Overwatch

Privacy, ethics and security report

Deliverable 6.3 - UPDATE

Work package: **WP6**
Dissemination level: **PU**
Lead partner: ALPHA
Authors: **Elizabeth A. Nerantzis**
Due date: **30/04/2026**
Submission date: **30/04/2026**

The OVERWATCH project has received funding from the Horizon Europe call "HORIZON-EUSPA-2021", topic HORIZON-EUSPA-2021-SPACE-02-52, under agreement No. 101082320

Deliverable	**Privacy, Ethics and Security Report**
Deliverable No.	D6.3 - update
Work Package	6
Dissemination Level	PU
Nature[1]	O
Author(s)	E.A. Nerantzis (ALPHA)
Co-Author(s)	-
Date	30/04/2026
Status	Final
Revision	ENG
Reviewed by (if applicable)	G.Vella, D.Sabia
Information to be used for citations of this report	Nerantzis E.A. (2026): Privacy, Ethics and Security report, D6.3, OVERWATCH. Horizon EUSPA Space 2021 Grant Agreement No 101082320.

Deliverable abstract	This is the update to the D6.3"Privacy, ethics and security" deliverable. It reports on the ethical, privacy and security requirements of the OVERWATCH project. More in detail, **it describes the privacy, ethical, and security aspects and considerations as well as the respective procedures that are in place at a EU and national level to ensure that the OVERWATCH project remains compliant with the applicable laws**. It also **provides guidelines and answers to privacy, ethical, data protection and security issues as well as on the technical approach that the OVERWATCH solutions will adopt for the relevant ethical issues**, in particular for the human involvement.
Keywords	#privacyrequirements, #ethicsrequirements, #securityrequirements #GDPRcompliance #EBIOScompliance #PESrequirement

[1] Nature of the deliverable: **R** = Report, **P** = Prototype, **D** = Demonstrator, **O** = Other

Table of Content

Figures

Tables

Document revision history

Version	Date	Modification reason	Modified by
1	17/01/2026	ToC	E.A. Nerantzis
2	23/04/2026	Issue 2. Update for M42: integration of AI Act, Data Act, PES survey, risk reassessment. Draft shared to ENG as peer reviewers	E.A. Nerantzis
3	29/04/2026	Peer review	D. Sabia, G. Vella

4	30/04/2026	Final draft share to Coordinator for EC submission	E.A. Nerantzis

List of authors, contributors and reviewers

No.	Name	Role	Organisation
1	Elizabeth A. Nerantzis	Author	ALPHA
2	Donato Sabia	Peer reviewer	ENG
3	Giuseppe Vella	Peer reviewer	ENG

Abbreviations

AI	Artificial Intelligence
AR	Augmented Reality
CEMS	Copernicus Emergency Management Service
CFR	Charter of Fundamental Rights
CR	Control Room
DGA	EU Data Governance Act
DMZ	Demilitarised Network
DPIA	Data Protection Impact Assessment
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ECR	Emergency Control Room
EGNSS	European Global Navigation Satellite System
EIAB	European Artificial Intelligence Board
ENISA	European Union Agency for Cybersecurity
EO	Earth Observation
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
PbD	Privacy-By-Design
PES	Privacy, Ethics and Security
PET	Privacy-Enhancing Technologies
PII	Personally Identifiable Information
TLS	Transfer Layer Security

Executive Summary

This document reports on the activities performed in Task 6.3 "Security, privacy and ethics", within the frame of Work Package 6 "Project Management" [RD01]. **It describes the ethical, privacy and security considerations as well as the respective procedures that are in place at European and national level to ensure that the OVERWATCH project remains compliant with the applicable laws. It also provides guidelines and answers to ethical, privacy, data protection and security issues as well as on the technical approach that the OVERWATCH solutions adopt for the relevant ethical issues, in particular for human involvement.** Two versions of this deliverable have been foreseen. This document represents Issue 2 (Final) of the "Privacy, ethics and security report":

Version	Content	Due date
Issue 1 (First Draft)	Guidelines and methodologies to ensure that privacy legislations are not infringed (such as General Data Protection Regulation and EU Data Act) on the protection of individuals, with regards to the processing of personal data. Preliminary identification of the ethical issues related to the specific aim of the project, and assessment of potential threats related to privacy, ethics and/ or security that may appear during the project, with suggested countermeasures to overcome them.	M12 (Oct 2023)
Issue 2 (Final)	Updated regulatory framework reflecting the entry into force of the EU AI Act and the EU Data Act. Updated information on the ethical issues and assessment of potential threats related to privacy, ethics and/or security that have emerged during the project, with suggested countermeasures. Outcomes of the internal Consortium PES survey conducted under Task 6.3.	M36 (April 2026)

