Deliverable 1.4

GDPR Compliance Report

Funded by
the European Union

Document Classification

Document Title	D1.4 GDPR Compliance Report
Author(s)	P01 – AIRBUS – Serena RIZZOLO
Work Package	WP1 – Project and Innovation Management
Dissemination Level	PU = Public
Nature	R = Report
Doc ID Code	20240229_STEP_D1.4_V1
Keywords	Data management, GDPR, compliance, criteria, guidelines

Document History

2024-02-22	Table of content defined	*SUB* ABGI – C. Pawlak
2024-02-22	V1 sent to P01	*SUB* ABGI – C. Pawlak
2024-02-29	Addition and validation	P01 AIRBUS – Serena RIZZOLO

Document Validation

Project Coordinator	P1 AIRBUS – Serena RIZZOLO serena.rizzolo@airbus.com
Date	2023-02-21

Document Abstract

This report presents the GDPR rules established by the EU and to be followed by the STEP Horizon Europe project (Grant Agreement n° 101134959).

It details the GDPR purpose, the project adaptation towards it, and good practices to follow during the action duration to ensure compliance with GDPR rules.

The Glossary of GDPR and a GDPR checklist are available in annexes.

Funded by the European Union. Views and opinions expressed are however those of the author(s) onlyand do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the HADEA can be held responsible for them.

Table of contents

1. Overview of the document purpose and key recommendations from the EU

The STEP project aims to enhance European capabilities in space optical missions. It focuses on developing a European supply chain for large format T2SL eSWIR space FPAs. This initiative is critical for closing the technological gap with US competitors and ensuring Europe's independence and competitiveness in space technology. Given the project's involvement in data processing activities across a consortium that includes industries, institutes, and academia, adhering to the General Data Protection Regulation (GDPR) is essential.
This document provides a GDPR compliance framework specific to the STEP project. It ensures that all project activities, from the initial design phase to prototype testing and international collaboration, comply with GDPR. The emphasis is on protecting personal data throughout the project's lifecycle.
Key Recommendations for GDPR Compliance within the STEP Project are the following:

- Integrate data protection early: start with data protection measures at the beginning of the project, embedding GDPR compliance in the development of T2SL technology and its application.
- Clarify the legal basis for data processing: clearly define the legal basis for handling personal data within the project, ensuring transparency in its use.
- Respect data subject rights: Set up procedures to ensure the rights of individuals, including project participants and others whose data might be indirectly involved, are protected.
- Security and incident response: put in place security measures to safeguard data against unauthorized access and loss. Develop plans for responding to data breaches, considering the project's specific needs.
- Manage data transfers and international cooperation: As the project involves international collaboration, ensure secure and compliant data sharing, especially when working with entities outside the EU.

The following sections of this document will detail these recommendations, offering the STEP project a clear path to GDPR compliance. Following this guidance, the project will not only comply with legal requirements but also strengthen its commitment to protecting personal data, which is vital for maintaining trust in its technological advancements and objectives.

2. Introduction about GDPR

The GDPR sets the standard for data protection and privacy in the European Union and the European Economic Area[1]. It also regulates the transfer of personal data outside these regions. The regulation became enforceable on May 25, 2018, marking a significant step forward in data protection rights for individuals. GDPR impacts every organization that processes the personal data of individuals in the

[1] https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en

EU, irrespective of the organization's location worldwide, making it a critical consideration for international projects and collaborations.

2.1 Objectives of the GDPR Compliance Deliverable

The main goal of this GDPR compliance deliverable is to outline the necessary steps and measures the STEP project must take to ensure full compliance with GDPR. The objectives include:

1. Identifying and mapping all data processing activities within the project to understand where and how GDPR applies.
2. Developing a clear understanding of the roles and responsibilities of project participants in relation to data protection.
3. Establishing a comprehensive GDPR compliance strategy that includes procedures for data protection, data subject rights, data security, and breach response.

2.2 Scope of the GDPR in the Context of the EU Collaborative Project

The scope of GDPR compliance for the STEP project is broad, given the project's extensive data processing activities. These activities range from the collection and use of personal data in research and development to the sharing of information across the consortium, which includes EU and potentially non-EU entities. The project must ensure that all personal data processing is lawful, transparent, and secure, regardless of whether the data pertains to EU citizens or individuals in non-EU countries participating in the project.

