EVENFLOW

Robust Learning and Reasoning for Complex Event Forecasting

Project Acronym:	EVENFLOW
Grant Agreement number:	101070430 (HORIZON-CL4-2021-HUMAN-01-01 – Research and Innovation Action)
Project Full Title:	Robust Learning and Reasoning for Complex Event Forecasting

DELIVERABLE

D1.2 – Data Management Plan

Dissemination level:	PU - Public, fully open
Type of deliverable:	DMP - Data Management Plan
Contractual date of delivery:	31 March 2023
Deliverable leader:	INTRA
Status - version, date:	Final – v1.0, 2023-03-29
Keywords:	Data management handling plan, FAIR, Data storage, Data processing, Quality control, Data security, GDPR

Funded by the European Union

This document is part of a project that is funded by the European Union under the Horizon Europe agreement No 101070430. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Commission. The document is the property of the EVENFLOW project and should not be distributed or reproduced without prior approval. Find us at www.evenflow-project.eu.

Executive Summary

This document serves as a report that a) provides an overview of the datasets generated and used in the context of the EVENFLOW project and the use cases, b) outlines how data will be generated and/or collected and processed, subject to all relevant regulations, c) assesses, on top of the methodology and standards to be introduced, whether and how this data will be shared as FAIR (Findable, Accessible, Interoperable and Reusable) and how it will be curated and preserved, in direct alignment with the ethics requirements.

More specifically, the EVENFLOW Data Management Plan (DMP) unifies and organizes the project's activities, processes, and procedures to enable a data management methodology that is appropriate for the project's needs, timeline, and scope. This is done by looking at the data that is now available and pertinent to the EVENFLOW operations, as well as their lifecycle and all other connected rules for treating them fairly (conventions, openness, metadata, reusability, etc.). Through an agreed-upon comprehensive policy for handling all data within the project's activities and across all the project's WPs (Work Packages) and tasks, EVENFLOW will fully adhere to and respect GDPR (General Data Protection Regulation) policies.

The DMP will be formulated and delivered in M6 of the project. Nevertheless, since the DMP is expected to mature during the project, it will constitute a living document to be updated regularly. INTRA will lead the activity, while all data provision partners will invest effort in safeguarding the proper data management.

Deliverable leader:	Dimitrios Liparas (INTRA)
Contributors:	All
Reviewers:	Nikos Katzouris (NCSR), Nikos Giatrakos (ARC)
Approved by:	Athanasios Poulakidas (INTRA)

Document History			
Version	**Date**	**Contributor(s)**	**Description**
0.1	2023-01-16	D. Liparas, A. Poulakidas	Initial ToC
0.2	2023-02-18	All	First draft version
0.3	2023-03-16	All	Complete draft version for internal review
0.4	2023-03-24	N. Katzouris, N. Giatrakos, D. Liparas, A. Poulakidas	Internal review updates
0.5	2023-03-28	D. Liparas	Consolidated version accepted by reviewers
1.0	2023-03-29	A. Poulakidas	QA and final version for submission

Table of Contents

List of Tables

Definitions, Acronyms and Abbreviations

Acronym/ Abbreviation	**Title**
AE	Affiliated Entity
AGV	Automated Guided Vehicles
AI	Artificial Intelligence
AP	Associated Partner
BRCA	BReast CAncer gene
CO	Coordinator
DMP	Data Management Plan
DOI	Digital Object Identifier
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EC	European Commission
FAIR	Findability, Accessibility, Interoperability, Reusability
GA	Grant Agreement
GDPR	General Data Protection Regulation
LCA	Life Cycle Assessment
ML	Machine Learning
PM	Personalized Medicine
WP	Work Package

1 Introduction

1.1 Project Information

EVENFLOW is developing hybrid learning techniques for complex event forecasting, which combine deep learning with logic-based learning and reasoning into neuro-symbolic forecasting models. The envisioned methods combine (i) neural representation learning techniques, capable of constructing event-based features from streams of perception-level data with (ii) powerful symbolic learning and reasoning tools, that utilize such features to synthesize high-level, interpretable patterns of critical situations to be forecast.

Crucial in the EVENFLOW approach is the online nature of the learning methods, which makes them applicable to evolving data flows and allows to utilize rich domain knowledge that is becoming available progressively. To deal with the brittleness of neural predictors and the high volume/velocity of temporal data flows, the EVENFLOW techniques rely on novel, formal verification techniques for machine learning, in addition to a suite of scalability algorithms for federated training and incremental model construction. The learnt forecasters will be interpretable and scalable, allowing for fully explainable insights, delivered in a timely fashion and enabling proactive decision making.

EVENFLOW is evaluated on three challenging use cases related to (1) oncological forecasting in precision medicine, (2) safe and efficient behaviour of autonomous transportation robots in smart factories and (3) reliable life cycle assessment of critical infrastructure.

Expected impact:

- New scientific horizons in integrating machine learning and machine reasoning, neural, statistical and symbolic AI
- Breakthroughs in verification, interpretability and scalability of neuro-symbolic learning systems
- Interpretable, verifiable and scalable ML-based proactive analytics and decision-making for humans-in-the-loop and autonomous systems alike
- Robust, resilient solutions in critical sectors of science and industry
- Accurate and timely forecasting in vertical sectors (healthcare, Industry 4.0, critical infrastructure monitoring)
- Novel FAIR datasets for scientific research
- Novel resources and approaches for verifiable, interpretable, scalable and knowledge-aware machine learning

Table 1: The EVENFLOW consortium.

Number[1]	Name	Country	Short name
1 (CO)	NETCOMPANY-INTRASOFT	Belgium	**INTRA**
1.1 (AE)	NETCOMPANY-INTRASOFT SA	Luxemburg	**INTRA-LU**

[1] CO: Coordinator. AE: Affiliated Entity. AP: Associated Partner.

Number[1]	Name	Country	Short name
2	NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS"	Greece	**NCSR**
3	ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS	Greece	**ARC**
4	BARCELONA SUPERCOMPUTING CENTER-CENTRO NACIONAL DE SUPERCOMPUTACION	Spain	**BSC**
5	DEUTSCHES FORSCHUNGSZENTRUM FUR KUNSTLICHE INTELLIGENZ GMBH	Germany	**DFKI**
6	EKSO SRL	Italy	**EKSO**
7 (AP)	IMPERIAL COLLEGE OF SCIENCE TECHNOLOGY AND MEDICINE	United Kingdom	**ICL**

1.2 Document Scope

This deliverable aims at collecting all data that will be handled by consortium partners in the frame of the EVENFLOW project.

The document will be maintained as online live page(s) within the project DMS throughout the project lifecycle.

1.3 Document Structure

This document is comprised of the following chapters:

Chapter 2 describes the initial datasets that the project has identified at the outset.

Chapter 3 outlines the project's strategy for making data FAIR, both internally and externally.

Chapter 4 describes the project's internal procedures for storing, exchanging and monitoring data.