The OVERWATCH Ethics and Security Manager (ESM) was identified and appointed early on in the project. The ESM is responsible for providing advice and coordinating activities for what concerns the fulfilment of the ethical obligations of OVERWATCH. The ESM is supported by the appointed Data Manager for certain activities, to ensure that all data collection and processing is carried out according to EU and national legislation and that ethics, privacy and data protection-related concerns are addressed, monitored and observed during the project duration.

In this context, the Privacy, Ethics and Security (PES) requirements and considerations have been identified and outlined. In particular:

Privacy. Applicable and reference principles together with main considerations are outlined for OVERWATCH, coming from several legal acts within the EU Law that address and regulate the issue of data protection (See section 3.1). These are:

- General Data Protection Regulation - GDPR (EU Regulation 2016/679);
- ePrivacy Directive - Directive 2002/58/EC (including EU Cookie Directive – Directive 2009/136/EC);
- EU Data Governance Act – Regulation (EU) 2022/868;
- EU Data Act - Regulation (EU) 2023/2854;

- Charter of Fundamental Rights (CFR) of the European Union (2012/C 326/02);
- Council Framework Decision (2005/222/JHA); and
- EU Artificial Intelligence Act – Regulation (EU) 2024/1689.

Compared to Issue 1, this update integrates two significant regulatory developments. The EU Data Act, which entered into force on 11 January 2024 and has been applicable since 12 September 2025, is assessed for its relevance to the OVERWATCH operational context, in particular Chapter V on business-to-government data access during public emergencies, the IoT data-sharing provisions potentially applicable to connected devices such as drones and AR equipment, and the cloud switching and interoperability requirements (see Section 3.1.4). The EU AI Act, published in the Official Journal on 12 July 2024 and entered into force on 1 August 2024, is described in its enacted form with its risk-based classification framework, phased implementation timeline, and governance architecture. The relevance of the AI Act for OVERWATCH is assessed in light of the internal PES survey findings (see Section 3.1.7 and Section 4).

The **privacy requirements** have been drafted and is based on the Privacy-by-Design approach selected for OVERWATCH (detailed in 3.2). They are summarised hereafter:

#	Principle	Description
1	Proactive not reactive; Preventative not remedial	PbD anticipates and prevents privacy invasive events beforethey happen.
2	Privacy as the default setting	PbD delivers the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact. No action is required on the part of the individual to protect their privacy — it is built intothe system, by default
3	Privacy embedded into design	PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
4	Full functionality – positive-sum, not-zero-sum	PbD seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through adated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.
5	End-to-end security – full lifecycle protection	PbD, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensuresa secure lifecycle management of information.
6	Visibility and transparency – keep it open	PbD seeks to assure all stakeholders that whatever thebusiness practice or technology involved, its component parts and operations remain visible and transparent, to users and providers alike.

7	Respect for user privacy – keep it user-centric	PbD requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

The "Expression des Besoins et Identification des Objectifs de Sécurité" (EBIOS) risk management approach for data privacy and protection has been selected for OVERWATCH. This approach follows the guidelines of Privacy-by-Design methodologies provided by the GDPR and allows the analysis of the risk posed to privacy by the processing of personal data (see Section 3.2). It is made up of the following steps: 1) Define the Context; 2) Define the potential Feared Events; 3) Define the scenarios of Threats; 4) Analyse risks; and 5) Identify measures for risk mitigation. The approach has been implemented since the early stages of platform development and is applied whenever a new processing operation is designed.