The STEP project operates within the Horizon Europe framework, which emphasizes open science, innovation, and broad collaboration across EU and associated countries. As such, GDPR compliance is not only a legal requirement but also a fundamental aspect of the project's commitment to ethical research and innovation practices. Ensuring GDPR compliance will enhance trust among project partners, participants, and the broader community, and will contribute to the project's success by fostering a secure and respectful environment for data processing.

In the following sections, we will elaborate on the GDPR Compliance Framework, detailing the relevant GDPR principles, roles and responsibilities, and the link with other deliverables such as the Data Management Plan. This will provide a solid foundation for understanding and implementing GDPR compliance throughout the STEP project.

3. GDPR Compliance Framework

3.1 GDPR Principles Relevant to the Project

The GDPR is built around several key principles that ensure data is processed lawfully, fairly, and transparently. For the STEP project, the following principles are especially pertinent:

- **Lawfulness, Fairness, and Transparency:** Processing must be lawful, fair, and transparent to the data subject. This means the project must have a legitimate reason for processing personal data and must inform data subjects about how their data is being used.
- **Purpose limitation:** Data collected for the project must be for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- **Data minimization:** The project should only process the data necessary to achieve its objectives. This means collecting only the data needed for the specific purposes stated.
- **Accuracy:** Personal data must be accurate and kept up to date. Inaccurate data should be corrected or deleted promptly.
- **Storage limitation:** Personal data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and confidentiality (security):** Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
- **Accountability:** The project must be able to demonstrate compliance with all these principles.

3.2 Roles and Responsibilities

Within the GDPR framework, there are specific roles that entail different responsibilities:

- **Data Controller:** The entity that determines the purposes and means of processing personal data. In the context of the STEP project, this is the consortium as a whole.
- **Data Processor:** The entity that processes personal data on behalf of the controller. WP Leaders in the STEP project act as processors if they handle data under the instructions of the controller.
- **Data Protection Officer (DPO):** A designated expert responsible for overseeing data protection strategies and compliance. The project should appoint a DPO if the processing operations require regular and systematic monitoring of data subjects on a large scale or involve special categories of data. The STEP DPO is represented by the Project Coordinator, Serena RIZZOLO.

3.3 Link with Data Management Plan

The Data Management Plan (DMP) is a document that outlines how data will be handled during and after the research project, ensuring that data is managed according to GDPR requirements. The GDPR Compliance Framework and DMP are closely linked, as both aim to ensure that personal data is processed securely, lawfully, and transparently. The DMP should address aspects such as:

- The types of personal data collected, stored, and processed.
- The legal basis for processing.
- Measures to protect data and ensure privacy.
- Procedures for data subject rights fulfillment.

Incorporating GDPR compliance into the DMP from the outset ensures that data protection is not an afterthought but is integrated into the project's data management practices from the start.

The Data Management Plan is the deliverable D1.3 and is scheduled at Month 2.

4. Compliance Measures

4.1 Legal Basis for Data Processing

Identifying and documenting the legal basis for processing personal data is a cornerstone of GDPR compliance. The STEP project must determine the appropriate legal basis for each data processing activity, which includes:

- **Consent:** Obtaining clear and explicit consent from data subjects for processing their personal data for one or more specific purposes.
- **Contract:** Processing necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Legal Obligation:** Processing necessary for compliance with a legal obligation to which the controller is subject.
- **Legitimate Interests:** Processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

4.2 Rights of Data Subjects

The project must ensure mechanisms are in place to uphold the rights of data subjects, including:

- **Right to Information:** Informing individuals about the processing of their personal data.
- **Right to Access:** Allowing individuals to access their personal data and obtain copies of it.
- **Right to Rectification:** Correcting inaccurate personal data without undue delay.
- **Right to Erasure ('Right to be Forgotten'):** Deleting personal data when it's no longer necessary for the purposes for which it was collected.
- **Right to Restriction of Processing:** Temporarily halting the processing of personal data.
- **Right to Data Portability:** Enabling individuals to receive their data in a structured, commonly used format.
- **Right to Object:** Allowing individuals to object to certain types of processing.

4.3 Data Protection by Design and by Default

The project must integrate data protection into its processing activities from the outset, ensuring that only necessary data is processed. This involves:

- Implementing appropriate technical and organizational measures that ensure and demonstrate that processing is performed in accordance with GDPR.
- Default settings to ensure that only the data necessary for each specific purpose is processed.