Chapter 5 provides some concluding remarks.

Appendix A lists the project data assets and their characteristics.

Annex 1 provides a consent form template to be used in EVENFLOW when needed. The form can be adapted to consent to a variety of activities.

2 Data Summary

We define the concepts and goals of data collection in this chapter of the Data Management Plan, in relation to the organizational framework of the EVENFLOW project. Following discussions with the EVENFLOW WP leaders, we have identified the following data points:

- Means of data collection.
- Types of data that will be collected.
- Data formatting.
- Predictions of data size and growth rate.
- Reproduction and re-usability of data (whenever applicable).
- Data versioning and control to align data, after modifications to the data.
- Tools and software for generating/modifying/processing data.

A definition and description of the data that will be created/distributed with the EVENFLOW project are provided below. The data can be categorized as:

- Scientific data relating to the 3 EVENFLOW use cases.
- EVENFLOW project management and project-related documentation, reporting and management files.
- Dissemination and communication documents.

All EVENFLOW data files may include numbers, images, software codes, audio files, video files, internal/external reports, etc. The structure of this chapter complies with the FAIR data management template of the EC.

In the chapters that follow, the data collection within the EVENFLOW project is defined, along with the purpose of the collected data and how it relates to the objectives of the project. Several potential data assets have been identified after the project’s initial round of analysis. These data assets will serve as the project's first input for continuous data management. In addition, these data assets will not only be collected, stored, and shared as planned; they will also be utilized as models to find new data assets, as the project progresses.

2.1 EVENFLOW Data Lifecycle

The full information life cycle that will be considered in the EVENFLOW project is examined in this chapter, considering the many points at which information will be created, managed, or used throughout the implementation of the project. The next step is to look at the information life cycle and the methods for managing, controlling, and reporting the relevant information.

2.1.1 Data Creation/Collection

This stage addresses the data creation and/or collection, as it relates to the various data assets provided by the EVENFLOW use cases, in addition to project reports and other documents. Within this stage, the creation and/or collection of data by each respective owner, in appropriate formats and layouts, is included, something that will allow for their processing by the other project elements. Some metrics that are related to this stage are presented below in Table 2.

Table 2: EVENFLOW Data Creation/Collection Indicators.

Performance Indicator	Means of Verification	Target Values
Format	Compliance with existing standards of data exchange	XLS, XML, etc.
Availability and Readability	Whole data package available, non-corruption, whole percentage collected	100% received 100% accessible
Fit for Use	Data follow data compliance for proper processing and review	100% usable by intended beneficiary/ies
Consistency and Completeness	Data are consistent and complete for the intended purpose	Including 100% of information for the intended purpose
Relation	Data processing follows a precise relation to their collection purpose	100% purpose precision

2.1.2 Data Processing and Analysis

The various data processors (the partners that will have access to the project data for processing or dissemination activities) are involved in this stage. In order to meet the objectives of EVENFLOW, we need to make sure that the appropriate partners can handle data in a concise manner. Every step towards data verification, organization, transformation, integration, and extraction is included in this stage. Data analysis refers to all actions carried out on the actual data, describing existing facts, identifying patterns, creating data clarifications, etc. This stage develops as a result of the processing stage that was previously mentioned and is closely related to it. Table 3 below presents a list of related indicators.

Table 3: EVENFLOW Data Processing and Analysis Indicators.

Performance Indicator	Means of Verification	Target Values
Data logic	Data are processed following a concise logic and approach	New and processed data follow precise data logic
Organization and Utility	Suitable content organization of data under processing	100% organized data
Validation	Ensuring that the data under processing are correct and relevant	100% validated and relevant data

Performance Indicator	Means of Verification	Target Values
Aggregation	Whenever multiple data need to be aggregated, ensure that this is done in a concise fashion	100% documented and concise aggregation of data
Transformation	Transformation of data to the proper format(s) for processing	100% of data ready for processing (transformed if needed)
Calibration	Data checked against empirical values or other similar data	Data properly calibrated

2.1.3 Data Publication and Utilization

While data utilization encompasses the phases leading up to data sharing (internally to EVENFLOW), data publication refers to the ability to share data openly to the public. This indicates that data should be independent of medium and agent to enable automatic implementation of the transfer. In order to ensure protection of proprietary data and the integrity of the data itself, this stage aims to make sure that data is shared with the necessary controlling mechanisms. As far as metadata are concerned, this stage is closely related to the next stage (data storage and reuse). A list of relevant indicators is provided below in Table 4.

Table 4: EVENFLOW Data Publication and Utilization Indicators.

Performance Indicator	Means of Verification	Target Values
Means-independent	Data are transferred in means-independent standard formats and/or accessed by means-independent and widely available tools (e.g. open-source)	100% means-independent transferability
Security	Data stored in a secure repository	At least access control provided

2.1.4 Data Storage and Reuse

Since it relates to data access, sharing, storage, archiving (including search capabilities) and reuse, the storage stage is considered to be very critical. The updated status of the data, which ensures that no newer versions exist, is a crucial consideration in this case. In addition, there should be procedures and practices in place to protect data from unauthorised access, corruption and unintentional loss. Data reusability, which falls under the purview of FAIR data treatment, is also closely related to data storage. Table 5 provides a list of associated indicators.

Table 5: EVENFLOW Data Storage and Reuse Indicators.

Performance Indicator	Means of Verification	Target Values
Up-to-date	Ensuring that the stored data are up-to-date for the specific purpose and no later version exists	100% updated
Retention	Properly setting expiration dates for all data, after which the data will be deleted	Expiration date provided

2.2 Types of Data Assets

In the following subsections, the types of data assets that have been identified as most relevant to EVENFOW, are presented and described.

2.2.1 Research Data

Description: The three EVENFLOW use cases, namely “Use Case I: Industry 4.0”, “Use Case II: Personalized Medicine (PM)” and “Use Case III: Infrastructure Life Cycle Assessment (LCA)” will involve AGV (Automated Guided Vehicles) training datasets (sensor data of the AGV (timeseries, camera feed, pointclouds, etc.)), BRCA (BReast CAncer gene) time interpolation datasets (inferred changes in gene expression during breast cancer progression), as well as SMART PIPE datasets (data gathered from sensors placed within the pipe), respectively. In addition, some surrogate datasets will be used, either because their characteristics resemble those of the use case datasets or because they constitute standard benchmarks for proving the effectiveness of the algorithmic techniques that will be developed in EVENFLOW.

Data utility: The various types of data will be used by the EVENFLOW partners for the research, development and evaluation activities of the project’s use cases. Outside of the project, the data can be useful for research purposes to: (i) researchers in robotics AI and computer vision (Use Case I), (ii) researchers in biomedical domain, biotech and pharma companies (Use Case II), and (iii) water/sewer management companies, maintenance companies, public administrations, pipe manufacturers, etc. (Use Case III).

Data format: CSV will be the common format for such data, but other formats will also be considered (e.g. PCD, IMG, DB3, JSON etc.).

