to provide to the data subject a copy of the personal data undergoing processing.

- **Right to rectification (Article 16)**

The data subject has the right to ask the controller for the rectification of inaccurate personal data concerning him/her.

- **Right to erasure (Article 17)**

With regard to the activities, the data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent and where there is no other legal ground for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

The above-mentioned rules do not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

According to Article 17, par. 2 of the GDPR “Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data”.

The above-mentioned rules do not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
 - for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
 - for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
 - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
 - for the establishment, exercise or defence of legal claims.
- **Right to restriction of processing (Article 18)**

The data subject has the right to obtain from the controller restriction of processing when the accuracy of his/her personal data is contested, for a period enabling the controller to verify the accuracy of the personal data, when the processing is unlawful, when the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; when verification is pending about the right to object.

Article 18 states that where processing has been restricted such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

- **Notification about rectification, erasure, restriction (Article 19)**

The controller has to communicate any rectification, erasure or restriction of processing personal data carried out to each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort.

- **Right to data portability (Article 20)**

As personal data are collected on the legal basis of consent, the data subject has the right to receive his/her personal data in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided.

The data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

- **Rights about automated individual decision-making, including profiling** (Article 22)

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless the processing is based on consent.

- **Communication of a personal data breach** (Article 34)

According to Article 34 of GDPR “When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller has to communicate the personal data breach to the data subject without undue delay”.

- **Exercise of data subject rights** (Article 12)

The data subject shall contact the controller and submit a request by sending an email to the contact point mentioned in the consent form.

The requested information will be provided to the data subject without undue delay and in any event within one month of receipt of the request.

Such a period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

The controller will inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

If the controller does not take action on the request, the data subject will be informed without delay and, at the latest, within one month of receipt of the request of the reasons for not taking action and the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

The controller prepared an internal policy to manage requests of data subjects in accordance with the GDPR.

5.2.4 Security Measures, Data Storage, Data Retention, Data Destruction, Data Breaches

According to Article 24 of the GDPR, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation itself.

The Consortium and its members are committed to ensuring the effective protection of the personal data of all participants in its activities. The processing of personal data does not involve data transfers towards non-EU countries with inadequate levels of protection.

- **Security measures for the protection of personal data**

The Consortium and its members are committed to implementing appropriate technical and organisational measures to guarantee in an effective manner the necessary safeguards for the processing of personal data. Article 32 of the GDPR recommends pseudonymisation and encryption of personal data as security measures which should ensure a level of security appropriate to the risk of processing.

Pseudonymisation and other security measures will be implemented in full compliance with the most recent rules, opinions and guidelines from European and national competent Authorities.

No data, which is not strictly necessary to accomplish the current study, will be collected; data minimisation policy will be adopted at any level of the study and will be supervised by the DPO and the EM of the study; any shadow (ancillary) personal data obtained in the course of the observation will be immediately cancelled.

Data presented in publications or to employers will be aggregated data only, in which individuals cannot be identified. Pictures, videos and audio will be recorded only after the signature of a detailed information sheet and consent form (see Annex 1). For audio files, no name of the participant, facilities, or companies will appear on the audio files. The audio and videos will not be used for any different purposes, nor disclosed to any third party and will be destroyed 2 years after the end of the project.

All the researchers involved in empirical studies and data collection activities will be trained about social, ethical, legal, and privacy issues and about current regulations.

- **Data storage**

Data may consist of digital or/or paper data. Digital data will be stored on hard disks disconnected from the network, stored in secured drawers; and/or on secured servers, with a defined protocol that limits access to authorised personnel.

The latest encryption techniques will be applied to all digital data.

Paper data will be stored in secured drawers with limited access to authorised personnel.

- **Data retention**

Project documentation, including technical documents describing the results of research activities, will be archived after the end of the project in password-protected servers.

- **Data destruction**

Data will be destroyed 2 years past the termination of the project. Paper data will be physically destroyed. Digital data will be overwritten to ensure that they are effectively scrambled and remain inaccessible.

- **Data breaches**

In the case of a personal data breach, the controller will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with GDPR rules, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The controller prepared an internal policy to manage the event of a data breach in accordance with the GDPR. Every person affiliated with one of the project beneficiaries has to report a suspected data breach to the following email address without undue delay to the DPO of the project.

5.2.5 Transfers of personal data to third countries or international organisations

Research activities involve connection with non-EU organisations, in particular the consortium includes Cranfield University, a partner from UK. Personal data might be imported from non-EU to EU. Non-EU countries will be required to comply with the legal and ethical requirements for participation in EU research and Horizon Europe guidelines.

6 Ethics

Although the U-AGREE project does not require specific ethical procedures to be implemented, all project activities will adhere to fundamental principles such as dignity, freedom, equality, solidarity, citizens' rights, and justice. Compliance with national, EU, and international ethical standards and regulations will be ensured throughout the project.

Participants involved in U-AGREE activities will be adults who do not belong to vulnerable groups and who voluntarily choose to take part. Full transparency will be maintained regarding the use of personal data, images, and videos, ensuring that participants receive clear and complete information before giving their consent. Any event organised within the project, such as workshops, webinars, or interviews, will only involve volunteers who have been thoroughly informed about the project's objectives and activities. The project will not engage children or individuals unable to provide informed consent.

