HEDGE-IoT

Holistic approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions

D1.4
Data Management Plan

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

DOCUMENT CONTROL SHEET

PROJECT INFORMATION

Project Number	101136216		
Project Acronym	HEDGE-IoT		
Project Full title	Holistic Approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions		
Project Start Date	01 January 2024		
Project Duration	42 months		
Funding Instrument	Horizon Europe Framework Programme	Type of action	HORIZON-IA HORIZON Innovation Actions
Call	HORIZON-CL5-2023-D3-01-15		
Topic	Supporting the green and digital transformation of the energy ecosystem and enhancing its resilience through the development and piloting of AI-IoT Edge-cloud and platform solutions		
Coordinator	European Dynamics Luxembourg SA		

DELIVERABLE INFORMATION

Deliverable No.	D1.4							
Deliverable Title	Data Management Plan							
Work-Package No.	WP1							
Work-Package Title	Project Management and Administration							
Lead Beneficiary	ED							
Main Author	Luigi Briguglio (CEL)							
Other Authors	Nikolaos Bilidis (ED), Emanuela Tangari (CEL), Kari Mäki and Sayawu Diaba (VTT), Marjorie Hoegen, Aytug Yavuzer (RWTH)							
Due date	M6							
Deliverable Type		Document, Report (R)	X	Data management plan (DMP)		Websites, press & media action (DEC)		Other
Dissemination Level	X	Public (PU)		Sensitive (SEN)		Classified		
	PU: Public, fully open SEN: Sensitive, limited under the conditions of the Grant Agreement Classified R-UE/EU-R – EU RESTRICTED under the Commission Decision No2015/444 Classified C-UE/EU-C – EU CONFIDENTIAL under the Commission Decision No2015/444 Classified S-UE/EU-S – EU SECRET under the Commission Decision No2015/444							

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Document Revision History

Version	Date	Description of change	List of contributor(s)
0.1	22/04/2024	Creation of the ToC, integration of baseline questionnaire	Luigi Briguglio (CEL)
0.2	11/06/2024	Applied new template, completion of the section 1, integration of the methodology in section 2, integration of the analysis of the baseline questionnaire and completion of the section 3	Luigi Briguglio, Emanuela Tangari (CEL)
0.3	17/06/2024	Added section 4	Luigi Briguglio, Emanuela Tangari (CEL)
0.4	18/06/2024	Release for peer-review	Luigi Briguglio, Emanuela Tangari (CEL), Nikolaos Bilidis (ED)
0.6	21/06/2024	Peer-review process refinement	Luigi Briguglio, Emanuela Tangari (CEL), Nikolaos Bilidis (ED), Kari Mäki and Sayawu Diaba (VTT), Marjorie Hoegen, Aytug Yavuzer (RWTH)
1.0	28/06/2024	Release for submission	Luigi Briguglio, Emanuela Tangari (CEL), Nikolaos Bilidis (ED)

PARTNERS

Participant number	Participant organisation name	Short name	Country
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LU
2	RHEINISCH-WESTFAELISCHE TECHNISCHE HOCHSCHULE AACHEN	RWTH	DE
~~3~~	~~ENGINEERING - INGEGNERIA INFORMATICA SPA~~	~~ENG~~	~~IT~~
4	EREVNITIKO PANEPISTIMIAKO INSTITOUTO SYSTIMATON EPIKOINONION KAI YPOLOGISTON	ICCS	EL
5	INESC TEC - INSTITUTO DE ENGENHARIADE SISTEMAS E COMPUTADORES, TECNOLOGIA E CIENCIA	INESC	PT
6	NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK TNO	TNO	NL
7	TAMPEREEN KORKEAKOULUSAATIO SR	TAU	FI
8	TEKNOLOGIAN TUTKIMUSKESKUS VTT OY	VTT	FI
9	TRIALOG	TRIALOG	FR
10	CYBERETHICS LAB SRLS	CEL	IT
11	CENTRO DE INVESTIGACAO EM ENERGIA REN - STATE GRID SA	NESTER	PT
12	INTERNATIONAL DATA SPACES EV	IDSA	DE
13	ELIA TRANSMISSION BELGIUM	ETB	BE
14	HRVATSKI OPERATOR PRIJENOSNOG SUSTAVA D.D.	HOPS	HR
15	UNIVERSITATEA TEHNICA CLUJ-NAPOCA	TUC	RO
16	CLUSTER VIOOIKONOMIAS KAI PERIVALLONTOS DYTIKIS MAKEDONIAS	CLUBE	EL
17	F6S NETWORK IRELAND LIMITED	F6S	IE
18	SOCIAL OPEN AND INCLUSIVE INNOVATION ASTIKI MI KERDOSKOPIKI ETAIREIA	INCL	EL
19	ABB OY	ABB	FI
20	ENERVA OY	ENERV	FI

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

21	JARVI-SUOMEN ENERGIA OY	JSE	FI
22	DIMOSIA EPICHEIRISI ILEKTRISMOU ANONYMI ETAIREIA	PPC	EL
23	DIACHEIRISTIS ELLINIKOU DIKTYOU DIANOMIS ELEKTRIKIS ENERGEIAS AE	HEDNO	EL
24	INDEPENDENT POWER TRANSMISSION OPERATOR SA	IPTO	EL
25	ELLINIKO HRIMATISTIRIO ENERGEIAS	HENEX	EL
26	HARDWARE AND SOFTWARE ENGINEERING EPE	HSE	EL
27	QUE TECHNOLOGIES KEFALAIOUCHIKI ETAIREIA	QUE	EL
28	ARETI S.P.A.	ARETI	IT
29	APIO S.R.L.	APIO	IT
30	ACEA ENERGIA SPA	AE	IT
~~31~~	~~VOLKERWESSELS ICITY B.V.~~	~~VWICI~~	~~NL~~
32	ARNHEMS BUITEN BV	AB	NL
33	STICHTING VU	VU	NL
34	COOPERATIVE ELECTRICA DO VALE DESTE CRL	CEVE	PT
35	REN - REDE ELECTRICA NACIONAL SA	REN	PT
36	MC SHARED SERVICES SA	SONAE	PT
37	ELES DOO SISTEMSKI OPERATER PRENOSNEGA ELEKTROENERGETSKEGA OMREZJA	ELES	SI
38	ELEKTRO GORENJSKA PODJETJE ZA DISTRIBUCIJO ELEKTRICNE ENERGIJE DD	EG	SI
39	OPERATO DOO	OPR	SI
40	SVEUCILISTE U ZAGREBU FAKULTET ELEKTROTEHNIKE I RACUNARSTVA	UNIZG	HR
41	INSTITUT JOZEF STEFAN	JSI	SI
42	KONCAR - DIGITAL DOO ZA DIGITALNE USLUGE	KONC	HR
43	DS TECH SRL	DST	IT

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Disclaimer

Funded by the European Union. Views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union. The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

EXECUTIVE SUMMARY

This document defines the Data Management Plan (DMP) for the HEDGE-IoT project, based on the baseline assessment performed during the first six months of the project lifecycle. This document is strongly intertwined with the Project Management Handbook (PMH) and the established Ethics and Regulatory Governance (ERGO) framework. Ethics and regulatory aspects are indeed considered when dealing with data management, and specifically with the personal data management of individuals.

The document provides the list of relevant data types related to the project activities, the identified data flows, i.e., data processed within the partners' premises and in the project shared environment), the access to existing datasets used for the project activities, and last but not least the FAIR (i.e., findable, accessible, interoperable and reusable) principles to manage data within the project, as well as the main principles from the General Data Protection Regulation (EU 2016/679) for management of personal data of individuals.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

TABLE OF CONTENTS

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

LIST OF TABLES

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

LIST OF FIGURES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

ABBREVIATIONS

AI	Artificial Intelligence
CA	Consortium Agreement
CI/CD	Continuous Integration / Continuous Deployment
DoA	Description of the Action
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DMP	Data Management Plan
EC	European Commission
ERGO	Ethics and Regulatory Governance
EU	European Union
FAIR	Findable, Accessible, Interoperable and Reusable
GA	Grant Agreement
GDPR	General Data Protection Regulation (EU 2016/679)
IoT	Internet of Things
ML	Machine Learning
PMH	Project Management Handbook
WP	Work Package

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

The purpose of the Data Management Plan (DMP) is to provide the HEDGE-IoT consortium with a key element to properly manage data (collected, processed and/or generated) throughout its whole lifecycle. Proper data management means that the HEDGE-IoT consortium relies, follows and respects the rules defined in the DMP. The DMP aims to ensure the "FAIR" principles (i.e., findable, accessible, interoperable and reusable), as defined in [1], and protect the privacy and sensitivity of data (either personal or IoT infrastructure specific or foreground research data) against unauthorised access, in compliance with the GDPR [2]. Therefore, the HEDGE-IoT consortium takes care of the appropriate definition of the DMP and that the HEDGE-IoT consortium adheres to the rules.