2.2.2 Stakeholder Data

Description: Part of the project work will involve the collection of end users' & system requirements, as well as social data obtained in the context of the ancillary social events (open surveys, workshops etc). No personal or sensitive data will be included in the data assets.

Data utility: The data will be used for the design and development of the EVENFLOW integrated system and software components. They will also be the reference for the exploitation and dissemination activities of the project results. For external users, the data can be used for analysing the stakeholders' involvement in EVENFLOW's adoption in market applications.

Data format: The data will be stored in their original format, along with generated PDF files that will be used for external distribution.

2.2.3 Project Management Data

Description: During the implementation of the EVENFLOW project, the project management team, but also all consortium partners, will create project management data, in the form of internal documents (project operation documents) used to monitor the progress of the project, such as deliverables, presentations, meeting agendas and minutes, internal reports, etc.

Data utility: The data will be used as reference for the day-to-day operation of the project.

Data format: Office documents (.docx, .pdf, .pptx, .xlsx, latex), agenda items (.ics), photos, etc.

2.3 DMP in EVENFLOW Work Packages

Data management in EVENFLOW is the responsibility of Task 1.4 "Data Management Plan" [M1-M36] (Leader: INTRA). This defines the technically sound, legally compliant and ethically justifiable data collection, use and sharing conditions that apply to the consortium partners and all data sets that are generated and used for developing the proposal objectives throughout the data lifecycle as deployed in the EVENFLOW use cases. The DMP shall describe all relevant technical and organisational policies, processes, safeguards and controls, as part of the project's legal compliance and ethics alignment plan, in the context of the use cases. On top of that, it aims to contribute to legitimate downstream data uses of personal data, subject to the GDPR and the Data Governance Act, as well as non-personal data, subject to Regulation 2018/1807 on the free flow of non-personal data and the Data Governance Act.

To ensure compliance with all the previously described data management decisions as they relate to the DMP, the following measures will apply to EVENFLOW:

- Work Package (WP) leaders will be responsible for adhering to the specifications above in their respective WPs.
- The project manager of each organization will be responsible for the DMP actions and will be accessible by the partner team, in case of issues related to the DMP.

- The project manager of each organization should ensure that personnel working on the project have read the EVENFLOW DMP and will apply all principles, as described in this document.
- Data owners have the ultimate responsibility to comply with the specifics of the EVENFLOW DMP, as well as with the related GPDR policies.
- For the overall EVENFLOW project management activities, INTRA (as the Project Coordinator) will be responsible for complying with the DMP.

3 Making Data FAIR

According to the FAIR (Findability, Accessibility, Interoperability, Reusability) principles, research results should be organized in a way that makes them more accessible, understandable, exchangeable, and reusable. FAIR data are encouraged by major funding bodies, such as the European Commission (EC), in order to maximize the integrity and effect of their research investment. Fair data management pertains to the EC recommendations for Findable, Accessible, Interoperable and Reusable data. The structure of this chapter complies with the EC's FAIR data management template[2].

3.1 Making Data Findable

To make data findable, EVENFLOW will assess, as well as use, standard services, such as B2SHARE[3] or equivalent, in making sure that appropriate metadata[4] are created. Metadata will be extracted, if possible automatically, following community standards. For datasets generated by the use cases, field experts may prefer to provide human-generated metadata where appropriate.

3.2 Making Data Accessible

Regarding peer-reviewed scientific publications related to the results of the EVENFLOW project, they will be published as open access, in accordance with the EVENFLOW Grant Agreement (GA). This includes the obligation to:

- deposit a machine-readable electronic copy of the published version or final peer-reviewed manuscript accepted for publication in a repository for scientific publications, together with the research data needed to validate the results presented in the deposited scientific publication as soon as possible.

Open access to the deposited publication via the repository must be ensured at the latest:

- on publication, if an electronic version is available for free via the publisher, or
- within six months of the publication (twelve months for publications in the social sciences and humanities domains) in any other case.

Open access via the repository on the bibliographic metadata that identifies the deposited publication must be ensured. It must be provided in a standard format and must include:

- the terms “European Union (EU)” and “Horizon Europe”;
- the name of the action, acronym and grant number;
- the publication date and length of the embargo period, if applicable, and
- a persistent identifier.

[2] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/temp-form/report/data-management-plan_he_en.docx

[3] https://b2share.eudat.eu/

[4] http://rd-alliance.github.io/metadata-directory/

With respect to research data, they will be made available to the extent possible and in accordance with the EVENFLOW GA. Regarding use case-specific data, as it is not yet exactly clear which data will be generated throughout the use cases, at this point it cannot be stated which of the retrieved data will be made publicly available. With respect to (sensitive) personal data, it should be noted that in the medical use case, any real patient data used for training are anonymized and will be made publicly available. Nevertheless, some data that are sensitive to the business of the use case providers will be protected. Finally, regarding stakeholder-related data, they will not be made openly available, as they mostly contain personal information. Nevertheless, anonymized results from workshops and other stakeholder engagement events will be made openly available through related deliverables.

The datasets produced in EVENFLOW will be made openly available via related platforms and repositories, such as Zenodo and OpenAIRE, accompanied by appropriate documentation and description of the data features and related metadata. It should be noted that Zenodo is an open-access repository developed under the European OpenAIRE program operated by CERN, which provides researchers the sharing, curation and publication of data and software. The OpenAIRE project was commissioned by the EC to support their nascent Open Data policy, by providing a catch-all repository for EC-funded research. It should be noted that with respect to data versioning, Zenodo automates the process by assigning to every publicly available upload a Digital Object Identifier (DOI), in order to make the upload uniquely citeable.

3.3 Making Data Interoperable

Data interoperability standards from the biomedical[5][6][7][8], industry 4.0[9] and manufacturing[10] domains will be employed in EVENFLOW to ensure that the data generated from the EVENFLOW use cases adhere to the interoperability requirements imposed by the respective domains.

3.4 Making Data Reusable

The data generated in EVENFLOW will be shared following CC-BY licences, which boost their reusability by guaranteeing that the data are free to be reused, while maintaining the traceability of the use and credit attribution to the data providers. In case data are produced or used with proprietary software (e.g. of use case partners), alternative and compatible open source tools will be suggested in the documentation accompanying the respective datasets. The data that will be shared on open data repositories will be linked to corresponding research publications on the project’s website and will be updated, subject to their use in follow-up research extending EVENFLOW.

[5] https://ihec-epigenomes.org/

[6] https://dcc.icgc.org/

[7] https://human-microbiome.org/

[8] https://www.matchmakerexchange.org/

[9] https://www.iiconsortium.org/IISF/

[10] https://www.mimosa.org/

4 General Data Protection Regulation (GDPR)

This section summarizes the GDPR compliance of EVENFLOW. The GDPR was formally introduced in May 2018 and has been applicable in all Member States in the European Union, as well as in the countries in the European Economic Area (EEA).