Participation in U-AGREE activities will be governed by the following principles:

1. Participants have the right to remain anonymous.
2. Personal data will be handled in accordance with national data protection laws and the GDPR of the European Commission.
3. Any data provided by participants will be treated with strict confidentiality.
4. Free and informed consent will be obtained from all participants, including for interviews. This process ensures that individuals fully understand the purpose, procedures, and potential outcomes of their involvement before making a voluntary decision to participate.
5. Participants have the right to be informed about who will benefit from their involvement in the project and, if applicable, to be notified of any commercial applications resulting from research activities involving their contributions.

All consortium partners will be responsible for ensuring that consent forms are properly collected from every individual taking part in the project.

7 Other issues

For any aspect not explicitly covered by the current document, U-AGREE will process data complying with GDPR and other local legislations respecting the following provisions:

- Compliance with institutional, national, and European legislation. The protection of data collected during U-AGREE research studies will comply locally with the participants' policies and funding programme guidelines.
- Each partner will process only the data necessary for the project specified purposes, and will make sure that they keep data accurate, up to date, and retained only for as long as is deemed necessary for the purpose of the collection and process thereof.
- Each partner will choose, for the data processing, employees with relevant professional qualifications, providing sufficient guarantees in terms of technical expertise and personal integrity to ensure such confidentiality. For data processing being carried out on behalf of the Controller, by other members of the Consortium, the relevant assignment will be made in writing.
- Each partner of the U-AGREE project will be responsible for the correct implementation of data protection procedures for its own organisation.

8 Annex 1 – U-AGREE consent form (template)

U-AGREE

Informed consent for [activity]

About this notice

- This Consent Form is addressed to interviewees involved in U-AGREE.
- The document aims to provide relevant information about the research activities that may require the processing of personal data.
- The document also aims to record the participant's consent to take part in research activities and the necessary processing of personal data.

About Travel Wise

- U-AGREE is an EU-funded research project (GA no. 101167187).
- U-AGREE will develop an integrated risk model linking the operations of unmanned aircraft (UAS) with some negative effects they may have with regard safety, security, privacy and environment. This risk model is intended to support the airspace risk assessments required by U-space European regulation as well as an amendment to SORA methodology so that risk can be quantitatively estimated, enabling digital implementations leading to swifter operational approval processes.
- A more accurate description of [project]research activities is available on the dedicated webpage: [website]

About your participation in [activity]

- This [activity] is part of the U-AGREE project and is administered by UPV for research activities related to the project.
- This [activity] aims to [purposes, aims and objectives]
- The [activity] does not have any commercial purpose. The involved participants do not receive any monetary benefits by conducting this activity. They participate on a voluntary basis and can withdraw from the activities at any time.
- The [activity] results may be published in project reports, journal articles, conference presentations, and via any other mode of scientific exchange and dissemination considered appropriate while protecting the participants' anonymity.

About the protection of your personal data

- This [activity] may involve the collection of your personal data [categories of data] also by means of [means]
- The controller of the related processing activities of your personal data is [responsible], on behalf of the Consortium of U-AGREE.
- As a participant, your personal data (e.g., [categories of data]) will be used by [project] only.

- The purposes of the processing within the project concern the [WP+T]. In particular, the [activity] aims to [purposes, aims and objectives].
- The personal data collected will be analysed separately and anonymously. The only exception may concern contact information, which could be furtherly used only with your free, explicit and withdrawable consent.
- The retention period of personal data collected by this interview will be no longer than ***. At the end of this period, data will be processed only if anonymised, with the only exception of contact information (see § 15).
- The [activity] results may be published in project reports, journal articles, conference presentations, and via any other mode of scientific exchange and dissemination considered appropriate while protecting the participants' anonymity. Data collected will be published in an anonymous form.
- [Audio recordings, photos and videos - i.e., means] taken during the [activity] may be used for scientific and dissemination purposes, while protecting the participants' anonymity and in respect of the consent provided.
- Personal data will be collected, processed and protected according to the General Data Protection Regulation (GDPR) (EU) 2016/679. Participants will have the right to request access to and rectification or erasure of personal data or restriction of processing concerning the data or to object to the processing as well as the right to data portability by sending an email to the responsible for data treatment listed hereafter. They will also have the right to lodge a complaint with a supervisory authority.

About U-AGREE contact points for these research activities

In case you need any further information about the above-mentioned research activities, the processing of your personal data or the exercise of your rights (§ 19), please, contact the following officer

Name and email address

- **Informed consent**

After reading the information sheet above and obtaining a copy of it,

Name and Surname of participant: _____

Organisation: _____

E-mail address: _____

I voluntarily provide my consent to participate in this [activity], aware that I can refuse to answer questions, and I can withdraw from the interview at any time, without having to give a reason.

- **Signature** _____

Moreover, I provide my consent to the processing of my personal data for the following activities:

	YES	NO
--	-----	----

to be audio recorded in order to ease my inputs to the [activity]		
to be present in the pictures/videos of the [activity]		

• **Signature** _____

Date: _____