PEERS
PracticE Ecosystem for standaRdS

Deliverable No. 1.3
Deliverable title – Ethical & Legal Aspects and Compliance Assessment

Date 30 April 2024

V1.0

Project Information

Project title	PracticE Ecosystem for standaRdS	
Project acronym	PEERS	
Project number	101074040	
Start date/ Duration	1st November, 2022	36 months
Topic	HORIZON-CL3-2021-DRS-01-04. Developing a prioritisation mechanism for research programming in standardisation related to natural hazards and/or CBRN-E sectors	

Work Package title	WP1: Project Coordination	
Task title	T1.4 Ethical & Legal Aspects and Compliance Assessment	
Deliverable title	D1.3 Ethical and Legal Protocol and Compliance Assessment	
Deliverable type	R- Document	
Doc. Version & WP no.	1	WP1
Due date	M18 - April 2024	
Lead Beneficiary	FIPRA International	
Leading author(s)		
Contributing author(s)	Jon Hall, Emma Loeber, Peter Tulkens	
Internal Reviewer(s)	Jon Hall	
SAB Reviewer(s)	David Crouch (TFC) 26/4/2024	
Release date	30/04/24	

Classification – This report is:									
Draft	X	**Final**		**Public**	X	**Sensitive**		**Confidential**	

Revision History

Date	Version	Author	Distribution/Substantive changes made
23-04-2024	v.01	Paul van der Werff (FIPRA)	First draft release to Internal Review.
26-04-2024	v.02	Paul van der Werff (FIPRA)	Second draft release to Internal Review
26-04-2024	V0.3	David Crouch	SAB Review
30-04-2024	V0.9	Paul van der Werff (FIPRA)	Final draft release for External Review
30-04-2024	V1.0	Blain Murphy (KPMG)	Submission to EC

Acknowledgement

This project has received funding from the European Union's Horizon Europe research and innovation programme under the Grant Agreement No. 101074040.

Disclaimer

This document reflects only the author's view and not those of the European Commission (EC). The EC and PEERS project partners are not responsible for any use that may be made of the data and information it contains and do not accept liability for loss or damage suffered by any third party as a result of using this data and information.

Table of Contents

List of acronyms and abbreviations

AI	Artificial Intelligence
CBRNe	Chemical, Biological, Radiological, Nuclear and explosives materials
CERIS	Community of European Research and Innovation for Security
ECB	External Complimentary Board
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
PEERS	PracticE Ecosystem for standaRdS
VR	Virtual Reality

EXECUTIVE SUMMARY

In EU Horizon projects, ethics and ethical compliance is an integral part of research. The ethical evaluation starts from the proposal phase and carries on throughout the project implementation. Ethical research conduct relative to the applicable legal framework is also significant for the quality and afterlife of research results. D1.3 looks into the ethical and privacy issues of the PEERS project, it will include ethical considerations and legal restrictions of data used in PEERS, as well as moral considerations regarding the use of human subjects in project activities.

The deliverable will first introduce the PEERS project and its purpose. Chapter 2 provides an overview of the ethical and legal framework while Chapters 3 and 4 explain how the PEERS project complies with this framework. Finally, Chapter 5 examines the considerations of post-project exploitation.

1 INTRODUCTION

1.1 INTRODUCTION TO PEERS

Funded by the European Commission's Horizon Europe Framework Programme, PracticE Ecosystem for standaRdS (PEERS) is a 36-month project that addresses the needs of the HORIZON-CL3-2021-DRS-01-04 call.

Launched on November 1st, 2022, PEERS aims to advance and reinforce the European Union's operational safety and security policies through the development of a practitioner-driven ecosystem focused on pre-normative / standardisation processes and supporting tools. The PEERS ecosystem supports the effective strengthening of preparedness and response in the field of CBRN-E through the practitioner-driven Better Practice Guide initiative, gamification, and e-Learning support. It primarily targets assisting Europe's CBRN-E practitioners, European research policymaking as well as other stakeholders including the research community and national standardisation bodies. A comprehensive engagement and consultation governance mechanism will be applied for the realisation of the ecosystem. Additionally, the ecosystem includes an integration capability to existing community-building platforms and a gamification strategy, aimed at encouraging solid user engagement, strengthening interactions activities, and furthering user training skills based on situational awareness.