4.1 GDPR compliance

Data confidentiality is an overriding concern throughout the EVENFLOW project and beyond, as the solution to be developed in EVENFLOW will continue to be used afterwards. To this end, EVENFLOW aims to be fully compliant with the GDPR. All stakeholder data that will be used in the project will be collected in accordance with applicable ethical standards and requirements in the countries involved in the data collection, and will be processed and handled in a secure way, in line with applicable rules and regulations on privacy and data protection.

4.2 General Data Protection Policy

The subsections below provide and describe the EVENFLOW Policy for General Data Protection.

4.2.1 Introduction

This General Data Protection Policy (the "**Policy**") is drafted by INTRA (the "**Project Coordinator**") with regard to the EU Horizon Europe Project EVENFLOW Grant agreement ID 101070430 (the "**Project**") executed by the list of partners included therein (the "**Project Partners**") in order to:

- Comply with the policy and legal requirements of the EU General Data Protection Regulation (Regulation EU 2016/679, the "**GDPR**")14, as in effect since 25 May 2018;
- Comply with all other applicable national and EU regulations and guidelines on personal data processing;
- Comply with applicable regulations and best practices with regard to research projects within the EU HE Research Programme;
- Raise awareness and improve knowledge among the Project Coordinator, the Project Partners, as well as their employees and/or agents and/or contractors (collectively, the "**Policy Recipients**").

Because the field of data protection is a dynamic legal field of constant change, new developments, in the form of new regulations, official reports and/or guidelines, are issued by EU and national legislators, as well as competent national authorities at a constant pace. In this context, this Policy may need to be periodically updated by the Project Coordinator, in order to remain relevant to legislative change. Accordingly, Policy Recipients will be duly informed, and will be asked to provide their renewed consent upon any such updates.

4.2.2 Definitions

For the purposes of this Policy the GDPR definitions, as set in Article 4, apply. In addition, “**Personal data**” means any information relating to an identified or identifiable natural person that is processed by any Project Partner and Policy Recipient during execution of the Project.

“**Controller**” means the owner of the personal data (usually the creator of the data itself), unless otherwise expressly clarified in this Policy or elsewhere in Project deliverables and/or reports.

“**Processor**” means each Project Partner, unless otherwise expressly clarified in this Policy or elsewhere in Project deliverables and/or reports.

“**Consent**” of the data subject means any freely given, specific, informed, unambiguous and in writing 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.

“**Supervisory authority**” means the competent Data Protection Authorities within the Project Partners’ jurisdictions.

The aim of the above definitions is to particularise and complement the definitions of Article 4 of the GDPR. Policy Recipients are advised to consult both texts in order to formulate the applicable definitions each time.

4.2.3 Policy Scope

The Controller determines in advance what is the law applicable to the processing of personal data in a particular case, considering that according to EU law such determination comes from legal principles and cannot be derogated by the parties.

4.2.3.1 Establishment

Each Project Partner is established on the territory of EU Member States. In the event of any change in establishment, the respective Project Partner shall notify the Project Coordinator duly and in writing.

Unless otherwise expressly specified, each Project Partner is considered the Controller in that Member State.

4.2.3.2 Processor outside the EU

In the event of any subcontracting to an organization not established on EU territory (such as subsidiaries pertaining to the same corporate group) that processes personal data of people staying on EU territory, on behalf of a Project Partner, that organization qualifies as Processor and ensures the fulfilment of the obligations imposed by the GDPR for that specific part of processing.

4.2.4 Personal data processing

The subsections that follow describe the policy relating to personal data processing. For consistency and completeness, it should be noted that in the EVENFLOW project, there is no processing of personal data whatsoever.

4.2.4.1 Personal data

Personal data means any information relating to natural persons, which is or can be identified, even indirectly, by reference to any other information including a personal identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special categories of data

Special categories of personal data include data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or data concerning a natural person's sex life or sexual orientation as well as the processing of genetic data and biometric data for the purpose of uniquely identifying an individual.

In the event of such processing, the Controller and/or Processor should follow special rules related to, such as acquiring specific informed consent from the data subjects and applying stricter safeguards.

When the Controller and/or Processor relies on the data subject's consent as a legal ground for processing special categories of data, they will meet all legal consent requirements; otherwise, the data may only be processed if and to the extent that it is based on one of the legal grounds listed in the GDPR for the processing of such data.

Data anonymization

Whenever possible, including non-detrimental to Project execution purposes, the Controller and the Project Partners shall undertake efforts to keep personal data processed by them for project purposes anonymous or pseudonymous.

According to the GDPR, “anonymous information” is information which does not relate to an identified or identifiable natural person, or personal data that are rendered anonymous in a way that the data subject can’t be identified. In this context, the GDPR does not apply to the processing of such anonymous information, including for statistical or research purposes.

Similarly, “pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Newsletters, social media and other dissemination material

Unless otherwise specified in the Project contract, the Controller shall be responsible for the personal data processing carried out for Project dissemination purposes. To this end, the Controller shall:

- Collect and keep all relevant personal data (including lists of contact details), or copies thereof;
- Monitor relevant communications;

- Issue to Project Partners instructions and guidelines on Project dissemination activities (including any EU or other state guidelines, whenever available);
- Inform the Project Partners of any policy or legal requirements, reviews and changes.

Minors

Processing of children's personal data requires a special legitimate basis. In the event of such processing the Controller shall be informed in advance and in writing by Project Partners.

4.2.4.2 Data processing

Data processing means any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organization, storage, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data.

4.2.4.3 Principles for legitimate processing

The European Union data protection law set forth the following specific principles which have to be complied with for the processing to be legitimate.

Pertinence and necessity - The Controller should implement management practices to fulfil the obligation to collect only relevant and necessary data for a specified purpose.

Purpose limitation - Personal data is collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The Controller has a clear overview of all purposes for which personal data is processed. Personal data is not processed for purposes besides the original purposes, unless the (secondary) use is compatible.

Data minimization - Personal data collected by the Controller must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and further processed; if the same purposes can be realized in a less data intensive way a preference is given to that method.

Data update - Personal data is accurate, and, where necessary, kept up to date. Every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Data retention - Personal data is kept in a form which permits identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed. The Controller and/or the Processor concerned should have processes and policies in place to:

1. determine what the applicable (minimum and maximum) retention periods are for the personal data that is being processed;
2. ensure that relevant retention periods are monitored.

4.2.5 Data protection legal roles

4.2.5.1 Controller

By determining the purposes and means of the processing of personal data, unless otherwise expressly specified in this Policy, the Controller is considered by law as the “Controller” and is the primary target of the provisions of the law.

Identification

The data Controller previously identifies itself as such and ensures an effective implementation of data protection measures, in order to comply with the principle that personal data are processed fairly and lawfully. The legal role of the Controller implies specific responsibilities because provisions setting conditions for lawful processing are essentially addressed to the Controller.