Mostly, HEDGE-IoT, working in the context of energy transmission and distribution – pertaining to a critical infrastructure - does not produce publicly open and accessible data for security and confidentiality reasons. Data collected, processed and/or generated from the HEDGE-IoT testing in pilots will be elaborated, with the objective to assess the HEDGE-IoT Digital Framework. As a consequence, data can be used for training Machine Learning/Artificial Intelligence (ML/AI) technologies and performing tests, obviously by taking care of appropriate data protection techniques, in compliance with the current and applicable European regulatory framework.

Moreover, HEDGE-IoT consortium will carry out training, dissemination and exploitation activities by managing data that can be published on the Web (i.e. website, social media) and shared on events (i.e. workshops, conferences, meetings) and publications (i.e. papers, articles, newsletters). Consequently, a proper FAIR data management plan includes description on how to make research data findable (i.e. based on metadata), accessible (e.g. through archives), interoperable (i.e. based on standard formats/protocols) and re-usable.

Due to the fact that rules and conditions may change during the project lifecycle, it is reasonable to consider this document as a "living document" that will be internally updated whenever it is needed to reflect up to date project information and procedures. In case of updates, the HEDGE-IoT consortium will report changes in the next Project Management Handbook (PMH) (e.g., available versions at months M18 and M30).

1.2 REFERENCE AND APPLICABLE DOCUMENTS

1.2.1 Reference Documents

For the preparation of the present deliverable D1.4 "Data Management Plan" (DMP), the authors used a set of reference documents, including scientific publications, manuals, technical reports and standards, representing valuable sources for the specific context. This list of sources is reported in the section REFERENCES. References give credit to sources and allow readers to easily find and verify the information that has been used.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

1.2.2 Applicable documents

The general indications for the project implementation are defined in the HEDGE-IoT Grant Agreement (GA), the Consortium Agreement (CA), and the Project Management Handbook (D1.1 - PMH). As a result, the present deliverable "Data Management Plan" (D1.4 – DMP) does not replace any of these applicable documents, and partners should abide by the following order of precedence:

- **Grant Agreement**
- **Consortium Agreement**
- **D1.1 "Project Management Handbook"**
- **D1.4 "Data Management Plan"**

1.3 STRUCTURE OF THE DOCUMENT

- **Chapter 1 - Introduction**: outlines the purpose, reference documents, and structure of the data management plan. It establishes the baseline for ensuring alignment with FAIR data management principles, and details about data types and flows of the HEDGE-IoT project.
- **Chapter 2 – Methodology and baseline assessment**: defines the methodology adopted by HEDGE-IoT project to identify the data types and flows, and the baseline assessment performed at the beginning of the project.
- **Chapter 3 – Data summary, usage and management**: describes and analyses data types used and managed within the scope of the HEDGE-IoT project, and the list of deliverables.
- **Chapter 4 - FAIR Data management and GDPR compliance**: describes FAIR principles to be adopted during the HEDGE-IoT project lifecycle, and rules from the GDPR regulation.
- **Chapter 5 – Conclusions**: serves as a comprehensive summary of the project's data management strategies and procedures.

The document is complemented with two appendixes:

- **Appendix A – Baseline questionnaire**: the questionnaire proposed and used by the HEDGE-IoT project to gather and collect information about ethics and data management concerns;
- **Appendix B** - **HEDGE-IoT privacy policy**: the proposed HEDGE-IoT privacy policy to be considered when dealing with processing of personal data of individuals within the context of the project activities.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

2 METHODOLOGY AND BASELINE ASSESSMENT

The HEDGE-IoT project, and specifically its Task 1.4 "Ethics, exchange requirements specifications and data management", has established an Ethics and Regulatory Governance (ERGO – see Figure 1) framework to drive the research and innovation process by

(i) **setting key principles** from existing and forthcoming EU regulatory frameworks, to be considered by the development team during the whole lifecycle;

(ii) based on these principles; **providing ethics and regulatory requirements** to be embedded into the development of the system;

(iii) **monitoring and performing the assessment** of the project activities and outcomes; and

(iv) **providing recommendations and blueprints** for improvements of best practices and future regulations.

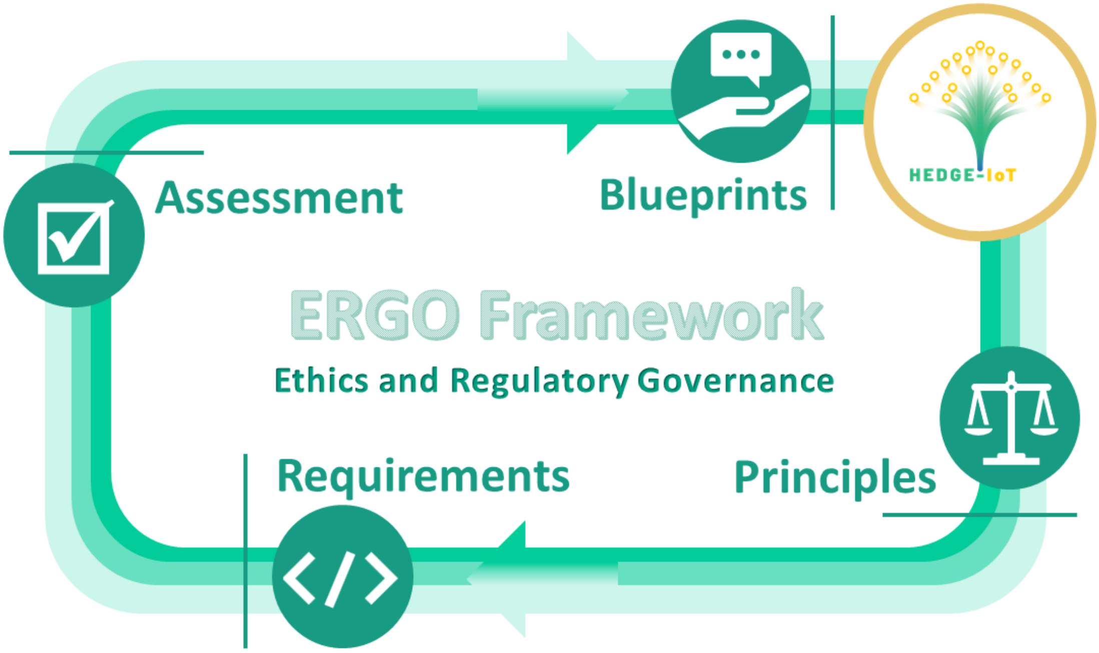


FIGURE 1. THE HEDGE-IOT ERGO FRAMEWORK

The ERGO framework enables an iterative and incremental monitoring and assessment process. It allows the project consortium to gather, collect, and analyse data from experiences. In so doing, the project can identify concerns, countermeasures and lessons learned.

The ERGO framework is applied since the beginning of the project and performed a baseline assessment for the preliminary identification of (i) potential ethics and regulatory concerns; and (ii) data management concerns (e.g., types and flows). This document reports the specific results of the baseline assessment belonging to data management concerns, while the D2.1 "Requirements on

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

an IoT Cloud/Edge System for the Energy Ecosystem" (due date month M8) will report results on ethics and regulatory perspectives, impacting the requirements definition process.

2.1 THE BASELINE ASSESSMENT

The HEDGE-IoT project is experiencing a novel approach to simplify and improve efficiency of the consortium' engagement. Usually, foreseen project activities have to be assessed with two questionnaires for the ethics and data management aspects. However, the experience of CEL allowed to merge most of overlapping questions into a single online questionnaire, due to the fact that data management and regulatory compliance are strongly intertwined, as clarified since the introduction of this document. This approach has two advantages:

- The single online questionnaire is more efficient, reducing the number of similar questions, and partners are more engaged;
- The single online questionnaire provides enough data to understand concerns and misunderstanding of each single partner, and therefore face-to-face meeting can be arranged between CEL and the specific partner.

The baseline assessment questionnaire is structured in 5 main sections, as shown in the Table 1.

SECTION	DESCRIPTION
1. Activity	Main activities of the partner in the project
2. Personal Data	Generated, processed, managed by the partner in the project
3. Personal Data Processing	Techniques and rules applied to process personal data
4. Data Management	Data types, flow and principles adopted by the partner
5. Technology	Technology deployed and adopted by the partner in the project

TABLE 1. SECTIONS OF THE BASELINE QUESTIONNAIRE

The baseline assessment questionnaire is available in Appendix A and it has been circulated in April 2024, to ensure partners have a better understanding of the specific project activities, objectives, data and technology. The data collection was completed in over 2 months, and in June 2024 CEL performed the data analysis.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3 DATA SUMMARY, USAGE AND MANAGEMENT

This section provides the summary of data to be used and managed during the whole HEDGE-IoT project lifecycle. This summary of results from the baseline questionnaire was submitted to the project consortium during the first 6 months, therefore it represents the expected data types and formats according to preliminary plans. It is reasonable that during the implementation of the technology and the deployment in the pilots, the project consortium might have further details, and in that case, the project will evaluate an update of this section to be reported in a refinement of the "Project Management Handbook" (i.e., at month M18 or month M30).