PEERS brings together an experienced, multi-disciplinary team of specialists, to work together as a focused delivery team on meeting policymaker and practitioner expectations over the course of the project and deliver transformational change in the European CBRN-E environment.

1.2 PURPOSE OF THE DELIVERABLE

The PEERS consortium is committed to upholding the highest ethical and legal standards for the duration of the project, ensuring its sustainability beyond the development phase of the project. The PEERS project involves the development of an online ecosystem that gathers data on pre-normative

research and standardisation processes. It also aims to develop wider tools to support stakeholder engagement, such as a virtual reality system.

The purpose of the deliverable is to demonstrate that the PEERS consortium has taken the necessary steps to ensure that both the activities of the project and the PEERS solution is ethically and legally compliant. It will outline the ethical and legal framework to which the PEERS project is held, focussing on data protection, cybersecurity, and AI legislation, and showcase the steps taken to ensure compliance with established guidelines.

2 THE ETHICAL AND LEGAL FRAMEWORK

2.1 ETHICAL ISSUES IN RESEARCH

Research projects under the Horizon Europe programme are required to consider ethical and legal compliance in the conceptual and implementation phase of the project. In the context of the project, the following ethical considerations must be complied with:

- Respect the integrity and dignity of persons.
- Recognise the rights of individuals to privacy, personal data protection and freedom of movement.
- Honour the requirement for informed consent and continuous dialogue with research subjects.
- Respect the principle of proportionality

2.2 LEGAL FRAMEWORK IN ETHICS IN HORIZON EUROPE PROJECTS

Research projects under the Horizon Europe programme must adhere to legal obligations designated in the treaties and established regulations. The Lisbon Treaty and the charter of fundamental rights of the EU reference the fundamental rights such as the right to the integrity of a personal protection of personal data. Under the Lisbon treaty, the following articles should be considered:

Article 7 Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8: Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 13: Freedom of the arts and sciences

The arts and scientific research shall be free of constraint. Academic freedom shall be respected

Furthermore, Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe provides an overview of the ethical principles to adhere to.

Article 19 Ethics

1. Actions carried out under the Programme shall comply with ethical principles and relevant Union, national and international law, including the Charter and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols.

   Particular attention shall be paid to the principle of proportionality, to the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and to the need to ensure protection of the environment and high levels of human health protection.

2. Legal entities participating in an action shall provide:
   a. **an ethics self-assessment identifying and detailing all the foreseeable ethics issues** related to the objective, implementation and likely impact of the activities to be funded, including a confirmation of compliance with paragraph 1 and a description of how it will be ensured;
   b. a confirmation that the activities will comply with the European Code of Conduct for Research Integrity published by All European Academies and that no activities excluded from funding will be conducted;
   c. for activities carried out outside the Union, a confirmation that the same activities would have been allowed in a Member State; and
   d. for activities making use of human embryonic stem cells, as appropriate, details of licensing and control measures that shall be taken by the competent authorities of the Member States concerned as well as details of the ethics approvals that shall be obtained before the activities concerned start.
3. Proposals shall be systematically screened to identify actions which raise complex or serious ethics issues and submit them to an ethics assessment. The ethics assessment shall be carried out by the Commission unless it is delegated to the funding body….Ethics screenings and assessments shall be carried out with the support of ethics experts. The Commission and the funding bodies shall ensure the transparency of the ethics procedures without prejudice to the confidentiality of the content of those procedures.
4. Legal entities participating in an action shall obtain all approvals or other mandatory documents from the relevant national, local ethics committees or other bodies, such as data protection authorities, before the start of the relevant activities. Those documents shall be kept on file and provided to the Commission or the relevant funding body upon request.
5. Actions which do not fulfil the ethics requirements referred to in paragraphs 1 to 4 and are therefore not ethically acceptable, shall be rejected or terminated once the ethical unacceptability has been established.