Accountability

The GDPR provides full accountability of the company/Controller regarding the compliance of its processing of personal data with the law. To ensure the effectiveness of that obligation, it prompts the Controller to follow an overall approach, achieving a genuine system of control and management of its pertinent information. So, accountability and compliance systems are elements of the framework for the protection of personal data, in the cause / effect relationship: to be compliant and able to prove it (accountability), the Controller needs to put in place a comprehensive compliance system.

Data protection by design

The Controller considers data protection issues from the outset and from the design of the Project, within the whole lifecycle of processing, in order to manage the issues in a proactive way, to reduce costs and improve efficiency.

Data protection by default

The Controller standardizes data protection principles in personal data processing, products and services. The measures adopted ensure that:

- personal data is processed for purposes not different from the original purposes,
- only data necessary for these purposes are collected, and
- data are not disclosed without human intervention.

4.2.5.2 Joint Controller

If at any time during the Project execution the Controller processes personal data in conjunction with a third party, by jointly determining the purposes and means of the processing, they both act as joint Controllers. Both joint Controllers determine the mutual responsibilities with a specific arrangement.

4.2.5.3 Processor

Unless otherwise specified expressly in this Policy, all Project Partners act as Processors during Project execution.

A processor processes personal data on behalf of the Controller – that is, the Controller delegates all, or part of the processing activities to them. In such an event the Project contract assumes the role of the relevant required written agreement as per GDPR requirements.

The Processor warrants that it shall provide sufficient guarantees to ensure compliance with the GDPR, has implemented appropriate controls to meet data protection requirements defined by the agreement, instructions and/or legal requirements and ensures the protection of the rights of data subjects.

Auditing

The Controller ensures the commitment of the Processor(s) to enable and contribute to any review activities, including inspections, conducted by the Controller or other (EU authorities') auditors and/or reviewers, as appropriate.

Security

Each Project Partner undertakes that it adopts appropriate security measures to ensure the security, integrity and confidentiality of personal information and electronic communications at an adequate level with regard to Project purposes, and at any event at no lower level than processing of similar data within its own organisation.

4.2.5.4 DPO

Whenever required, following applicable GDPR and Member State respective legal requirements, the Project Coordinator (INTRA), may designate a Data Protection Officer ("DPO") for assistance in monitoring internal compliance with the GDPR.

Identification

Each Processor appoints a DPO in accordance with the criteria and the requirements set forth in the GDPR, as applicable to it. In such an event, it shall notify the Controller in writing accordingly.

Designation compulsory vs. voluntary

Each Processor documents the reasons supporting the designation of the DPO or, rather, the reasons why such designation is deemed not necessary. This documentation forms part of the data protection documentation system of that Processor.

Professional requirements

The DPO has sufficient authority, professional qualities and independence to ensure success in his role, according to the GDPR provisions.

Tasks

The organization assigns to the DPO at least the tasks listed in the GDPR.

Notification to Supervisory Authority

Whenever a DPO is appointed, the organization notifies the Supervisory Authority of such designation and publishes DPO's contact details.

4.2.5.5 People in charge of processing

Individuals who process personal data under the authority of the Controllers or Processor(s) must receive specific formal instructions. Hence, the Controller gives specific instructions, relating also to the implementation of security measures and safeguards, to all its personnel in charge of processing personal data.

Training and awareness

All Project Partners' employees should be well informed and aware of data protection implications and be able to carry out their obligations in their work. A data protection education and communication program should be in place and supported by a monitoring system that confirms all employees and/or contractors are appropriately trained on their data protection responsibilities.

Policies and procedures

Data protection policies and procedures exist, are documented in writing, are formally approved by management, implemented, reviewed, updated and approved when there are changes to applicable laws and regulations.

All Project Partners understand, and the Controller may ask them to overview all their personal data processing, the data protection risks and the applicable rules and procedures. In such an event, they shall provide it with all requested information to the best of their ability without undue delay.

4.2.6 Notice and consent

In Annex 2, a consent form template that the EVENFLOW project has prepared and that can be adapted to any kind of activities, is provided.

4.2.6.1 Notice

Each Controller and/or Processor, as appropriate, provides the information required by law to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The data protection notice informs data subjects about the processing of personal data relating to them, even when the personal data is not collected from them as well as of their rights, in order to let them verify in particular the accuracy of the data and the lawfulness of the processing.

4.2.6.2 Free and informed consent

Personal data is processed if and to the extent that the data subject has given valid consent to the processing for one or more specific purposes, or another legal basis for processing exists.

Systems or applications are able to document the explicit consent of the data subject so that it can be evidenced at any time.

Other legal grounds for a legitimate personal data processing are the following:

- performance of a contract;
- legal obligation;
- vital interest of data subject;
- public interest;
- legitimate interest of the Controller or third party.

If "legitimate interest" is used as a basis, the interests that have preceded to the decision, need to be documented as well as any possible mitigating measures which will be taken to be able to proceed with personal data processing based on the defined interests.

4.2.6.3 Withdrawal of consent

Data subject's consent can be withdrawn at any time; even though it will not affect the lawfulness of processing based on consent before its withdrawal.

4.2.7 Rights of data subjects

The individual whom the data refers to (data subject) is entitled with specific rights set forth by the law. The GDPR requires that each Controller and/or Processor, as appropriate, must facilitate the exercise of the data subject's rights, take action on the request within a specific time frame and must communicate the information requested in an intelligible and easy to access form.

4.2.7.1 Right of access

Any individual must be able to exercise the right of access to data relating to him which are being processed.

4.2.7.2 Right to rectification

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request rectification of their personal data. The procedure specifies in which cases rectification is legitimate.

If a data subject's request for rectification is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

4.2.7.3 Right to erasure

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request erasure of their personal data. The procedure specifies in which cases erasure is legitimate.

If a data subject's request for erasure is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

4.2.7.4 Right to restriction of processing

Each Controller and/or Processor, as appropriate, should have a procedure in place for data subjects to request restriction of processing of their personal data. The procedure specifies in which cases restriction is legitimate.

If a data subject's request for restriction of processing is legitimate, this is executed across all relevant data storage facilities, including those managed by third parties.

4.2.7.5 Right to data portability

Each Controller and/or Processor, as appropriate, determines which processes are subject to the right of data portability as well as when the requirements for such right are met.

Data subjects can request from each Controller to receive a machine-readable copy of the personal data the Controller holds about them and where possible, enable the transfer of this data to another data Controller.

Portability right can be exercised when:

- processing operations are based on data subject's consent or on contract
- personal data concerns the data subject and are the same that the latter has provided to the organization
- the right does not adversely affect rights and freedoms of others
- The processing is carried out by automated means.

Each Controller and/or Processor, as appropriate, implements appropriate measures and procedures to provide data subject, who is entitled to, with a structured, commonly used and machine-readable copy of the personal data it holds about him and where possible, to enable the transfer of this data to another data Controller indicated by data subject.