3.1 TYPES OF ACTIVITIES

The baseline assessment begins with the identification of clusters of activities in which the partners will be involved. Four clusters have been identified (i.e., Management and Compliance, Implementation, Piloting and Assessment, Communication/Dissemination/Exploitation) and the partners selected their most relevant ones (see Figure 2). Implementation also includes use cases, requirements, specification, software development, deployment and validation. For this reason, it represents the most relevant activity in the project (more than 80% of the answers). Piloting and Assessment of results is the second most relevant activity in the project with around 60% of the answers.

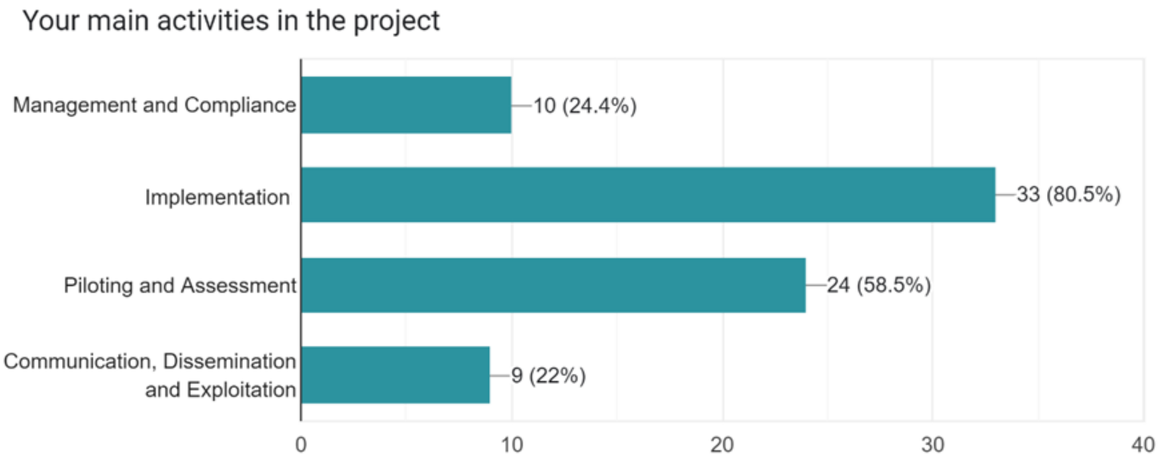


FIGURE 2. TYPES OF ACTIVITY IN HEDGE-IOT

This information is useful to comprehend the potential data types and formats that will be used during the project lifecycle, as well as the procedures to be adopted to ensure a FAIR data management.

3.2 DATA TYPES

The baseline questionnaire identifies 8 main data types that will be used during the HEDGE-IoT project, specifically: text (e.g., text documents for reports, deliverables, publications, blogs), spreadsheet (e.g., spreadsheets for reporting and data gathering); presentation (i.e., slides for presentation); dataset (e.g., data from pilots, data for assessment purposes, data from workshops and meetings); software code; audio (e.g., audio recordings from meetings and workshops, audios for podcast); video (e.g., video recordings from meetings and workshops, videos for communication purposes); other (i.e., optional data type for the additional data types relevant to the HEDGE-IoT partners). The Figure 3 and Figure 4 show data types, their relevance in the whole project lifecycle and their relevance per cluster of activities. It is worth to remark the major role played by text, presentation and spreadsheet. Dataset and software code represent the key data types during the project implementation, piloting and assessment.

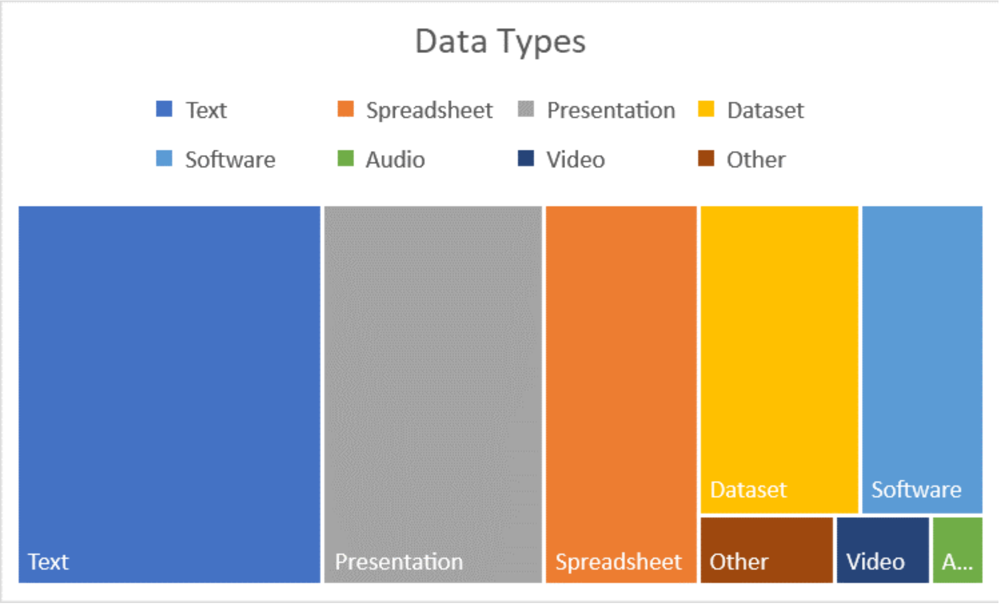


FIGURE 3. DATA TYPES IN HEDGE-IoT

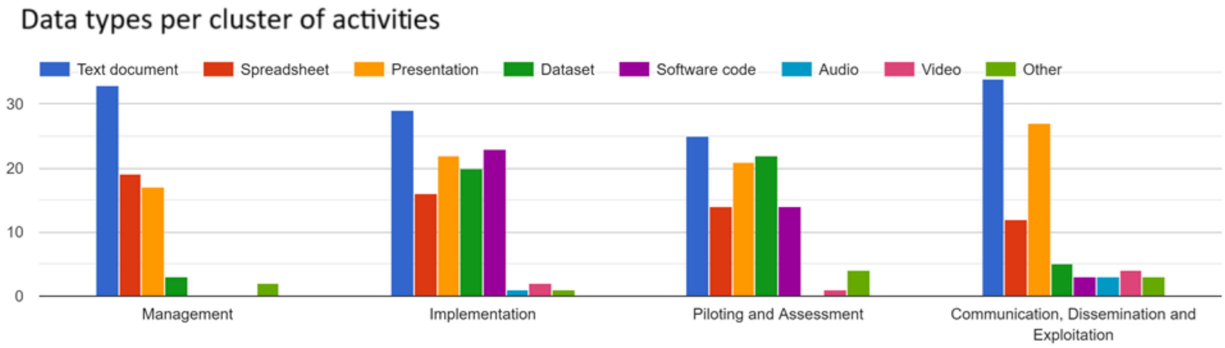


FIGURE 4. DATA TYPES PER CLUSTER OF ACTIVITIES

Moreover, the data is mostly gathered and collected from software systems (e.g., SCADA, Management Systems), hardware devices (e.g., meters, sensors connected to HV/MV/LV stations, IoT devices), datasets (e.g., public and/or private datasets, databases) and finally from humans (e.g., interviews, roundtables, focus groups, data from devices deployed at user premise) as shown in Figure 5. These answers will confirm that the ERGO framework, established by the HEDGE-IoT project, will be useful to take care of potential "personal data" processed during the project lifecycle.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

For this reason, this document provides section 4 with details on appropriate procedures for data management and to ensure compliance with the GDPR regulation.

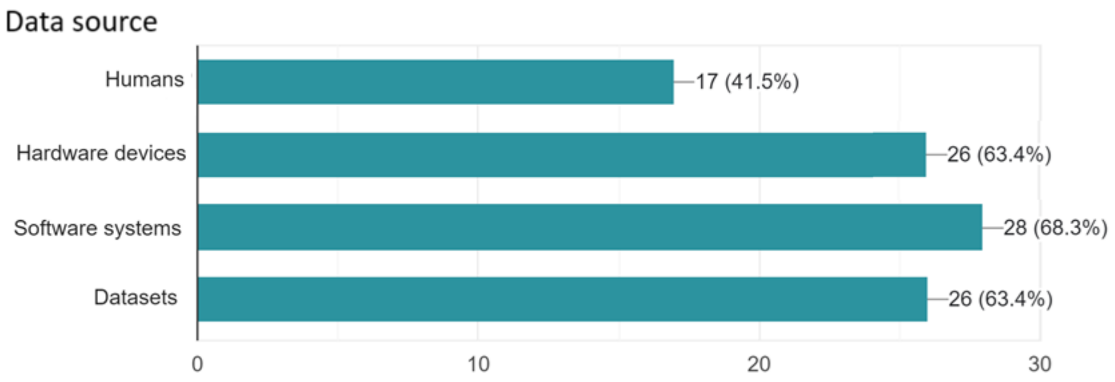


FIGURE 5. DATA SOURCE

3.3 DATA FLOW

The HEDGE-IoT project adopts and follows the "FAIR" data principles of the Horizon Europe along the whole project lifecycle (i.e., from data creation to use). For a suitable definition of data management procedures, it is fundamental to identify and understand the data flow.