4.4 Security Measures and Data Breach Protocols

To safeguard personal data, the project should implement security measures tailored to the risk level of the processing activities, including:

- Encryption and anonymization techniques.
- Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems.
- Regular testing and evaluation of the effectiveness of security measures.

In case of a data breach, the project must have protocols to promptly assess the risk to individuals' rights and freedoms and report the breach to the relevant supervisory authority within 72 hours, and to the data subjects without undue delay if the breach poses a high risk to their rights and freedoms.

4.5 Procedures for Handling Data Subject Requests

The project should establish procedures for responding to requests from data subjects exercising their rights under GDPR. This includes:

- Establishing a clear point of contact for data subjects.
- Setting timelines for response: generally within one month of receipt.
- Providing information and actioning requests free of charge, except in cases of unfounded or excessive requests.

5. Conclusion

Implementing the GDPR Compliance Framework in the STEP project is essential for making sure that all activities follow the strict data protection and privacy rules set by the GDPR. By carefully planning and applying compliance measures, and by continuously checking these efforts, the project can maintain high standards of data protection. This not only meets legal requirements but also boosts the project's reputation for being trustworthy and respectful of personal data privacy.

The main steps detailed in this document — from determining the legal basis for processing data to protecting the rights of individuals, embedding data protection from the start, ensuring strong security, and setting up clear ways to respond to requests from people about their data — are crucial for the project's commitment to follow GDPR. Following these guidelines helps the project not only to comply with the law but also to show its commitment to safeguarding personal data.

It will be important to regularly revisit and update the project's approach to GDPR compliance to reflect any changes in how data is handled, the project's goals, or in legal requirements. This ongoing process ensures that the project adapts to new data protection challenges and opportunities, keeping a high level of privacy and security.

In summary, focusing on GDPR compliance is fundamental to conducting ethical research and innovation within the STEP project. By integrating these principles into the project's operations, it sets a standard for responsible data management that reflects European values and contributes to the project's success in the competitive field of space technology.

Additional supporting documents are provided in the appendices and include a glossary of terms related to GDPR and a checklist for ensuring the project meets GDPR standards, to help put these compliance measures into action.

6. Appendices

6.1 Glossary of GDPR-related terms

Personal Data: Any information related to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as 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.

Processing: 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.

Data Controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Data Protection Officer (DPO): An expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

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

Data Subject Rights: The rights of individuals to control their personal data. These rights include access to data, correction, deletion, processing restriction, data portability, and objection to processing.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Legitimate Interest: Processing of personal data that is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

Data Minimization: The principle that personal data collected should be limited to what is necessary in relation to the purposes for which they are processed.

Accountability: The principle that the data controller is responsible for, and must be able to demonstrate compliance with, the GDPR principles relating to processing of personal data.

6.2 GDPR Compliance Checklist

Compliance Task	Description and Action Points	Done
Identify Personal Data	Identify if any personal data is included in the deliverable/report/material.	
Legal Basis for Processing	Confirm the legal basis for processing any personal data mentioned. Justify the inclusion of personal data based on GDPR legal grounds (consent, contract, legal obligation, etc.).	
Data Protection Impact Assessment (DPIA)	Determine if a DPIA is needed for the processing activities described.	
Anonymization and Pseudonymization	Apply necessary data anonymization or pseudonymization techniques. If personal data is not essential, consider whether it can be anonymized or pseudonymized.	
Data Subject Rights	Ensure information on data subject rights and how they can be exercised is included.	
Security Measures	Describe any data security measures relevant to the processing activities.	
Data Sharing and Transfers	Review and document any data sharing or transfers, ensuring compliance with GDPR.	
Consent and Withdrawal	If applicable, detail how consent is obtained and can be withdrawn.	
Retention Policy	Mention the data retention policy applicable to the data processed.	
Contact Information for Data Concerns	Include contact information for data protection inquiries (e.g., DPO contact details).	
Review for Sensitive Information	Ensure no sensitive or unnecessary personal data is included, unless absolutely necessary and legally covered.	

GDPR Statements and Disclaimers	Add necessary GDPR statements or disclaimers related to data processing. For materials to be disseminated publicly, ensure clear GDPR statements are included, especially regarding consent and data subject rights.	
Training and Awareness for Handling Data	Confirm that individuals involved in preparing the deliverable are trained on GDPR.	
Documentation and Record-Keeping	Ensure proper documentation of GDPR compliance efforts related to the deliverable. Maintain records of how personal data in the deliverable was processed and protected, in case of audits.	