Ethics. The legal and ethical framework for the involvement of humans in the OVERWATCH project is provided. In particular, specific reference to the following is outlined: the EU General Data Protection Regulation (GDPR); the EU Data Act; the EU AI Act; the Charter of Fundamental Rights of the European Union; the ePrivacy Directive; and the European Code of Conduct for Research Integrity (see Section 3.3). Moreover, since the early stages of the project an "ethical checklist" has been used in order to assess the presence of possible issues, especially at the beginning of research activities. The checklist is the following:

Item	Check (Yes/No)
Is the proposed research adequately designed, so that it will be of informational value?	YES
Does the research pose risks of physical or psychological harm to participants by using deception, obtaining sensitive information or exposing them for risks in terms of safety and/or security hazards?	NO
If risks exist, does the research adequately control these risks by including procedures, such as debriefing, removing or reducing risks of physical harm, or obtaining data anonymously? If that is not possible, will the research procedures guarantee that information will remain confidential?	YES
Is there a provision for obtaining informed consent from all participants? Will the researcher provide sufficient information to potential participants so that they will be able to give their informed consent? Is there a clear agreement in writing (the informed consent form) between the researcher and the potential participants? The informed consent should also make it clear that the participant is free to withdraw from the study at any time.	YES
Will participants receive adequate feedback at the completion of the study, including a debriefing if that is necessary?	YES
Do I as researcher accept my full responsibility for the ethical and safe treatment of all participants?	YES
Have I as part of the project informed the Ethics Board about the ethical issues I have identified and of which I am aware?	YES

The items posed in this checklist will be monitored and updated in order assess potential ethical concern that may arise during the execution of the OVERWATCH project. Also, an Informed Consent template has been developed, this is provided in Annex.

Security. When collecting personal data, ethical and legal obligations to ensure that participants' information is properly protected are in place. This is fundamental to safeguarding their rights and freedoms, and minimising the risks related to data processing. As explained in D6.2 Data Management Plan [RD07], the **data collected by OVERWATCH partners will be preserved in their own premises. Each partner has an accountable person for its data management and protection. Each OVERWATCH organisation has already in place high security measures and procedures aimed to avoid breaches in confidentiality and misuse of the collected data**. The security aspects have been analysed identifying the issues that may potentially affect the OVERWATCH system at the level of primary assets (data) and supporting assets (software and hardware architecture). In this context, a series of measures and actions have been set up in place, and implemented, in order to identify events that could affect OVERWATCH data collection (such as feared events and threats); analyse the level of risk; identify the measures to be adopted for risk mitigation; and identify measures on primary and supporting assets (see Section 3.4.2). The identified OVERWATCH potential measures on primary assets are the following:

Potential measure	Description
Non-disclosure of personal and location data	Data related to the profile of the users must not be disclosed. These data will be only accessible to their direct owners and to users responsible for the management of the OVERWATCH platform. To prevent disclosure of unnecessary information (individual identity and location of an individual). The exact location of users will not be tracked to not disclose private information. Nonetheless, it is important that all the information provided in the report must be geo-localised. This requirement is directly connected to the previous one, i.e. non-disclosure of personal data. The approach adopted in OVERWATCH to avoid location tracking will be based a data separation technique that decouples the user personal data from the report's locations. User' personal data will be never displayed in the graphical interface, where the reports will be associated only with the user type (professional).
Data anonymization and pseudonymisation	Whenever possible, personal data shall be anonymised in such a way that the individuals concerned are no longer identifiable by any means reasonably likely to be used. Where re-identification remains possible, including where the identity of the original reporting user needs to be retrieved, the data shall be treated as pseudonymised personal data and shall remain subject to applicable GDPR obligations. Any re-identification of the original reporting user shall be strictly limited to duly authorised personnel, and protected through appropriate technical and organisational measures, including role-based access controls, separation of identifying information and associated re-identification keys, encryption, secure key management, and audit logging. Information derived from generated reports shall, whenever possible, be used and shared only in aggregated and anonymised form. Direct identifiers and other information that may enable identification shall be removed, generalised, masked, or otherwise transformed, unless their retention is strictly necessary, lawful, proportionate, and subject to appropriate safeguards.

Data minimization	Data minimisation at the earliest stage of processing is a core concept of privacy-enhancing technologies. In OVERWATCH only personal data necessary for the respective purpose of the project will be collected and processed. In the data collection stage and in the following processing stage, personal data treatment willbe minimised as much as possible. Consequently, personal data will be erased or effectively anonymised as soon as it is not anymore needed for the given purpose.
Image objects detection and blurring	The detection of faces or other sensible objects (e.g., car plates) from images collected via the chatbot application and/or is another privacy issue that must be addressed. This aspect is still under discussion whether blurring is necessary as the type of client foreseen is to be found in the law enforcement and decision-making authorities. Yet, should it be required OVERWATCH will exploit one of the many open-source libraries and APIs for image detection and blurring that are still available on the market avoiding 'reinventing the wheel'.