The HEDGE-IoT project identifies two main treatment processes and flows, namely **standalone** and **shared** modes (see Figure 6):

- **Standalone mode** – data management (i.e., gathering, collection, processing, storage, access) is performed exclusively by a specific partner, without sharing data within the project consortium or with any other external actor. This is the case when a partner is dealing with specific information and has to respect ethics and regulatory principles (e.g., personal data processing according to GDPR or confidential data according to company policies). However, for the specific purposes of the project, this does not hamper the partner to share just results of data processing (e.g., reports and documents) within the consortium;

- **Shared mode** – as well as other online services, data management is performed through the HEDGE-IoT shared infrastructure (i.e., https://eurodyn.proofhub.com/ – see Figure 7), which allows the project consortium to collaborate and perform activities, sharing data and results.

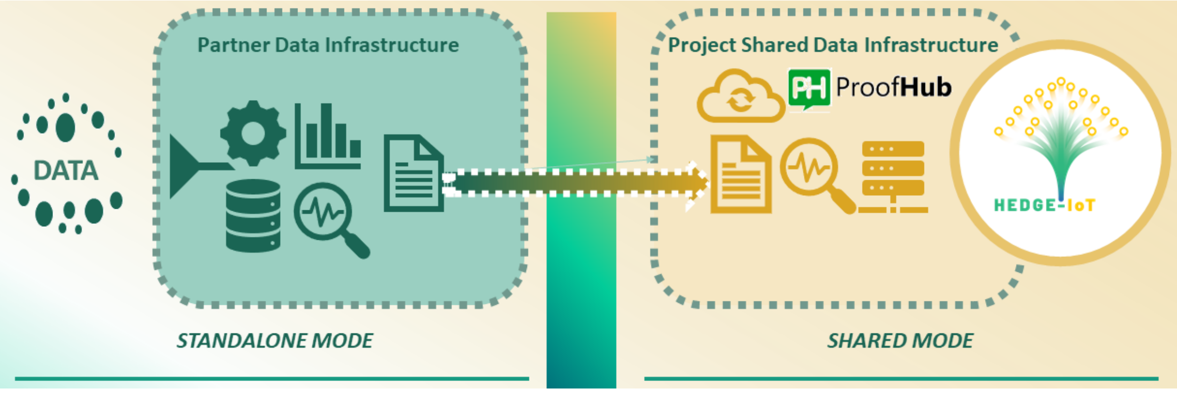
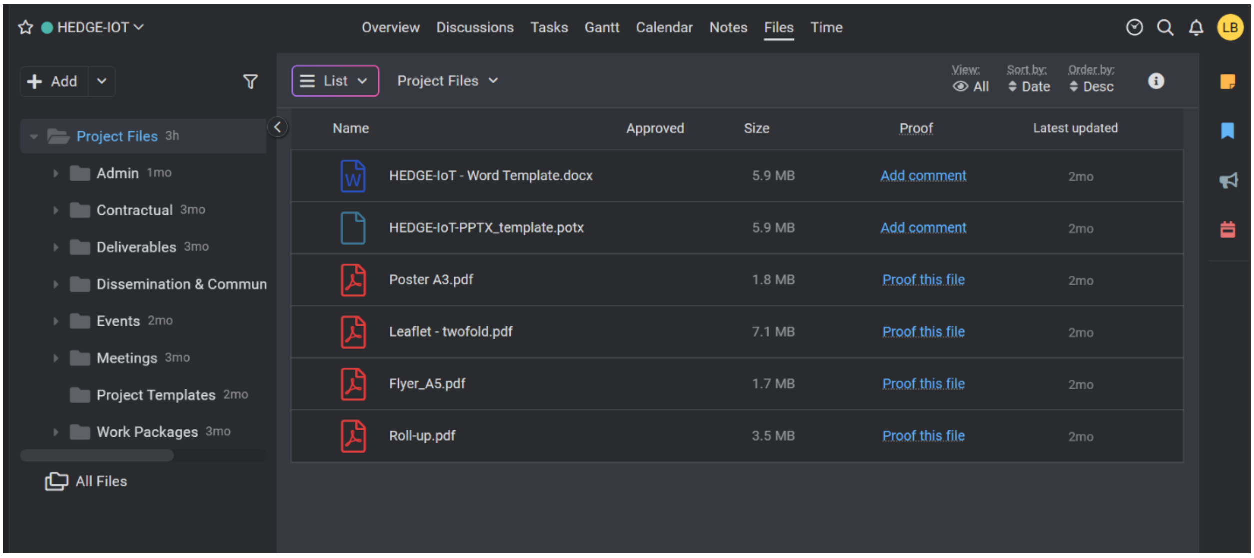

DATA
Partner Data Infrastructure
STANDALONE MODE
Project Shared Data Infrastructure
ProofHub
HEDGE-IoT
SHARED MODE

FIGURE 6. DATA FLOW IN THE HEDGE-IOT PROJECT



Project Files 3h
- Admin 1mo
- Contractual 3mo
- Deliverables 3mo
- Dissemination & Commun
- Events 2mo
- Meetings 3mo
- Project Templates 2mo
- Work Packages 3mo

Name	Approved	Size	Proof	Latest updated
HEDGE-IoT - Word Template.docx		5.9 MB	Add comment	2mo
HEDGE-IoT-PPTX_template.potx		5.9 MB	Add comment	2mo
Poster A3.pdf		1.8 MB	Proof this file	2mo
Leaflet - twofold.pdf		7.1 MB	Proof this file	2mo
Flyer_A5.pdf		1.7 MB	Proof this file	2mo
Roll-up.pdf		3.5 MB	Proof this file	2mo

FIGURE 7. HEDGE-IOT SHARED DATA INFRASTRUCTURE

3.4 ACCESS TO EXISTING DATASETS

Datasets are collection of data with a shared format and goal-relevant content [3], and these are relevant resources to be used for the HEDGE-IOT activities. The project builds on existing knowledge that is publicly available from scientific publishers and standardisation bodies and fora most importantly ETSI, ISO/IEC and CEN/CENELEC. The Table 2 summarises some of the different datasets that are input to the project.

DATASET NAME	DESCRIPTION OF DATASET	OWNER/SOURCE	ACCESS CONSIDERATIONS

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Scientific publications	Journals, books, conference proceedings, etc.	Publishers such as Springer[1], IEEE[2], ACM[3] and others.	Available at a cost based on unit purchase or subscription basis.
Open Access Scientific Publications	Online open access scientific publications.	Respective copyright holders, such as publishers and authors, e.g. arXiv[4], Zenodo[5].	Typically, available at no cost on the Internet.
ETSI Standards	European Standard (EN), ETSI Standard (ES), ETSI Guide (EG), ETSI Technical Specification (TS), ETSI Technical Report (TR), ETSI Special Report (SR), ETSI Group Report (GR), ETSI Group Specification (GS)	ETSI and authors of working drafts.	Available at no cost on the Internet. Working drafts available for members.
ISO/IEC Standards	Standard Development, Technical Committee (TC), Joint Technical Committee (JTC), Subcommittees (SC), IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE), IEC Quality Assessment System for Electronic Components (IECQ), IEC System for Certification to Standards Relating to Equipment for Use in Renewable Energy Applications (IECRE)	ISO/IEC and authors of working drafts (e.g., JTC1 /SC42 on Artificial Intelligence).	Typically, available as pay-per-view on the Internet. White papers available at no cost on the Internet.
CEN/CENELEC Standards	Standard development, Joint Technical Committee (JTC), Working Group (WG), Technical Report (TR), CEN/CLC Governance and Data Quality in AI	CEN/CLC and authors of working drafts (e.g., CEN/CLC TR 18115:2024).	Typically, available as pay-per-view on the Internet. White papers available at no cost on the Internet.
Open Source Project Repositories and associated Project Sites	Code repositories maintained e.g. on GitHub, Google code and other places.	Depends on Open Source license used.	Typically, available at no cost on the Internet.

TABLE 2. EXISTING DATASETS

3.5 DATASETS AND OUTPUTS TO BE PRODUCED

The HEDGE-IOT project has planned to produce and deliver the following categories of outputs, including inter-alia:

- **Deliverables**;
- **Scientific publications**;

[1] e.g. https://springeropen.com/

[2] e.g. https://ieee.org/

[3] e.g. https://dl.acm.org/

[4] https://arxiv.org/

[5] https://zenodo.org/

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

- **Contributions to standards**;
- **Software contributions;**
- **Datasets from experimentation and test with the project pilots**.

3.5.1 Deliverables

The HEDGE-IOT project has planned a total of 37 deliverables, distributed along the 42 months in:

- **26 public deliverables** (i.e., fully open and automatically posted online);
- **11 sensitive deliverables** (i.e., limited under the conditions of the Grant Agreement).