The ethics requirements stipulated in the HORIZON-CL3-2021-DRS-01-04 call are included in the grant agreement in the form of deliverables.

2.3 LEGAL FRAMEWORK FOR DATA MANAGEMENT

Considering the primary potential ethical and legal issues that could arise in the PEERS project is associated with the handling of data, this section provides an overview of the legislative directives that guide the conduct of the project.

As developed in the PEERS management plan (D1.1), the data that will be handled within the PEERS project can be categorized into two types of data: open data (publicly available data – standards and stakeholders) and personal data.

Open Data
The Open Data Directive' (Directive (EU) 2019/1024) entered into force on 16 July 2019 is the guiding regulation with regards to access and handling of data generated by public sector bodies, such as a government departments, agencies, and standardisation bodies. The aim of the directive is to:

- Reduce the exceptions which allow public bodies to charge more than the marginal costs of dissemination for the re-use of their data.
- Facilitate research data resulting from public funding – Member States will be asked to develop policies for open access to publicly funded research data.
- Strengthen the transparency requirements for public–private agreements involving public sector information, avoiding exclusive arrangements.

Personal Data
The EU Legislation on the protection of Personal Data is governed by the following legislative documents:

- Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR)
- Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data
- Regulation (EU) 2018/1725 on the protection of natural persons regarding the processing of personal data by the EU institutions, bodies, offices, and agencies
- Guidelines on Transparency under Regulation 2016/679
- Guidelines on Personal data breach notification under Regulation 2016/679
- Guidelines on Consent under Regulation 2016/679
- Guidelines on Data Protection Impact Assessment (DPIA)

Each beneficiary is reminded that under the General Data Protection Regulation 2016/679, the data controllers and processors are fully accountable for the data processing operations, which means that every beneficiary is ultimately responsible for their data collection and processing. Any violation of the data subject rights may lead to sanctions as described in Chapter VIII, art.77-84 from the GDPR legislation.

3 DATA HANDLING IN THE PEERS PROJECT

3.1 SUMMARY OF DATA TYPES MANAGED IN PEERS

As specified in the Data Management Plan (D1.1), the PEERS project collects multiple types of data for the ecosystem demonstrator, and research applications.

It should be noted that certain CBRN-related data is sensitive and may require permission for use. Furthermore, depending on from where it is derived, it may be also considered export controlled under EU or national rules. This is addressed in section 3.2.4 below.

3.1.1 PERSONAL DATA

This category concerns information that relates to an identified or identifiable individual, or any information that obviously relates to a particular person and can be used to identify them. This includes personal data arising from registrations to the PEERS platform and that collected in surveys, interviews, and engagement activities.

3.1.2 OPERATIONAL AND OBSERVATIONAL DATA

This category encompasses both curated and raw data stemming from the implementation, testing, and operation of the demonstrators (operational data), as well as data derived from associated qualitative endeavours such as surveys, interviews, fieldwork, engagement activities (observational data), or events. It may contain personally identifiable information pertaining to individuals or organizations.

3.1.3 SIMULATION DATA

This type of data will be derived from models and modelling activities throughout the project. Ensuring the reproducibility of this data relies on understanding the input parameters, maintaining version control of both the input and software code, and documenting details about the running environment, including the operating system, release date, software dependencies, and so forth.

3.1.4 DERIVED OR COMPILED DATA

This data type will be obtained from data mining or statistical analysis. The reproducibility of this data is subject to the good documentation of original data. This is a key part of the role of the platform.

3.1.5 METADATA

Metadata refers to information about the data itself. The reproducibility of metadata hinges on the accessibility of the original data that the metadata describe. The anticipated data types (as outlined in Table 1) and data formats (detailed in Table 2) that were developed for the data management plan (D1.1) are described below.

Note that the current dataset is not storing editable files or data streams, with the dataset available only through a read-only download link. This prevents visitors to the platform from amending the dataset without oversight. In future, the PEERS project plans to put a ticket-system in place to allow visitors to submit an update to the group that curates the dataset. This will ensure the dataset remains up-to-date and meets data quality requirements while preventing unauthorised data manipulation.