4.2.7.6 Right to object

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subjects have the right to object on grounds relating to their particular situation (unless the processing is necessary for the performance of a task carried out for reasons of public interest). The right to object is explicitly brought to the attention of the data subject at the latest at the time of the first communication with the data subject, presented clearly and separately from any other information. Measures should be in place to assess such objections and to ensure that such processing ceases when the request is legitimate and needs to be respected.

Data subjects have the right to object, on request and free of charge, to the processing of personal data relating to them for purposes of direct marketing.

4.2.7.7 Automated decision making

Data subject has the right to object to any automatic decision-making (including profiling).

Each Controller and/or Processor, as appropriate, will have determined which processes entail automated decision-making (including profiling) and will have established measures to allow data subjects to object to such automated decision making and profiling. Suitable measures are in place to safeguard the data subject's rights and freedoms and legitimate interest, at least the right to obtain human intervention on the part of the Company/Controller, to express his or her point of view and to contest the decision.

4.2.7.8 Timely response to exercise of rights

Each Controller and/or Processor, as appropriate, must confirm to data subjects without delay whether data relating to them are processed and communicate the data to them in an intelligible form. Each Controller and/or Processor, as appropriate, should implement internal procedures in order to be able to provide a timely response to the requests of data subject for the exercise of his rights.

Measures have to be implemented in a way that effectively allows an individual to exercise his or her right to personal data, and that enables Each Controller and/or Processor, as appropriate, to respond to such request appropriately within the required timeframes.

Notification to recipients

In case of a legitimate exercise of rights to rectification, erasure or restriction of processing recipients of the personal data should be informed of the rectification, erasure of that data or of the restriction of processing.

Each Controller and/or Processor, as appropriate, should have a procedure in place for communicating any rectification or erasure of personal data or restriction of processing to the recipients to whom the personal data has been disclosed and for disclosing these recipients to the data subject, if so requested.

4.2.8 Data protection documentation system

4.2.8.1 Register of processing

Each Controller and/or Processor, as appropriate, regarding their processing activities must set up a relevant record, maintained in writing (including in electronic form) and made available easily and swiftly to the supervisory authority on request, as per applicable legal requirements within their respective Member States. The record of processing activities shall contain all the information required by GDPR.

Consequently, the Controller shall have an up-to-date overview of all personal data processing activities and shall maintain records within the Project that meet the legal requirements posed by the GDPR. By doing so, the Controller will be able to demonstrate compliance to any Supervisory Authority or other state or EU authority concerned.

For the avoidance of doubt, each Project Partner carries the same responsibility above within its own respective organisation.

4.2.8.2 Register of data breaches

A specific register where the breaches have to be recorded together with other information specified by the law, must be maintained by the Controller and shown to the Supervisory Authority upon request. This register is an important element of the data protection documentation system.

Project Partners need to notify immediately and in writing the Controller of any personal data breach within their respective organisations that affects execution of the Project in any way, and to cooperate with the Controller while applying relevant GDPR legal requirements.

4.2.9 Data protection assessment

4.2.9.1 Assessment

In the event that a Data Protection Impact Assessment (“DPIA”) is carried out under the Project, the Controller shall ensure that personal data receives the appropriate level of protection in accordance with the assessed data protection risk.

The decision whether to carry out a DPIA under the Project, unless undertaken in respective Project contract, will be made by the Controller upon prior written consultation with the Project Partners.

Adequacy of protection

The Controller, assisted by Project Partners, should have a process in place in order to assess for all processing the risks of varying likelihood and severity for the rights and freedoms of natural persons, taking into account the nature, scope, context and purposes of personal data processing.

Impact assessment in case of high risk (DPIA)

When the preliminary assessment highlights that processing represents high risks, a formal and documented DPIA is carried out by ascertaining possible impact on data subject.

DPIA is conducted in such a way to meet all the requirements set forth by the GDPR (art. 35) in order to confirm the quality and validity of the findings.

Prior consultation to Supervisory Authority

The Controller has a process in place and roles are assigned in order to ensure that when a DPIA determines that the processing represents high risks, the competent Supervisory Authority is consulted prior to the processing.

4.2.10 Technical and organizational measures

The Controller and each Project Partner, as appropriate, adopts appropriate technical and organisational measures with regard to Project execution (the “Measures”), and reviews and updates them where necessary, to ensure and to be able to demonstrate that processing is in compliance with GDPR.

Each Project Partner shall notify relevant Measures to the Controller in writing. In the event of any queries or further requests by the Controller, each Project Partner undertakes to address them duly and in writing.

In the event that any Project Partner has notified the Measures to its competent Supervisory Authority, it shall inform the Controller thereof, and shall provide respective copies thereof.

4.2.11 Data breach

According to GDPR, the Controller and/or Processor, as appropriate, has to implement adequate Measures in order to prevent personal data breaches.

In addition, the Measures should be able to minimize the adverse effects, in case a security breach to personal data relating in any manner to the Project occurs anyhow.

Should a data breach occur, GDPR sets forth that the Controller and/or Processor, as appropriate, has to notify it to the Supervisory Authority providing specific information, without undue delay and in any case no later than 72 hours from the time of knowledge.

When the breach leads to significant risk of serious adverse effects on the data subject(s) or serious adverse consequences for the protection of personal data, also the latter must be informed without undue delay.

4.2.12 Data transfers to third countries

No international transfers of personal data are expected to take place under the Project.

In the event that any Project Partner wishes to carry out such personal data processing in a third country, it shall notify the Controller in writing and in advance. Unless otherwise expressly specified, any international data transfers carried out by any Project Partner for any reason during Project execution take place at its own exclusive liability and responsibility; same Project Partner shall hold all other Project Partners (including the Controller) harmless from any legal or other claims arising for such personal data processing.

In case of violation of data protection principles and rules, each Project Partner (including the Controller) is responsible for damages and is subject to sanctions. Possible violations may involve civil liability and sanctions in order to ensure that any relevant damage is compensated.

The Project Partner (including the Controller) that is liable for said damages and/or sanctions shall hold all other Project Partners harmless from any claims, costs, and expenses arising from relevant GDPR infringement.

4.2.13 EVENFLOW Repository Personal Data Protection and Privacy policy

The following Personal Data Protection and Privacy Policy is uploaded onto the Project website and SharePoint:

1. Introduction. This Personal Data Protection and Privacy Policy (the “**Policy**”) aims at providing details of the processing, and related methods of use, of personal data referred to users/visitors (the “**User(s)**”) of this website that can be reached at the address https://evenflow-project.eu/ (the “**Website**”).

This Policy refers to the EU Project [EVENFLOW, 101070430], (the “**Project**”).

Web users and visitors are recommended to read this Privacy before sending any personal information and/or filling in any electronic form posted on this website.

This information is given in accordance with applicable EU data protection law, in particular the EU General Data Protection Regulation, and EU applicable Privacy law.

2. Controller. The Controller is the actual data owner per data case i.e., it is expected to be an EVENFLOW partner that has full ownership or is the creator of the dataset.