The following two paragraphs report the list of the public and sensitive deliverables. The tables Table 3 and Table 4 list the deliverables, sorted by due date.

The HEDGE-IOT project will provide public deliverables available through its website at https://hedgeiot.eu/resources/.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3.5.1.1 Public Deliverables

DEL #	DELIVERABLE TITLE	RESP.	DUE DATE
D7.1	COMMUNICATION AND DISSEMINATION PLAN	F6S	M3
D1.4	DATA MANAGEMENT PLAN	ED	M6
D2.1	REQUIREMENTS ON AN IOT CLOUD/EDGE SYSTEM FOR THE ENERGY ECOSYSTEM	RWTH	M8
D2.2	FUNCTIONAL SPECIFICATIONS OF THE HEDGEIOT SYSTEM	TRIALOG	M10
D7.3	DISSEMINATION, EXPLOITATION AND MARKET EXPLORATION, STANDARDISATION, AND COMMUNITY BUILDING (FIRST RELEASE)	F6S	M12
D3.1	HEDGE-IOT INTERFACES AND TOOLS FOR INTEROPERABILITY	TNO	M13
D3.3	HEDGE-IOT TECHNOLOGICAL ENABLERS (FIRST RELEASE)	INESC	M13
D4.1	HEDGE-IOT INTEROPERABILITY FRAMEWORK AND INTEGRATED SOLUTION (FIRST RELEASE)	DST	M15
D6.1	OPEN CALLS PREPARATION AND ANNOUNCEMENT	INCL	M15
D2.3	HEDGE-IOT REFERENCE ARCHITECTURE (FIRST RELEASE)	ED	M18
D5.2	PRE-DEMO PHASE REPORT	ICCS	M18
D3.2	HEDGE-IOT INTERFACES AND TOOLS FOR INTEROPERABILITY 2	TNO	M19
D3.4	HEDGE-IOT TECHNOLOGICAL ENABLERS (INTERMEDIATE RELEASE)	INESC	M19
D4.2	HEDGE-IOT INTEROPERABILITY FRAMEWORK AND INTEGRATED SOLUTION (INTERMEDIATE RELEASE)	DST	M21
D7.4	DISSEMINATION, EXPLOITATION AND MARKET EXPLORATION, STANDARDISATION, AND COMMUNITY BUILDING (INTERMEDIATE RELEASE)	F6S	M27
D2.4	HEDGE-IOT REFERENCE ARCHITECTURE (FINAL RELEASE)	ED	M28
D5.3	FULL DEMO PHASE REPORT	ICCS	M28
D6.2	OPEN CALLS INTERMEDIATE REPORT	INCL	M28
D3.5	HEDGE-IOT TECHNOLOGICAL ENABLERS (FINAL RELEASE)	INESC	M30
D6.4	REGULATORY BLUEPRINT AND CONTRIBUTION TO THE EU DIGITALISATION OF ENERGY ACTION PLAN (FIRST RELEASE)	CEL	M31
D4.3	HEDGE-IOT INTEROPERABILITY FRAMEWORK AND INTEGRATED SOLUTION (FINAL RELEASE)	DST	M32
D6.3	OPEN CALLS FINAL REPORT	INCL	M36
D5.10	DEMONSTRATIONS ACROSS TECHNOLOGIES AND SCENARIOS	ICCS	M40
D6.5	REGULATORY BLUEPRINT AND CONTRIBUTION TO THE EU DIGITALISATION OF ENERGY ACTION PLAN (FINAL RELEASE)	CEL	M42
D6.6	STAKEHOLDERS' PERSPECTIVE ON HEDGE-IOT RESULTS	VTT	M42
D7.5	DISSEMINATION, EXPLOITATION AND MARKET EXPLORATION, STANDARDISATION, AND COMMUNITY BUILDING (FINAL RELEASE)	F6S	M42

TABLE 3. LIST OF PUBLIC DELIVERABLES

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3.5.1.2 Sensitive Deliverables

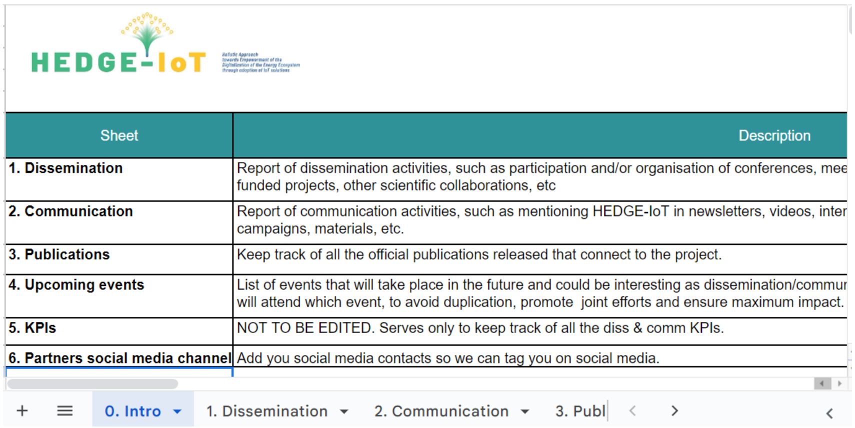
DEL #	DELIVERABLE TITLE	RESP.	DUE DATE
D1.1	PROJECT MANAGEMENT HANDBOK 1	ED	M2
D7.2	EXPLOITATION, IPR AND MARKET EXPLORATION	CLUBE	M5
D5.1	GUIDELINES FOR DEMO PREPARATION	ICCS	M12
D1.2	PROJECT MANAGEMENT HANDBOOK 2	ED	M18
D1.3	PROJECT MANAGEMENT HANDBOOK 3	ED	M30
D5.4	FINISH DEMO REPORT	ABB	M38
D5.5	GREEK DEMO REPORT	PPC	M38
D5.6	ITALIAN DEMO REPORT	ARETI	M38
D5.7	DUTCH DEMO REPORT	AB	M38
D5.8	PORTUGUESE DEMO REPORT	CEVE	M38
D5.9	SLOVENIAN DEMO REPORT	EG	M38

TABLE 4. LIST OF SENSITIVE DELIVERABLES

3.5.2 Scientific publications

The HEDGE-IOT project plans to publish several papers, articles in journals and press releases during its whole lifecycle, in the context of dissemination activities (WP7).

In addition, a list of successful submissions to scientific journals, will be internally gathered and collected by the Innovation, Dissemination & Exploitation Manager (F6S) through the "HEDGE-IoT_CommDissPublication report" (see Figure 8)(accessible to the project consortium on project shared data infrastructure), published on the project website at https://hedgeiot.eu/resources/ and reported through the EC project management portal.



Sheet	Description
1. Dissemination	Report of dissemination activities, such as participation and/or organisation of conferences, mee funded projects, other scientific collaborations, etc
2. Communication	Report of communication activities, such as mentioning HEDGE-IoT in newsletters, videos, inter campaigns, materials, etc.
3. Publications	Keep track of all the official publications released that connect to the project.
4. Upcoming events	List of events that will take place in the future and could be interesting as dissemination/commur will attend which event, to avoid duplication, promote joint efforts and ensure maximum impact.
5. KPIs	NOT TO BE EDITED. Serves only to keep track of all the diss & comm KPIs.
6. Partners social media channel	Add you social media contacts so we can tag you on social media.

HEDGE-IoT
Holistic Approach towards Empowerment of the Digitalization of the Energy Ecosystem through adoption of IoT solutions
+
0. Intro
1. Dissemination
2. Communication
3. Publ

FIGURE 8. THE HEDGE-IOT COMMUNICATION, DISSEMINATION, PUBLICATION REPORT

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

3.5.3 Standards

The HEDGE-IoT project plans to contribute to standardisation working groups and subgroups specifically addressing innovation topics such as: IoT, interoperability, security, semantic interoperability, Artificial Intelligence, data spaces, digital twins, smart energy and smart grid.

Partners of the project are already involved in ISO/IEC JTC1 SC27 (Security techniques), SC41 (IoT and digital twins) and SC42 (Artificial Intelligence).

Contributions to standards will be reported in the deliverables D7.3 (due date M12) and D7.4 (due date M27).

3.5.4 Software

As specified in the D1.1 (PMH), the HEDGE-IoT project plans to develop software by adopting advanced software versioning, code review and continuous integration / continuous deployment (CI/CD) tools.

Tools will be available both in a shared environment (e.g., for integration and fine-tuning of developed solutions) and in partners' premises for a standalone development (e.g., internal development before commit of new stable version). At this phase of the project, all available alternatives (e.g., GitHub[6], GitLab[7], Jira[8]) are still under evaluation.

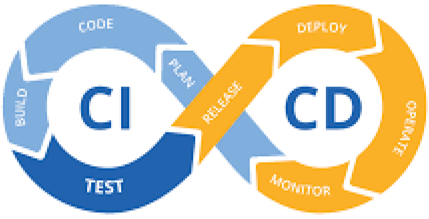


FIGURE 9. CI/CD DEVELOPMENT PROCESS

Forthcoming deliverables, especially the ones related to software development and integration, as well as the updates of project management handbook, will provide specific details about the software code management in HEDGE-IoT.