Table 1: Expected types of Meta-data (From D1.1)

Meta data types	
Lists of stakeholders	European research projects outputs
Lists of standards	Better practice guide initiative outputs
Participants in activities (name, email address, affiliation)	Catalogue of approved equipment and services
Stakeholder opinions on pre/standards	List of identified research gaps and needs
European regulation framework related to the scope of PEERS	Technical data for the platform (user accounts, credentials, logs, etc.)
Statistics on platform use and users of the platform	Stakeholder data (regardless, if legal entity or natural person): name, title, affiliation, preferred language, relevant standardisation areas, standardisation body memberships, most important standards for the stakeholder, market area of operation, stakeholder feedbacks on standards

Table 2: Expected types of data formats (From D1.1)

Data Formats	
Online and offline documents (MS Office, Google docs, OpenOffice, PDF)	Source code
Standard formatted or codec compressed media files (videos, audio, pictures)	Compiled software components (py, js, jnlp, php, apk, exe etc.)
Metadata files (xml), website components (html, etc.)	Unstructured database files (json, raw).
Structured database files (csv, db etc.),	

3.2 DATA HANDLING COMPLIANCE ASSESSMENT FOR PEERS

The PEERS project is to take particular care of the following categories of data that may raise ethical risks:

- Complex processing operations and/or the processing of personal data on a large scale and/or systematic monitoring of a publicly accessible area on a large scale;
- Data processing techniques that are invasive and deemed to pose a risk to the rights and freedoms of research participants, or techniques that are vulnerable to misuse;
- Collecting data outside the EU or transferring personal data collected in the EU to entities in non-EU countries.

In line with the European legal framework (see section 1.5), internal compliance efforts of the PEERS project will focus on the following activities:

- Procedures for data collection storage, protection, retention, and destruction
- Protection of personal data
- Collection and/or processing of personal sensitive data

3.2.1 Data Protection Officers and GDPR compliance

As specified in the data management plan (D.1.1), KPMG FA, coordinator of the PEERS project, appointed Dr. Blain Murphy as a Data Protection Officer (DPO). His role is to assist in ensuring internal compliance to data protection obligations and provide advice regarding the project's Data Protection Impact Assessments (DPIAs).

It should be noted that respective partners are required to follow their own internal data protection and European GDPR regulations. In line with GDPR, individual beneficiaries are responsible for their own data processing, so the respective beneficiaries are to involve their own DPOs, who will ensure the implementation and compliance of the procedures and protocols in line with internal processes and national regulations. This also includes options to withdraw consent and procedures that must be in place to deal with privacy violations in a timely manner.

3.2.2 Procedures for data collection, storage, protection, retention and destruction

3.2.2.1 Data storage, retention and destruction principles

As described in the data management plan (D1.1), digital copies of all data will be stored for a maximum of three years after the conclusion of the grant award. All information and data gathered and elaborated will be suitably described in the respective Deliverables. All public Deliverables will be made available and archived on the project website (www.peers-project.eu) and through the EU Community Research and Development Information Service (CORDIS) for the project.

Furthermore, as specified in the data management plan (D1.1), KPMG hosts a SharePoint where all project documentation is stored. This includes, for example, deliverables (all versions), meeting agendas, minutes and presentations, and any other document used for the development of the project. By handling the documents in one overall platform, the PEERS consortium ensures easy collaboration and findability of project documentation. The SharePoint server is accessible by invitation only and access will be granted to consortium members after being vetted by the data management Officer.

Note that the current dataset is not storing editable files or data streams, with the dataset available only through a read-only download link. This prevents visitors to the platform from amending the dataset without oversight. In future, the PEERS project plans to put a ticket-system in place to allow visitors to submit an update to the group that curates the dataset. This will ensure the dataset remains up-to-date and meets data quality requirements while preventing unauthorised data manipulation.