Identified OVERWATCH potential measures on secondary assets are the following:

Potential measure	Description
Administration	To deliver consistent security administration and management, OVERWATCH will need a set of tools to define, administer and manage security policies consistently across the whole platform. Besides the technical aspects of risk mitigation, processes will also be inspected and detailed to identify the person/s who will be responsible for each task/activity/process. Where required, a Data Manager is designated to advise on and monitor compliance with data protection obligations. The Data Manager's contact details are published and communicated to the competent supervisory authority, and the Data Manager acts as a contact point for the supervisory authority on issues relating to processing. An Ethics and Security Manager (ESM) supports the operational implementation of security and privacy policies, coordinates awareness and training activities, and facilitates internal workflows (e.g., incident handling and evidence collection) in cooperation with the Data Manager and relevant technical and management roles. In the event of a personal data breach, notification to the supervisory authority and, where applicable, communication to affected data subjects is handled by the controller in accordance with GDPR requirements, with the Data Manager and ESM supporting the assessment, documentation, and mitigation actions.
Authentication and Perimeter Security	Users need to reliably identify themselves and then have that identity propagated throughout the OVERWATCH platform to access resources. All the users must be authenticated on the OVERWATCH platform. Moreover, user credentials must be stored securely. Since the OVERWATCH platform has been designed as a collection of remote services, the main authentication mechanism that will be adopted will be based on a token-sharing authentication through active sessions. In more details, each service communicating with the OVERWATCH platform is required to establish a trusted communication session. In the "handshaking" phase, when two services interact (e.g., AR, drones) for the first time, an encrypted token will be generated by the OVERWATCH platform and provided to each client service. This token will be used by clients to authenticate their requests. Similarly, the OVERWATCH platform will enable each client request

	only on the bases of a successful token verification.
Authorization - Restricted access to data and report information	Security administrators can define security policies at the database, table, column, and file levels, and can administer permissions for specific LDAP-based groups or individual users. Rules based on dynamic conditions such as time or geolocation can also be added to an existing policy rule. A permission-based mechanism may be integrated into the OVERWATCH platform to implement different access level for the information.
Secure communication and data transfer	All the information collected in a report by a first responder must be transmitted to the OVERWATCH platform on secure and trusted communication channels (e.g., based on HTTPS). The same also applies to data delivered to the users (e.g., through their chatbot app). The main focus is to avoid the leakage of the information, as well as malicious sniffing of sensible data. To this end, proper set of certificates will be generated and used to establish secure communications on the channels. The main protocol used for the data exchange will be the HTTP, since the OVERWATCH platform will expose data and functions through a series of RESTful services. Therefore, the protocol adopted for data exchange in the communication between the OVERWATCH platform and external modules will be the HTTPS, that combines HTTP with the SSL encryption. The same encrypted channel will be also used to exchange the token generated for authentication.
Data backup and recovery	Table 3-12 reports the risk treatment measures illustrated in this paragraph and in section 3.4.2.2 describing how they are adopted to mitigate each of the presented list and which is the effect in terms of re-estimation of severity and likelihood levels. Also, thanks to MinIO - single node multi drive - replicable and scalable on more logic file systems are enabled, allowing the data backup and recovery as well.
Secure data storage	The sensible information gathered from user-generated reports will be saved securely inside the OVERWATCH platform. The same strategy is also required for users' profile information and credentials. Different techniques can be adopted for these two categories of data. In the former case, a signature (hash) based encryption on the data could be applied. This is a one-way encryption strategy that would have the only objective of uniquely identify the user who created and/or validated the report data. On the other hand, two-ways encryption (i.e., encoding-decoding) can be adopted to securely store users' credentials. The same two-ways encryption strategy can be applied to data stored in the OVERWATCH platform data lake. More specifically, all the data collected from external sources that are under restricted privacy constraints outside the scope of the OVERWATCH project must be guaranteed.
Audit	Auditing is the monitoring and recording of selected user data actions. It can be based on individual actions, such as the type of query statement executed, or on combinations of factors that can include username, application, time, etc. Security policies can trigger auditing when specified elements are accessed or altered, including the contents within a specified object. Audit logs are retained for no longer than necessary for the purposes of accountability, security monitoring, and incident investigation, in line with the storage limitation principle. In the OVERWATCH project, the current operational retention period for audit logs is set to 1 year.