[6] https://github.com/
[7] https://about.gitlab.com/platform/
[8] https://www.atlassian.com/software/jira

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

4 FAIR DATA MANAGEMENT AND GDPR COMPLIANCE

The ERGO framework, mentioned in Section 2 and established by the HEDGE-IoT project since the early beginning, allows to ensure the protection of individuals' personal data as well as privacy rights during the whole project lifecycle. This confirms the commitment of HEDGE-IoT to respect EU "values and rules".

The forthcoming deliverable D2.1, dealing with requirements, will provide an analysis of the answers gathered by the project partners with the baseline questionnaire during the months of April – June 2024. This analysis will provide details about ethics and regulatory aspects.

This section provides a non-exhaustive list of activities concerning the processing of personal data of individuals belonging to the HEDGE-IoT consortium. Moreover, HEDGE-IoT Privacy Policy is available in Appendix B, and it is applicable to the above list of activities.

4.1 NAMING AND VERSIONING CONVENTIONS

The Project Management Handbook (PMH – D1.1) provides coding conventions and data/document versioning rules. Therefore, the HEDGE-IoT partners are invited to check rules and conventions in that document. For the convenience of the reader, the most relevant code convention is related to the deliverables, which are encoded as: HEDGE-IOT_[DELIVERABLE CODE]_VA.BB where:

- [DELIVERABLE CODE] is the identifier assigned by the DoA to the specific deliverable;
- VA is the serial number for the major release of the deliverable;
- BB is the serial number for the minor release of the deliverable (e.g., updates during the preparation/review phase).

For instance, the final version of this document to be submitted to the EC is encoded as HEDGE-IOT_D1.4_v1.0.

4.2 DATA IDENTIFICATION AND SEARCHING CAPABILITIES

During the HEDGE-IoT project lifecycle, each partner will use the shared environment (i.e., HEDGE-IoT Proof Hub) to upload, share and download documents, reports and to get access to project data.

According to the project schedule, its work breakdown structure and the naming convention, the Project Coordinator organised the shared environment in different sections and folders, enabling to easily and efficiently identify, search and browse the project data.

Moreover, the shared environment allows to identify data owners/authors, as well as contributors and dates of modification.

To further support searching capabilities, each document owner/author will also include some metadata (e.g., keywords) to the document.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

As clarified in section 3, most of the data used and managed by the HEDGE-IoT consortium is based on non-proprietary formats, therefore this ensures the interoperability feature.

4.3 MAIN PRINCIPLES APPLICABLE TO PERSONAL DATA PROCESSING

As a general rule, when processing personal data of individuals, each partner commits to respecting GDPR [2], as well as any other applicable data protection and privacy regulations. This section provides some of the most relevant principles in personal data processing.

Personal data must be processed **lawfully, fairly, and transparently** in relation to the data subject. Each partner commits to ensuring compliance with principles such as purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability.

Accordingly, in any case of personal data processing, the relevant HEDGE-IoT partner will be and remain accountable and responsible for the data collected during the project. When dealing with personal data processing, partners have to obtain **consent** before collecting data, unless another lawful basis is applicable.

Moreover, all partners processing personal data are informed of their obligations as potential data processors (where appropriate) through current **guidelines**, as well as issues beyond data and information protection and privacy.

Personal data have to be processed in a manner that ensures appropriate **security**, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using suitable technical or organisational measures.

Technical or organisational measures have to allow the identification of data subjects only for as long as necessary for the purposes of which the data is processed. At the end of the project, all processed personal data have to be **destroyed** in compliance with specific legal requirements.

4.4 DATA AND PROCESS RELATED TO PROJECT MANAGEMENT

This section identifies the set of project management activities potentially performing personal data processing. These activities and related personal data concerns have been reported by the partners through the baseline assessment. For each activity, the section provides description and guidelines to be considered during the whole project lifecycle.

ACTIVITY	DESCRIPTION AND GUIDELINES
HEDGE-IoT mailing lists	To achieve the HEDGE-IoT results, manage the project activities and ensure appropriate communication (e.g., tasks, events, and the progress of the project) among the whole HEDGE-IoT consortium, it has been established a series of mailing lists, namely • An "ALL" mailing list for general purpose communication. It includes at least one contact person per partner; • A "GA" mailing list, including the contacts of the project's General Assembly, with one representative contact person per partner; • A "CB" mailing list including only the Coordination Board members of the consortium;

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

	• "WP2", "WP3", "WP4", "WP5", "WP6" and "WP7" mailing lists for the related work packages. The mailing lists created are restricted only to HEDGE-IoT partners, and at the end of the project will be erased (i.e., with the acknowledgement of last payment performed). The management of such mailing lists (hedge-iot_XXX@eurodyn.com), i.e. the additions and/removals, are responsibility of ED (the Coordinator). In any case, it will be the responsibility of each partner to ensure the consent of the relevant persons before including their email addresses in the mailing lists; moreover, each person included in a mailing list has the right to opt-out by contacting the Coordinator.
Meetings and related material	During HEDGE-IoT meetings (either virtual or in person) it is possible that documents will be created and used, such as agendas, presentations, minutes and signature lists etc. These documents will be created and managed only within the Consortium and its partners, and will be used only for the purposes of the relevant meeting. Moreover, each partner might have access to the document, which will be stored in the Proof Hub (project shared environment). The storage of these documents will be limited to the project duration. To the extent permissible by law, any person whose personal data will be included therein shall have the right to request at any time to the Coordinator to opt-out.
Workshops/Conferences, training and dissemination sessions	Events such as workshops, conferences and plenary meetings might be attended by one or more individuals belonging to the consortium. In this case, personal data such as name, surname, company affiliation, emails and pictures/video recording might be collected. Such data might be collected and processed not only for the purposes of organising the event, but also for dissemination. In the latter case, before the publication, the relevant individual might request to opt out from the publications by emailing to the Coordinator. The data will be stored in the HEDGE-IoT shared environment, and the data will be kept until the end of the project.
Reporting	Reports providing for updates on the Project progress, as well as on financial data, might contain personal data. These reports might be shared either within and outside the consortium for compliance purposes with national financial law, and in particular with the EC.
Deliverables, internal documents and other HEDGE-IoT reports	During the lifetime of the HEDGE-IoT Project, a set of documentation and reporting will be provided relating to the project deliverables and/or internal documents etc. These files will be used to fulfil project contractual obligations (e.g., GA, CA and DoA) and shared to: HEDGE-IoT partners, EC, and, depending on the nature of the document, shared with externals (as this might be the case for those deliverables that have a public dissemination level and that might be published on HEDGE-IoT website). In these documents, the name or email of authors may be included. Following this, as far as the internal (to HEDGE-IoT) and EC distributed documents are related, they will be used only for the purposes of reporting and stored in the HEDGE-IoT cloud server under the deliverables section. 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 more than 5 years after the project end.
HEDGE-IoT website - cookies	In the cases that in any HEDGE-IoT application (web) the usage of cookies is needed, a related pop-up window informing the users must be present, prompting the users to accept (or not) the conditions under which their personal information are stored. HEDGE-IoT will maximise efforts to reduce the usage of cookies in its web developments.
Other cases	As a general principle, in any case according to which personal data needs to be added in any kind of document for the purposes of the HEDGE-IoT Project, the controller (i.e. the document creator) shall have to notify the data subjects that their personal data will be included into the related document, specifying purposes, retention period, storage requirements etc.

Table 5. Activities and guidelines

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

5 CONCLUSIONS

This document identifies and provides the HEDGE-IoT consortium with a Data Management Plan (DMP), ensuring alignment with FAIR (i.e., findable, accessible, interoperable and reusable) data management principles, as well as with rules from the GDPR regulation (EU 2016/679) when dealing with personal data management. The document specifies the common methodology adopted by the HEDGE-IoT project to identify data types and to assess the ethics and regulatory concerns (i.e., the ERGO framework). Indeed, data management is strongly intertwined with ethics and regulatory aspects, especially when dealing with personal data.

The baseline assessment performed during the first six months of the HEDGE-IoT lifecycle is not reporting critical concerns about data types used and managed within the scope of the project. Most of the project will use and manage standard and non-proprietary formats. By adopting non-proprietary formats, interoperability principle is satisfied. The most relevant data types are textual/spreadsheet/presentation documentation (e.g., deliverables, reports), datasets (e.g., for validation purposes) and software code. Moreover, this document relies on the naming and versioning conventions established in the Project Management Handbook (PMH). Concerning the datasets that the HEDGE-IoT project will use for piloting and validation purposes, it is important to remark that HEDGE-IoT will not have any needs to process personal data. Therefore, in case of data models containing personal data (e.g., from smart meters deployed in households, customer load profiles), data will be opportunely anonymised/pseudonymised/aggregated before they are used and processed.