3.2.2.2 PLANNED DATA CLASSIFICATION AND REVIEW PROCESS

Furthermore, as described in the data management plan (D1.1) and the data quality assurance process (described in D1.2), the PEERS project has put in place a data classification and review process which is described as follows:

Step 1 – Quality: The Technical Manager (Partner: UOG) reviews the dataset, deliverable or other result including metadata and FAIR compliance in Task 1.2 with involvement of an internal reviewer (selected from either consortium partners or stakeholders). If all reviewers say 'GO' without need to change, the Technical Manager transfers it to the Project Data Protection Officer (PDPO – Partner: KPMG-FA) for personal and sensitive data clearance.

Step 2 – Data Protection: The PDPO transfers the item to consortium member DPOs and to the assigned member of the security advisory board. If the result falls into category 1, it notifies the Technical Manager and stores the result on a secure cloud repository with restricted access. In case further use of data is not foreseen in the project, the PDPO archives the data and deploys encryption on it. Otherwise, it forwards to the Project Coordinator for a business sensitivity check.

Step 3 – Sensitivity: The Project Coordinator consults with the consortium and if there is a reason to put the result into category 4 (1-year embargo), the coordinator creates a memo including justification and revision date within 1 year. It then notifies partners and stores the result in a secure repository with access restricted to consortium members and other parties having an NDA and/or NCC with the consortium. If there is no need for embargo, it uploads the result to the most appropriate platform, includes a link on the Project website and shares it on social media. Partner, SFC, is responsible for curation and storage.

Note that where any dataset has a potential security risk, they have been transferred using a secure methodology.

3.2.2.3 ARCHIVING AND PRESERVATION

As described in D1.1, public deliverables will be archived on the project website (www.peers-project.eu). The internal datasets will be backed up periodically so that they can be recovered (for re-use and/or verification) in the future. Published datasets, raw or aggregated, will be stored within internal and external repositories and thereby ensure sustainability of the data collection. Records and documentation will be in line with common standards in the research fields to ensure adherence to standards, practices, and data quality. Data will be retained for a maximum of three years after the conclusion of the grant award. The expected commercialisation of the ecosystem will ensure long-term data curation and preservation beyond the project period.

3.2.3 PROTECTION OF PERSONAL DATA

The development of the PEERS ecosystem involves personal data collection and processing. As specified in the data management plan (D1.1), the PEERS project will respect the data protection principles which are: lawfulness, fairness, and transparency; purpose limitation; data minimisation;

accuracy; storage limitation; integrity and confidentiality; and accountability. More detail on the data protection principles is provided in Annex A.

Detailed requirements and descriptions of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants will be described by the tasks that implement them. Where necessary, data will be anonymised or pseudonymised. Data minimisation principles will be followed in line with applicable legislation, including GDPR.

3.2.4 HANDLING OF "SENSITIVE" DATA

The PEERS consortium is committed to the principle of data minimisation as specified by the legislation, primarily GDPR. Data procedures therefore do not involve the gathering of data considered sensitive such as ethnicity, political opinions, or religious/philosophical beliefs.

Since the PEERS ecosystem aims to be a repository of European and NATO standards in the field of CBRNe crisis management and response, "sensitive data" in the context of the project revolves primarily around copyrighted texts of standards or other "restricted" documents in this field. This will be particularly true of NATO standards, the majority of which are restricted. The PEERS Project will only publish NATO standards that are publicly available. Reference will be made to those standards not publicly available through external sources only. Some of this data may also be export controlled under EU or national rules and, where this is true, the PEERS project will ensure compliance by restricting the availability of this data to the country to which it originated. Where this is not possible, the data will not be published to the PEERS platform.

The PEERS Project generally aims to minimise issues associated with the handling of this sensitive data by ensuring that all information contained within the documents, products, standards, regulations, policies, and practices published to the PEERS ecosystem will be publicly and legally available.

As specified in the data management plan (D1.1) research data containing business sensitive information of consortium members or third parties (e.g., copyrighted texts of standards) will be held back for 1 year to enable participating industrial partners to secure International Property Rights (IPR). Furthermore, the Security Advisory Board, chaired by Ms Patricia Compard, and also includes Mr. Chris Singer and Prof. David Crouch will monitor deliverables for potential sensitive information.