The risk analysis performed in Section 3.4 has been updated in this issue to reflect the evolution of the project since Issue 1. The comparison between the risk map presented in Issue 1 and the updated assessment confirms a tangible and measurable improvement in the overall risk posture, with all nine feared events repositioned to levels that can be considered acceptable for the system in the current implementation context.

Survey on Privacy, Ethics and Security Requirements. In the context of Task 6.3, an internal consortium PES survey was carried out in order to verify, on the basis of direct input from the project partners, the extent to which the assumptions, data flows and safeguards described in this deliverable remain consistent with the actual implementation activities carried out since Issue 1. The survey collected responses from five partners involved in the development and validation of the OVERWATCH platform and was structured around four thematic domains: data flows and personal data processing; human involvement and ethical considerations; AI-based components and their preliminary qualification under the EU AI Act; and the evolution of the security posture. The main findings are summarised as follows:

- The data flows originally described have remained unchanged, confirming the continued validity of the privacy analysis and the Privacy-by-Design assumptions set out in Section 3.2.
- No personal data has been processed in practice by the surveyed partners, and no GDPR roles or DPIA obligations have been triggered to date.
- Human involvement has already been substantial across pilots, demonstrations, workshops and training activities; informed consent forms were used where applicable, and no ethical concerns or sensitivities have been identified.
- One partner reported AI-based components in decision-support contexts, preliminarily classified as minimal risk under the EU AI Act, with human validation and uncertainty indicators applied as safeguards. This classification is considered provisional and subject to reassessment as the technical components mature and as the deployment context evolves.
- The security posture of the consortium remains controlled, with no major incidents reported, one dependency-related risk identified, and targeted improvements in authentication, encryption and audit logging reported by one partner, which is fully consistent with the risk treatment framework described in Section 3.4.

In light of the above, at this stage no major issues are present in relation to any of the three pillars addressed by this deliverable. The governance structures, risk treatment measures and ethical safeguards currently in place provide a coherent and proportionate response to the risks and obligations identified.

As the project approaches its conclusion and the regulatory landscape continues to evolve - notably with the full applicability of the EU AI Act and the EU Data Act, and the ongoing Digital Omnibus negotiations[2] - the consortium is confident that the governance framework, risk management methodology and ethical safeguards established through this deliverable provide a solid and adaptable

[2] Digital Omnibus negotiations refer to ongoing policy discussions among EU institutions aimed at improving coherence and reducing regulatory fragmentation across the Union's digital acquis, including instruments such as the General Data Protection Regulation, the AI Act, the Digital Services Act, and the Data Act. These discussions do not currently correspond to a single legislative proposal or structured interinstitutional negotiation (e.g., trilogues), but rather reflect a broader regulatory alignment effort.

basis not only for the remaining project activities, but also for the responsible transition of the OVERWATCH solution towards future operational deployment.

1 Introduction

1.1 Brief overview of OVERWATCH

OVERWATCH aims to create a more intuitive, decentralised, informed, and precise system for several types of disasters, deployable in several phases of the disaster. The developed system will ensure a safer, more resilient, and capable response infrastructure, carrying out the crisis operation more cohesively. Leveraging on the state-of-the-art approach, OVERWATCH will design and develop a backend management platform that will cover the whole lifecycle of data management going from the data ingestion, harmonization, standardization, and data processing into exploitable information.
Being supported by EGNSS (European Global Navigation Satellite System) and CEMS (Copernicus Emergency Management Services), the project aims to develop an Integrated holographic crisis management map to improve communication, information gathering, and coordination among disaster response teams, The system will be validated through two demonstrations in different countries. Extensive use of state-of-art Artificial Intelligence techniques will guarantee to extrapolate valuable information coupling the variety of EO (Earth Observation) data with data collected from other sources (e.g., drones). This data will be stored in a dedicated Geospatial repository within the Management backend platform, which will be directly linked with an AR (Augmented Reality) user interaction/display module, providing the users with an immersive and dynamic overview of the event.