For these aspects, the chapter 4 (FAIR Data management and GDPR compliance) provides details about the compliance with the FAIR data management principles and a detailed list of rules and guidelines to be adopted by the project when dealing with personal data processing, and therefore to ensure compliance with the GDPR regulation. Specifically, for each project management activity it has been defined the related guidelines to be considered.

For the sake of clarity and completeness, this document provides two useful appendixes: the "Baseline Questionnaire", presenting the questionnaire proposed and used by the HEDGE-IoT project to gather and collect information about ethics and data management concerns; and the "HEDGE-IoT Privacy Policy", presenting the proposed HEDGE-IoT privacy policy to be considered when dealing with processing of personal data of individuals within the context of the project activities.

Considering that changes could occur during the HEDGE-IoT project lifecycle, aspects considered and reported in this DMP could require an update, the project team will:

- Continuously monitor and assess the use and management of data, by submitting new questionnaires and performing iterative assessments.
- Continuously perform "vis-à-vis" calls to discuss the results of the assessment, clarify doubts and reduce potential misunderstandings.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

These two “suggestions for improvements” are considered within the Ethics and Regulatory Governance (ERGO) framework established by the project to ensure compliance with EU “values and rules”.

REFERENCES

[1] European Commission, "EC H2020 Programme, Guidelines on FAIR Data Management in Horizon 2020, Version 3.0," 2016. [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

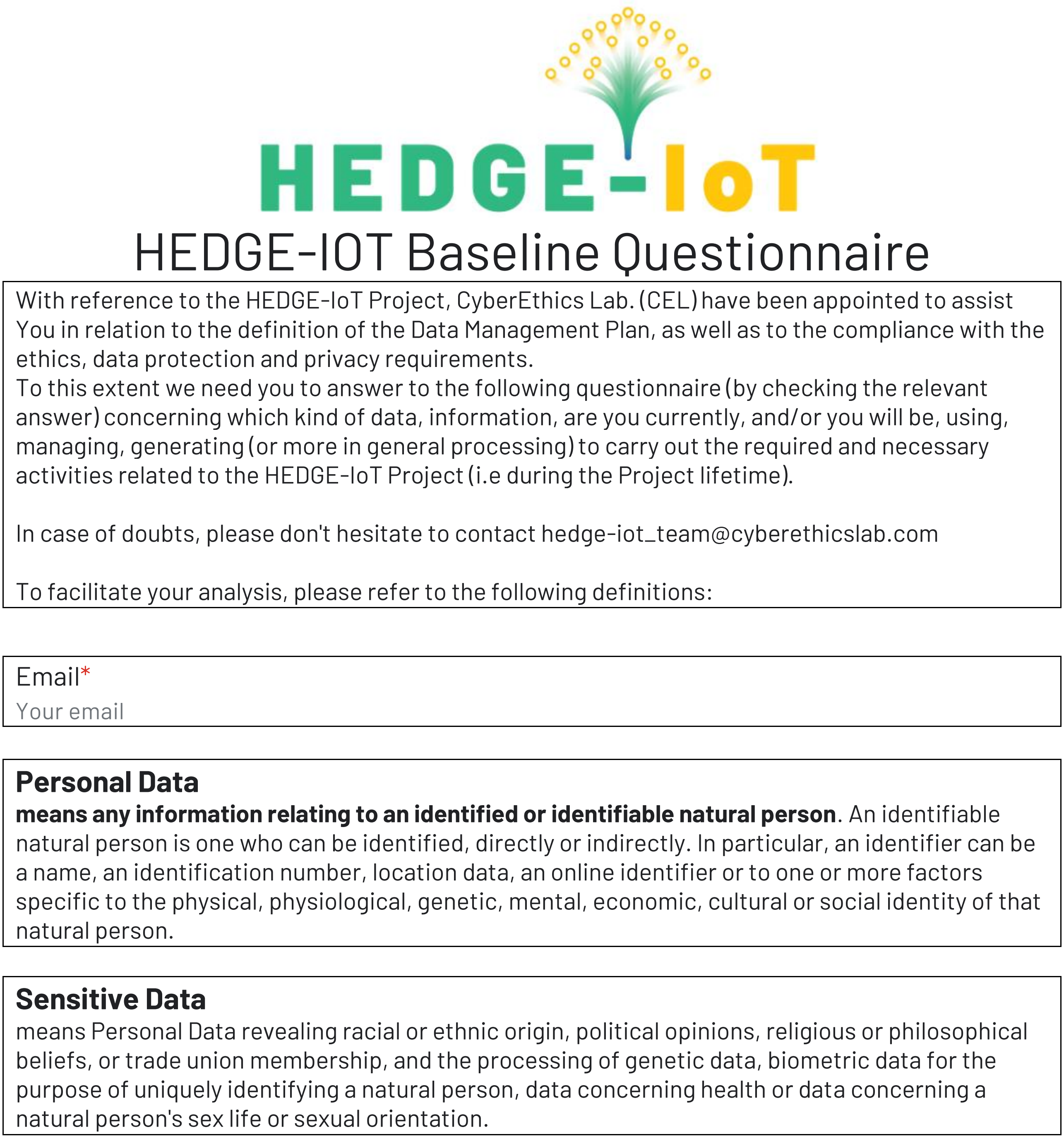
[2] European Parliament and the Council, "General Data Protection Regulation (GDPR) - EU 2016/679," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed June 2024].

[3] ISO/IEC, "ISO/IEC 22989:2022 "Information technology — Artificial intelligence — Artificial intelligence concepts and terminology"," 2022. [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:22989:ed-1:v1:en.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

APPENDIX A – BASELINE QUESTIONNAIRE



HEDGE-IOT Baseline Questionnaire

With reference to the HEDGE-IoT Project, CyberEthics Lab. (CEL) have been appointed to assist You in relation to the definition of the Data Management Plan, as well as to the compliance with the ethics, data protection and privacy requirements.
To this extent we need you to answer to the following questionnaire (by checking the relevant answer) concerning which kind of data, information, are you currently, and/or you will be, using, managing, generating (or more in general processing) to carry out the required and necessary activities related to the HEDGE-IoT Project (i.e during the Project lifetime).

In case of doubts, please don't hesitate to contact hedge-iot_team@cyberethicslab.com

To facilitate your analysis, please refer to the following definitions:

Email*
Your email

Personal Data
means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly. In particular, an identifier can be a name, an 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.

Sensitive Data
means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Data Processing
means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling
means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Company*
Please, select your company name
Choose

Your main activities in the project*
□ Management and Compliance
□ Implementation: Use cases, requirements, specification, implementation, deployment, assessment
□ Piloting and Assessment
□ Communication, Dissemination and Exploitation
□ Other: □

Q1 - Do you process personal data?
(GDPR definition: any information relating to an identified or identifiable natural person)
*
○ Yes
○ No
○ Maybe

Processing of personal data

Q2 - Do you process sensitive data?
(*GDPR definition: **special category of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs**....*)
*
○ Yes
○ No
○ Maybe

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Further requests on data treatment

You answered yes at least at one of personal/sensitive data. So, it is important to provide further details on your data treatment process.

Q3 - Do you have any reason, or justification, that legitimate you to process the personal data? (e.g. consent to process personal data)*

○ Yes
○ No
○ Maybe

Q4 - Do you clarify the purpose of the collection of the personal information and of the use of such information to the relevant individual?*

○ Yes
○ No
○ Maybe

Q5 - Do you provide an information sheet providing the main terms of the data processing (i.e. a privacy policy) to the subjects whose data are processed?*

○ Yes
○ No
○ Maybe

Q6 - Are you processing personal data previously collected for other reasons (so called "secondary use")?*

○ Yes
○ No
○ Maybe

Q7 - Do you perform activities of profiling with the personal data object of the data processing?*

○ Yes
○ No
○ Maybe

Q8 - Do you perform tracking activities (e.g. by using individuals' positions), or observation of the data subjects, by means of the personal data collected?*

○ Yes
○ No
○ Maybe

Q9 - Which are the protection mechanisms you plan to apply to personal data?*

□ None
□ Anonymisation
□ Pseudonymisation
□ Aggregation
□ Encryption
□ Other: □

Q10 - Do you share the personal data that you collect inside or outside the HEDGE-IoT Project? If you share the personal data with a subject outside the HEDGE-IoT Project, please provide the relevant name and details here below.*

○ Yes
○ No
○ Maybe

Q10b - Provide details on data sharing inside or outside the project*

Your answer

Data Management

Q11 - For the purposes of project activities, please, specify the type of data you plan to generate/manage/process*

	Text document	Spreadsheet	Presentation	Dataset	Software code	Audio	Video	Other
Management	□	□	□	□	□	□	□	□
Implementation	□	□	□	□	□	□	□	□
Piloting and Assessment	□	□	□	□	□	□	□	□
Communication, Dissemination and Exploitation	□	□	□	□	□	□	□	□