3. Scope. This Policy covers this web site only, and no other personal data processing under the Project or any other websites owned or run in any manner by the Controller or Project Partners.

4. Policy and information notice. This site has been designed with the main function of providing information on the activities of the Project. Therefore, in most cases, the collection of the user's personal data is not required.

In certain instances, such as the "newsletter" section and in order to allow the transmission of our newsletter, the interested user is required to fill out a data collection form. In these cases, the user is always free to provide his/her own data and consent to relevant processing. We recommend reading this Policy before providing the data.

In addition, should it be necessary in limited cases to collect personal information for other purposes, this will be clearly shown in the information privacy notices required by law, in order to enable transparency and user awareness. Consent forms and other documentation will be used each time, as appropriate.

The above information aims to define limits and methods of personal data processing of each service, according to which the visitor can freely express his consent and eventually allow the collection of data and its subsequent use.

5. Traffic data. The computer systems and software procedures used to operate this website acquire, during their normal operation, some personal data whose transmission is implicit in the use of Internet communication protocols.

This category of data includes: IP addresses, browser type, operating system, the domain name and website addresses from which you are logged in or out, the information on pages visited by users within the site, the time of access, time period of user's staying on a single page, the internal path analysis and other parameters regarding the user's operating system and computer environment.

This technical / IT data is collected and used only in an aggregated and not immediately identifiable manner; they could be used to ascertain responsibility in case of hypothetical crimes against the site or upon public authorities’ request.

6. Cookies. No cookies are used by this repository.

7. Redirects to other websites. From this website, you can connect through special links to other websites of Project Partners within the Project, or of third parties as applicable each time. Controller hereby assumes no responsibility regarding the possible processing of personal data by third-party sites and in respect of the management of authentication credentials provided by third parties.

8. Purposes of processing and data retention. The processing of personal data is carried out mainly by using electronic procedures and media for the time strictly necessary to achieve the purposes for which the data were collected. The User, however, has the right to obtain the cancellation of his data for legitimate reasons.

9. Optional supply of personal information. The supply of personal data required from the User, unless otherwise noted, is optional, but in case of refusal it could be impossible to fulfil the request, or the related activity mentioned.

10. Place of personal data processing. Data processing related to web services of this website takes place, unless otherwise expressly stated, at Controller's establishment, which provides for the corresponding repository management. Personal data are only handled by technical personnel of the Controller, specifically in charge of processing, or others charged with occasional maintenance operations. These persons have received specific instructions on the confidentiality of this data.

11. Scope of data flow and dissemination. The data may be used by the Controller and/or the Project Partners' employees, as persons in charge of processing, to whom appropriate operating instructions have been given, as well as by third parties who perform operating activities on behalf of them and who act as data processors, in order to fulfil contractual obligations regarding the Project. Personal data are not disseminated to unspecified recipients. Detailed information on the names of the data processors can be requested by writing to the project coordinator.

12. Data protection rights. With regard to the processing of personal data, User has the right, at any time, to obtain confirmation of whether or not the data exists and to have it communicated to him/her in an intelligible format. Users also have the right to know the content and the origin of the data, to check its accuracy or to ask that it be integrated, updated or adjusted. Finally, Users have the right to ask that the data be deleted or made anonymous or to request the blocking of data processed in violation of the law; moreover, they may oppose the processing of the data for legitimate reasons. Requests should be addressed to the project coordinator.

13. Policy updating. The possible entry into force of new laws, as well as the evolution and updating of User services or developments in the Project could make it necessary to vary the method of processing of personal data. It is therefore possible that our policy may be modified over time and therefore we invite the visitor to periodically visit this page. To this end, the policy document highlights the date of the last version.

4.2.14 EVENFLOW Day-to-Day Data Usage and Related Processes

Despite the fact that EVENFLOW does not use any direct personal data (in the form of data coming out or processed during its research activities), it recognises the needs for creating some process related policies so that there is overall agreement of the usage/storage/retention/opt-out etc of data from every-day (day-to-day) project activities. A list of such matters is included below where the means that the consortium will tackle them reflects the whole consortium agreed approach.

4.2.14.1 EVENFLOW list of contacts

The EVENFLOW list of contacts relates to a single XLS file that includes the names of all the consortium partners and persons and their email address. It also indicates the purposes of contacting each person per organisation (admin, technical, legal etc) and the emailing lists that each belongs to. Only the EVENFLOW consortium partners have access to this list of contacts. The purpose of this list is to keep a well organised list of contacts for the EVENFLOW communications. The data will be erased after the project end (30/09/2025) and not kept or maintained. This list is being stored at the POTO SharePoint. Any person has the right to opt out of this list by direct email to the project coordinator.

4.2.14.2 Meetings' related material

This relates to any document created and used for the purposes of project meetings. These may relate to agendas, presentations, minutes, signature lists or any other internal document created for the purposes of EVENFLOW meetings. All these documents will be created and maintained for internal purposes of EVENFLOW. They will be kept for 5 years after the project's end (30/09/2025). Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the meeting.

4.2.14.3 Workshops/Conferences and Training sessions

These data relate to the creation of workshops, agendas, programmes, participants' lists etc and in general dissemination material related to EVENFLOW organised workshops. Regarding the external publication of this material, we consider that this material can be fully anonymized so that it excludes personal information from the presenters/participants in the related programmes/agendas that will be shared publicly. For the parts of the related material that will be used for the workshop organisation internally to EVENFLOW, the related files will be stored in the EVENFLOW SharePoint under the section meetings. The data will be kept for 5 years after the project end for auditing reasons (i.e., 30/09/2025). Any person has the right to opt out of being mentioned in these by direct email to the project coordinator before or after the event.

4.2.14.4 Reporting

Reporting refers to internal and external (EC) documents including EVENFLOW progress of activities, technical overviews etc. Related files will include documents (reports with no personal identifiable information) and financial data (C forms) sometimes including personal data. The purpose of this data is financial so that partners can claim budget requests for their related effort in EVENFLOW. C forms will be maintained by the project coordinator only and stored at internal and secure SharePoint. This (per partner) data is not to be shared with anyone internally or externally to EVENFLOW, will be kept for 5 years after the project end (for audit purposes, i.e., 30/09/2025) and will be deleted after this date. Opting out of these data will be possible but will require an updated Form C to be submitted by the project partner.

4.2.14.5 Deliverables, internal documents and other EVENFLOW reports

During the EVENFLOW project run-time, a large series of documentation and reporting will be provided relating to the project deliverables and/or internal documents etc. These files will be used for the project contractual obligations and shared to: EVENFLOW partners, EC, everyone (depending on deliverable type). In these documents, the name or email of authors may be included. Following this, as far as the internal (to EVENFLOW) and EC distributed documents are related, they will be used only for the purposes of reporting. Reports that will be shared publicly (public deliverables) will mention only the partner's name and not any other personal information. All reports will be kept for 5 years after the project's end for auditing reasons (i.e., 30/09/2025).