3.2.5 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

To assess the potential risks with regards to privacy rights arising from the research activities, a Data Protection Impact Assessment (**DPIA) will be implemented as part of the development of the PEERS ecosystem**. A DPIA is a systematic process designed to identify and assess the potential risks to individuals' privacy rights arising from the processing of personal data in a particular project or activity. It involves identifying and assessing risks such as unauthorized access, data breaches, inaccuracies, and discriminatory impacts. It also involves considering the measures in place to mitigate these risks, such as **encryption, access controls, and data anonymisation.**

3.2.6 PROTECTING DATA FROM CYBERATTACK

The PEERS platform website is deployed on the web server and domain name of the University of Galway, ensuring it is thoroughly monitored and maintained by professional staff. The website also employs Secure Sockets Layer (SSL), an encryption-based internet security protocol to ensure privacy, authentication, and data integrity in internet communications. This is evidenced by the fact that the website is prefixed by HTTPS rather than HTTP (https://peers.universityofgalway.ie/).

Additional security measures include displaying the resources in the Knowledge Dashboard using a Javascript library (Highcharts) that has built-in security measures, as well as ensuring the regular update of the underlying content management system (WordPress).

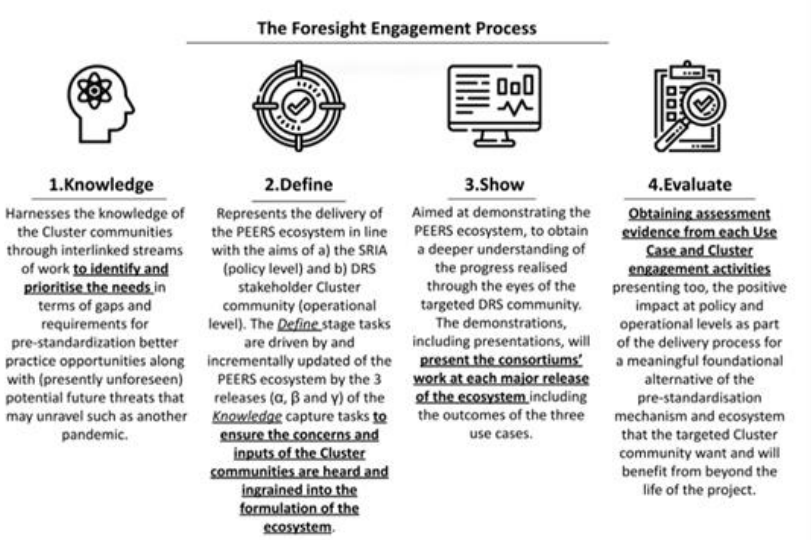
4 WIDER ETHICAL AND LEGAL COMPLIANCE CONSIDERATIONS

4.1 ENSURING ETHICAL AND LEGAL COMPLIANCE TO INTEGRITY AND DIGNITY OF PERSONS

Furthermore, in consultation with ethical and legal guidelines from EU authorities, the PEERS consortium has identified the following ethical considerations that must be complied with, with respect to maintaining the integrity and dignity of persons:

4.1.1 COMMUNITY ENGAGEMENT AND STAKEHOLDER CONSULTATION

Community engagement and stakeholder consultation is a central component of the PEERS project. Indeed, the primary methodology in developing and assessing the PEERS ecosystem is through a **co-creation approach** resulting in the practitioner-driven Better Practice Guide initiative, gamification and e-Learning support. Practitioners in the CBRNe and disaster risk management community are invited to join to **Co-Creation Group,** a voluntary consultation mechanism that forms a central pillar of PEERS's community engagement. As described in D2.1, the PEERS Co-creation Group, set up by TFC, is targeting groups of experts involved in the field of CBRN-E from policymakers and practitioners through to researchers and standardisation professionals. The principles of '*listen, learn, observe and then use the accumulation of knowledge to act and engage with the Community'* are applied. The following illustration provides an overview highlighting these principals in PEERS.