Q12 - Please, specify the source of data*

□ Humans (e.g., interviews, roundtables, focus groups, data from devices deployed at user premise)
□ Hardware devices(e.g., meters, sensors connected to HV/MV/LV stations)
□ Software systems (e.g., SCADA, Management Systems)
□ Datasets (e.g., public and/or private datasets, databases)
□ Other:

Q13 - Do you plan to adopt specific proprietary (non standard) formats?*

○ Yes

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

○ No
○ Maybe

Q14 - Please provide the retention time for data generated/managed/processed during the project*

○ None
○ Project duration
○ 5 years
○ More than 5 years

Q15 - Do you plan to store data inside EEA countries?*

○ Yes
○ No
○ Maybe

Q16 - Are you aware of EU security and privacy rules to be applied?

in case of doubts, please contact HEDGE-IOT_team@cyberethicslab.com *

○ Yes
○ No
○ Maybe

Technology

Q17 - For the purpose of the project, please, specify if you plan to use/adopt/implement specific technologies*

□ Not Available information
□ Blockchain
□ Machine Learning
□ Artificial Intelligence
□ 5G
□ Documentation processing (e.g., Text/Sheet/Presentation processors)
□ Other: □

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

APPENDIX B – HEDGE-IOT PRIVACY POLICY

The present data protection policy (the "**Policy**") is drafted by CEL with regard to the European Union's Horizon Europe Project HEDGE-IoT - Grant Agreement number 101136216 - (the "**Project**") executed by the list of Partners included therein in order to:

- comply with the policy and legal requirements of GDPR;
- comply with applicable regulations and best practices with regard to research projects within the EU Horizon Europe Research and Innovation Programme;
- raise awareness and improve knowledge among the Coordinator, Partners, as well as their employees and/or agents and/or contractors (collectively, the "**Policy Recipients**").

Due to its dynamicity and continuous evolution of the European regulatory framework in the field of data protection, this Policy may need to be periodically updated by the Coordinator, to keep it aligned with the legislative changes. Accordingly, Policy Recipients will be duly informed, and will be asked to provide their renewed consent upon any such updates.

While every effort has been undertaken by CEL to compile a comprehensive, accurate, relevant and lawful Policy, it is expressly clarified that this Policy does not constitute legal advice neither does it warrant compliance to any applicable laws or regulations. This Policy makes no warranties, express or other, on lawfulness, completeness, fitness for a purpose, or merchantability. Recipients and addressees of this Policy are advised to engage legal counsel prior to applying this Policy for their own aims and purposes.

For the purposes of this Policy the GDPR definitions, as set in Article 4, shall be found applicable.

POLICY SCOPE

The present Policy aims to provide the set of rules and principles applicable to the data processing carried by the HEDGE-IoT partners with regard to personal data of individuals involved in the HEDGE-IoT project.

The relevant 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.

Establishment

Each partner is established on the territory of an EU Member States, or in any case within the European Economic Area. In the event of any change in establishment, the respective partner shall notify the Coordinator duly and in writing.

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

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

on EU territory, on behalf of a partner, that organization qualifies as processor and ensures the fulfilment of the obligations imposed by the GDPR for that specific part of processing.

PERSONAL DATA

Personal data means any information relating to natural persons, that 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 – Sensitive 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 respectively comply with specific rules related to the processing of such data of special categories, as collecting specific informed consent from data subject and applying stricter safeguards. When the controller and/or processor relies on data subject's consent as a legal ground for processing special categories of data, it will meet all legal consent requirements; otherwise, they are only processed if and to the extent it is based on one of the legal grounds listed in the GDPR for the processing of such data.

Data anonymisation

Whenever possible, including non-detrimental to project execution purposes, the relevant controller and 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 rendered anonymous in such a manner that the data subject is not or no longer identifiable. 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.

Children’s personal data

Processing of children's personal data requires a special legitimate basis. However, as of today, HEDGE-IoT activities do not involve children.

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, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data whether the latter are contained or not in data bank.

Principles for legitimate processing

EU data protection law, and more in particular article 5 of GDPR, set forth the following specific principles which have to be complied with for the data processing to be considered legitimate.

Lawfulness, fairness and transparency – The relevant controller shall ensure that the personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject.

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

Purpose limitation - Personal data are 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.

Accuracy - 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.

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

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

DATA PROTECTION LEGAL ROLES

Controller

By determining the purposes and means of the processing of personal data, unless otherwise expressly specified in this Policy, a Partner is considered by law as a "controller" and it is the primary target of the provisions of the law.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

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 controller implies specific responsibilities because provisions setting conditions for lawful processing are essentially addressed to the controller.

Accountability*:* 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 system 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;
- data are not disclosed without human intervention.

Joint controller*:* In the event that at any time during Project execution the controller processes personal data in conjunction with a third party, by jointly determining the purposes and means of the processing, they shall be both qualified as joint controller. Both joint controllers determine the mutual responsibilities by executing a specific arrangement.

Processor

It is possible that a controller decides to appoint a processor to carry on in concrete the processing activities concerning certain personal data. If this might be the case, the relevant processor will process personal data on behalf of the controller – that is, the controller delegates all or part of the processing activities to them. In such event the between the controller and the processor shall be executed a written agreement whereby the parties will determine terms and conditions of their reciprocal obligations and responsibility.

In any case, the processor (either if it is internal to the Consortium or outside the Consortium) shall warrant that it shall provide sufficient guarantees to ensure compliance with the GDPR, shall implement 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.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Auditing: The controller ensures the commitment of the processor(s) to enable and contribute to any review activities, including inspections, carried out by the controller or other (EU authorities') auditors and/or reviewers, as appropriate.

Security: Each 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 lever than processing of similar data within its own organisation.

Data Protection Officer (DPO)

Whenever required, following applicable GDPR and Member State respective legal requirements, the Controller and each Processor, may designate a DPO for assistance in monitoring internal compliance with 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 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 relevant DPA of such designation and publishes DPO's contact details.

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 of its personnel in charge of processing personal data.

Training and awareness: All 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.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

All 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 event, they shall provide it with all requested information to the best of their ability without undue delay.

NOTICE AND CONSENT

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, in particular for any information addressed specifically to a child. The data protection notice informs data subjects about the processing of personal data relating to them, even when the personal data are 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.

Free and informed consent

Personal data are 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:

1. performance of a contract;
2. legal obligation;
3. vital interest of data subject;
4. public interest;
5. 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.

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.

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, act on the request within a specific time frame and must communicate the information requested in an intelligible and easy to access form.

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Right to be informed

Data subjects have the right to be provided with clear, transparent and easily understandable information about how their information are processed, as well as their rights. This is why the Consortium is also providing the information contained hereto in the present Policy.

Right of access

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

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.

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.

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.

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 subject can request the organization to receive a machine-readable copy of the personal data the organization holds about them and where possible, enable the transfer of this data to another data controller. Portability right can be exercised when:

1. processing operations are based on data subject's consent or on contract;
2. personal data concerns the data subject are the same that the latter has provided to the organization;
3. the right does not adversely affect rights and freedoms of others;
4. 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

Co-funded by the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

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.

The right to lodge a complaint

Any data subjects have the right to lodge a complaint about the way their personal data are handled with the relevant national DPA.

The right to withdraw consent.

Provided that data subjects have given their consent allowing any kind of activities on their personal data, and provided that the lawful basis for such data processing is the consent, they have the right to withdraw that consent at any time by contacting the relevant Partner in charge of the data processing. Withdrawing consent will not however make unlawful the use of their information while consent had been apparent.

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

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.

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

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

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.

DATA PROTECTION DOCUMENTATION SYSTEM

Register of processing

Each controller and/or processor, as appropriate, with regard to 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 so doing, the controller will be able to demonstrate compliance to any DPA or other state or EU authority concerned. For the avoidance of doubt, each Partner carries the same responsibility above within its own respective organisation.

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 DPA 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.

DATA PROTECTION IMPACT ASSESSMENT

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 Partners.

Adequacy of protection

The controller, assisted by relevant processor, 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, considering the nature, scope, context and purposes of personal data processing.

Impact assessment in case of high risk (DPIA)

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

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 a Data Protection 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 DPA is consulted prior to the processing.

TECHNICAL AND ORGANIZATIONAL MEASURES

The controller and each 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 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 DPA, it shall inform the controller thereof, and shall provide respective copies thereof.

DATA BREACH

Pursuant 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 DPA 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.

DATA TRANSFERS TO THIRD COUNTRIES

No international transfers of personal data are expected to take place under the project. In the event that any partner wishes to carry out such personal data processing, it shall notify the controller in writing and in advance. Unless otherwise expressly specified, any international data transfers carried out by any partner for any reason during project execution take place at its own exclusive liability and responsibility; same partner shall hold all other partners (including the controller) harmless from any legal or other claims arising for such personal data processing.

SANCTIONS AND DAMAGES

In case of violation of data protection principles and rules, the relevant/responsible partner 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 partner (including the controller) that is liable for said damages and/or sanctions shall hold all other partners harmless from any claims, costs, and expenses arising from relevant GDPR infringement.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement number 101136216. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

HEDGE-IoT