4.2.14.6 Source codes

As far as the inclusion of personal information inside source codes is concerned, EVENFLOW intends to not use any such information into actual source code files produced in the framework of EVENFLOW foreground. In case that any partner wishes to include any personal information, a related consent form will have to be created, used and signed by the data owner(s).

4.2.14.7 Usage of cookies (in EVENFLOW sites)

In the cases that in any EVENFLOW application (web) requires the usage of cookies, a related pop-up window informing the user must be present, prompting the user to accept (or not) the conditions under which her/his personal information is stored. The cookie policy of the EVENFLOW website can be found here. EVENFLOW will maximize efforts to reduce the usage of cookies in its web developments.

4.2.14.8 Lists of stakeholders and EVENFLOW contacts

This list refers to internal to EVENFLOW lists of external stakeholders including potential technology/results up-takers, major links with end-users and other stakeholders. This list will be used for communication purposes of EVENFLOW, no external access will be allowed (restricted to EVENFLOW partners). When people are being registered to this list, a consent by email will have to be sent by the data owner. The data will be kept until the EVENFLOW end, i.e. 30/09/2025. Any person has the right to opt out of being mentioned in these by direct email to the project coordinator.

4.2.14.9 Project related research data

Any data circulated internally to EVENFLOW for research purposes must be fully anonymized by the data owner (in this case the data Controller) and not relating in any case to personal information as stated in the sections above.

4.2.14.10 Any other EVENFLOW-related data

In case that personal information needs to be added in any other document in EVENFLOW, the Controller (document creator) will have to notify the data owners of their personal details being included into the related document, purpose, retention, storage etc.

5 Conclusions

This document supports the EVENFLOW project management procedures and policies, through the provision of a comprehensive Data Management Plan (as part of WP1 ``Project Management & Coordination”). A description of the data that will be used in all activities of EVENFLOW is provided at the start of the document. This enables an overview of the EVENFLOW data lifecycle and lists the different categories of data assets. In addition, an overview of the EVENFLOW policy and the General Data Protection Regulation (GDPR) are presented. This document also describes the potential data that can be generated or collected during the EVENFLOW project's lifetime, as well as how the project intends to make the data FAIR and ensure the security and privacy of personal and sensitive data.

This deliverable is a living document and will be regularly updated during the evolution of EVENFLOW, according to new findings and refinements of data generated by the project. This process will include latest updates on data, actual data shared, metadata provided, as well as information on their public sharing and related platforms.

Appendix A Initial data assets

In Table 6 below, the potential data assets that have been identified at the beginning of the EVENFLOW project are listed. It should be noted that some surrogate datasets will also be used, with characteristics derived from those of the use case datasets. If significant, they will be included in an update of the DMP.

Table 6: Initial data assets in EVENFLOW.

#	Name of dataset	Relevant project task(s)	Name of activity linked to the collection of the dataset	Type of data	Format of data	Expected size of data[11]	Expected data velocity [12]	Storage of data[13]	Stakeholders that may find meaningful utility for the dataset[14]	Describe the utility of the dataset (for the indicated stakeholders group)	Includes personal data? (Y/N)	Data availability (Open /Closed)	If data will be closed (or can be shared under restrictions), please provide a justification	Data accessibility for open data[15]	Please indicate the expected time that data will be made open	Responsible partner / collaborating partners
1	Project Operation Documents	T1.1 (project management)	Typical project operations	Documents used for the project operations (deliverables, meeting MoM, action items etc.)	Office documents (.docx, .pdf, .pptx, .xlsx, latex), agenda items (.ics), photos etc.	10GB at the end of the project	N/A	Central project SharePoint site	Consortium	Project operations	Y	Closed	This data will remain closed as it contains information that is useful only for internal project management purposes	N/A	N/A	INTRA, All consortium partners
2	AGV Training Datasets v1	T3.2	EVENFLOW use case	Sensor data of the AGV (timeseries, camera feed,	csv, pcd, img, db3	~50GB depending on	N/A	Local storage	Researchers in robotics AI,	Sensory data of an AGV during operation in	N	Open	N/A	TBD	July 2023	DFKI

[11] (Refers to estimated expected size of the data based on similar past experiences of the project partners unless otherwise indicated)

[12] (e.g. KB generated per month)

[13] (e.g. local storage, central repository, etc.)

[14] (e.g. academic institutions/research centres, technology companies, etc.)

[15] (e.g. Zenodo, OpenAIRE, etc.)

#	Name of dataset	Relevant project task(s)	Name of activity linked to the collection of the dataset	Type of data	Format of data	Expected size of data[11]	Expected data velocity[12]	Storage of data[13]	Stakeholders that may find meaningful utility for the dataset[14]	Describe the utility of the dataset (for the indicated stakeholders group)	Includes personal data? (Y/N)	Data availability (Open /Closed)	If data will be closed (or can be shared under restrictions), please provide a justification	Data accessibility for open data[15]	Please indicate the expected time that data will be made open	Responsible partner / collaborating partners
				pointclouds, etc.)		compression			computer vision	an industry 4.0 factory						
3	AGV Training Datasets v2	T3.2	EVENFLOW use case	Sensor data of the AGV (timeseries, camera feed, pointclouds, etc.)	csv, pcd, img, db3	~50GB depending on compression	N/A	Local storage	Researchers in robotics AI, computer vision	Sensory data of an AGV during operation in an industry 4.0 factory, including human workers	Y	Closed	Contains images of individuals	N/A	N/A	DFKI
4	BRCA Time Interpolation Datasets	T3.3	EVENFLOW use case	Inferred changes in gene expression during breast cancer progression	csv	4 TB (corresponding to 254,140 trajectories between patients, each trajectory interpolated with 50 points)	N/A	Local storage	Researchers in biomedical domain, biotech and pharma companies	Cancer longitudinal data with high granularity is difficult to collect. The simulations of expression changes over time would facilitate the identification of disease biomarkers	N	Open	N/A	Zenodo	January-February 2023	BSC
5	SMART PIPE Datasets	T3.4	EVENFLOW use case	Data gathered from sensors placed within the pipe	csv	TBD	N/A	Local storage or cloud shared	Water/sewer management companies, maintenance companies, public administrations, pipe manufacturers, etc.	Measure data regarding any pipe and the flowing fluid within its status (integrity, temperature,	N	Open	N/A	TBD	September 2023	EKSO

#	Name of dataset	Relevant project task(s)	Name of activity linked to the collection of the dataset	Type of data	Format of data	Expected size of data[11]	Expected data velocity [12]	Storage of data[13]	Stakeholders that may find meaningful utility for the dataset[14]	Describe the utility of the dataset (for the indicated stakeholders group)	Includes personal data? (Y/N)	Data availability (Open /Closed)	If data will be closed (or can be shared under restrictions), please provide a justification	Data accessibility for open data[15]	Please indicate the expected time that data will be made open	Responsible partner / collaborating partners
										pressure, flow, etc.)						