1. Figure Foresight engagement process for Co-Creation

Furthermore, **as described by D2.1**, the Crisis Management Innovation Network Europe (CMINE) will facilitate the creation of a **Demonstrator Group,** which aims to ensure practitioners (both individuals and representing organisations) contribute to and evaluate the new PEERS Ecosystem. CMINE uses a pre-existing Online Community Platform to host a network of global partners. The intention is that all PEERS partners will work to identify and 'sign-up' relevant members to partake in its activities, particularly its demonstrations and evaluations. A fully inclusive approach will be taken to all potential members of the Group, be they individuals or organisations. All opinions are welcomed, and diversity / innovation of thinking is encouraged. Within the Demonstration Group, a specific External Complimentary Board (ECB), specifically composed of experienced standardisation partners external to the consortium will be established during the lifespan of the project.

4.1.2 FAIRNESS AND EQUITY

With regards to **fairness and equity,** the PEERS consortium is committed to conduct its research activities in compliance with ethical standards such as ensuring the respect for human rights and fair distribution of benefits and burden. In this context, the project has established measures to ensure compliance. To assess the gender diversity of the PEERS project, the consortium conducted an internal gender diversity and inclusion questionnaire to ensure compliance with this ethical consideration. Continuous assessment and improvement on this domain will be required for the duration of the project.

Through the Co-Creation Group and internal reviews, the PEERS consortium will regularly evaluate the ethical implications of the platform's activities and make adjustments as necessary to address emerging issues or concerns.

Finally, with regards to ensuring that **gender diversity** is respected throughout the project, the PEERS consortium conducted an internal gender diversity and inclusion questionnaire to ensure compliance with this ethical consideration. The responses from the questionnaire indicate that 26

researchers and 22 non-researchers are participating in the project (48 members Total). Of which, 20 respondents of the questionnaire are women (12 researchers and 8 non-researchers). Continuous assessment and improvement on this domain will be required for the duration of the project.

4.2 ETHICAL AND LEGAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE ISSUES

In addition to the GDPR regulations (2.2), recent developments in AI regulation, including Regulation (EU) 2021/0106, have introduced specific requirements and safeguards for AI systems deployed within the EU, aimed at ensuring their safety, transparency, and accountability. Regulation (EU) 2021/0106 establishes a risk-based approach to AI regulation, categorizing AI systems based on their potential risk levels and imposing obligations such as data quality, traceability, and human oversight for high-risk AI systems. By complying with both GDPR and Regulation (EU) 2021/0106, the PEERS project aims to mitigate legal risks, uphold individuals' data rights, and ensure the responsible and ethical deployment of AI technology in our project.

5 ETHICAL AND LEGAL CONSIDERATIONS IN THE DISSEMINATION AND EXPLOITATION OF THE PROJECT OUTCOMES

The PEERS consortium is committed to adhere to ethical and legal considerations throughout the life-cycle of the project, but also in the communication, dissemination and exploitation of the project outcomes.

All consortium partners take responsibility for the communication and dissemination of results, as well as to ensure their visibility and accessibility. By implementing FAIR data principles, which advocates for data to be Findable, Accessible, Interoperable, and Reusable, the project will support the openness and re-use of data and therefore dissemination and replication. Further to this, stakeholder engagement is carried out in compliance with the EU GDPR. For example, prior to registering to the Co-Creation Group and Demonstrator Groups to access the PEERS ecosystem and receive any PEERS communication and dissemination materials and/or personal invitations to join PEERS events, relevant stakeholders have been asked to give consent to the collection and processing of their personal data, including e.g., name, surname, role/position, email. The data are stored securely, where access is only given to the partner team in charge of the platform design and management (i.e., UoG and TFC) and the team responsible for the coordination of the communication and dissemination activities (i.e., FORMIT). To collect feedback from the Co-Creation Group and Demonstrator Groups on the project activities and results, tailored interviews and Slido polls have also been organised under the coordination of FORMIT as WP6 leader. Answers have been analysed in an aggregated manner to ensure the anonymity of respondents.

As part of WP6, the sustainability efforts by PEERS partners have been instrumental in the definition of the project's business model, which is due at M35 (i.e., September 2025). At present, the project consortium has reported on the methodology applied to build the PEERS exploitation strategy in D6.6 (submitted in April 2023) and has been working on its update in D6.7, which is due at the same deadline as this deliverable (i.e., M18 – April 2024). Positioning focus groups involving the project

partners and the External Complementary Board members have also been held to foster discussion on the best scenario PEERS should opt for to ensure sustainability. As reported in D6.7, legal considerations have been made by FORMIT to build the case scenarios discussed for this purpose considering the 2x2 matrix and the SWOT analysis that have been developed. Further considerations will be made in relation to Intellectual Property Rights and their management within the PEERS Business Model, which will be reported on later in D6.8 at M35 and in the Data Management Plan (D1.1) updates.

6 CONCLUSION

This deliverable demonstrates that the PEERS consortium has taken the necessary steps to ensure that both the activities of the project and the PEERS solution is ethically and legally compliant. It outlines the ethical and legal framework to which the PEERS project is held, focusing on data protection, cybersecurity, and AI legislation, showcasing the steps taken to ensure compliance with established guidelines.

ANNEX A DATA PROTECTION PRINCIPLES

Principle	Analysis
Lawfulness, fairness, and transparency	**Lawful** processing means that the collection and processing of data relies upon a legal basis in accordance with Articles 6 and 9 of the GDPR. **Fair** processing means that data have not been obtained or otherwise processed through unfair means, deception, or without the data subject's knowledge, but rather in the interest of the individual concerned and within the bounds reasonably expected by the data subject**.** **Transparent** processing means that it should be transparent to natural persons that personal data concerning them are collected, used, consulted, or otherwise processed[1]. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used[2]. The transparency principle is further developed in Articles 12-14 of the GDPR, where it takes the form of an obligation to inform the data subjects.
Purpose limitation	This principle mandates that data be collected for specific, clear, and lawful purposes, and not used in ways incompatible with those purposes. The purposes for processing personal data must be established upfront, at the time of collection, to ensure lawful processing. Processing data for undefined or unrestricted purposes is unlawful, as it lacks clear boundaries[3]. Any further processing should not be incompatible with the initial purposes (Article 89 paragraph 1).
Data minimisation	Data minimisation means reducing the volume of personal data collected to what is genuinely required to attain the (specific) purpose of the processing[4]. The 'limited to what is necessary' criterion also requires 'ensuring that the period for which the personal data are stored is limited to a strict minimum[5].
Accuracy	Any personal data collected should be accurate and, where necessary, kept up to date. To this end, every reasonable step should be employed to ensure that personal data that are inaccurate, are erased or rectified without delay, having regard to the purposes for which they are processed.
Storage limitation	This principle stipulates that personal data should be kept only for as long as necessary to fulfil the purposes for which it was collected. Once the data is no longer needed, it should be erased or anonymised. Longer periods of retention are permitted solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

[1] Recital (39) of the GDPR.
[2] Ibid.
[3] de Terwangne C. (2020). Article 5: Principles relating to the process of personal data. In Kuner C. and others (eds). The EU General Data Protection Regulation (GDPR): A Commentary. New York: Oxford Academic, p. 315. https://doi.org/10.1093/oso/9780198826491.001.0001.
[4] EC (2021). Ethics and data protection, p.11.
[5] de Terwangne C. (2020), p.317.

	purposes and is subject to implementation of appropriate technical and organisational measures.
Integrity and confidentiality	This requires that personal data be processed in a manner that ensures its security, preventing unauthorised access, alteration, or disclosure. This principle applies throughout the processing lifecycle.
Accountability	The accountability principle under the GDPR signifies that data controllers are responsible for employing proper measures to adhere to the GDPR and also for demonstrating compliance with personal data protection laws[6]. The accountability requirements under the GDPR include other obligations, such as appointing a data protection officer or carrying out Data Protection Impact Assessments (DPIAs) for 'high risk' processing activities.

[6] Van Alsenoy, B. (2019). p. 44.


PEERS
PRACTITIONER-DRIVEN STANDARDISATION