1.2 Purpose of the document

The present document reports on the activities performed in Task 6.3 “Security, privacy and ethics”, within the frame of Work Package 6 “Project Management”[RD01].
Privacy and security aspects will be constantly monitored during the project execution following the guidelines of the EU legislation on electronic data processing and transmission over networks, and any changes in the legislation that could occur during the project and which may have an effect on the ongoing project. **The present document aims to provide guidelines and methodologies to ensure that privacy legislations are not infringed** (such as the Directive 95/46/EC and the General Data Protection Regulation) **on the protection of individuals, with regards to the processing of personal data**. Finally, **all the ethical issues related to the specific aim of the project will be analysed and presented**. In case specific threats related to privacy, ethics and/ or security will appear during the project, countermeasures will be suggested to overcome them.
Two versions of this deliverable have been foreseen [RD01]. This document represents the final issue of the D6.3 “Privacy, Ethics and Security Requirements” document:

Version	Content	Due date
Issue 1 (First Draft)	Guidelines and methodologies to ensure that privacy legislations are not infringed (such as General Data Protection Regulation and EU Data Act) on the protection of individuals, with regards to the processing of personal data. Preliminary identification of the ethical issues related to	M12 (Oct 2023)

	the specific aim of the project, and assessment of potential threats related to privacy, ethics and/ or security that may appear during the project, with suggested countermeasures to overcome them.	
Issue 2 (Final)	Updated regulatory framework reflecting the entry into force of the EU AI Act and the EU Data Act. Updated information on the ethical issues and assessment of potential threats related to privacy, ethics and/or security that have emerged during the project, with suggested countermeasures. Outcomes of the internal Consortium PES survey conducted under Task 6.3.	M36 (April 2026)

Table 1-1 PES requirement deliverables content – short description

1.3 Structure of the document

The document is structured/organised as it follows:

- Section 1 opens the deliverable with a brief overview and introduction
- Section 2 introduces the OVERWATCH ethics and security manager and the relations with the project's Data Protection Officer
- Section 3 presents the privacy, ethics and security aspects, explaining the regulatory framework and diving then into the details of the requirements related to each of the above categories
- Section 4 PES survey outcomes
- Conlusions

2 OVERWATCH ethics and security manager

Due to the involvement of public/private stakeholders and due to the necessity to collect, store and process data from different sources, including personal data; several ethical and data protection aspects (e.g., guarantee the anonymity of the information, ethical approvals andconsent forms, privacy policy, etc.) should be monitored and treated during the development of the project and its continuity. To ensure compliance with the ethics guidelines and requirements set out by the EC for the Horizon Europe Programme[3], an Ethics and Security Manager (ESM), i.e., Ms. Elizabeth A. Nerantzis (en@alphacons.eu) from ALPHA Consult, was appointed for OVERWATCH and is responsible for providing advice and coordinating activities for what concerns the fulfilment of the ethical obligations of OVERWATCH [RD01]. Working in full collaboration with the ESM, the project' Data Protection Officer (DATA MANAGER) was appointed - Mr. Federico Monteforte (federico.monteforte@ithacaweb.org) from ITHACA – in order to coordinate the data management assuring usability, accountability and quality of the data and the best way to valorise them [RD01] [RD07]. Also, OVERWATCH's ESM supports the DATA MANAGER, to ensure that all data collection and processing is carried according to EU and national legislation and that ethics, privacy and data protection-related concerns are addressed, monitored and observed during the project duration. Going further into detail, the ESM is in charge to ensure ethics and security

[3] Horizon Europe requirements: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf

clearance and compliance with national and international directives, standards and clauses. The ESM may screen the project deliverables for ethics and security before they are submitted to the European Commission and identify any potential misuse or dual use of the technical solutions under development. Moreover, the ESM will be assisted by specific competences available from a key person in the Consortium. The ESM will report directly to the Project Manager and through it to the Project Board. In the deliverables concerning design issues, the Ethics and Security Manager will make sure that each use case describes in detail how these issues have been approached:

- Detailed information on privacy/confidentiality and the procedures that will be implemented for data collection, storage, protection, sharing policies, retention and destruction and confirmation that they comply with national and EU legislation;
- The ethical consent protocols developed for each use case, and copies of the final Informed Consent Forms and Information Sheets (these items are provided in Annex);
- A detailed description of security measures implemented to prevent improper use, improper data disclosure scenarios and 'mission/function creep'. In addition, the potential "unforeseen usage" implications of the research will be examined and reported.

3 Privacy, ethics, and security aspects

Data privacy, data security and ethics are important aspects of research and innovation in the EU, especially in Horizon Europe projects. Hereafter a brief overview of some relevant EU legislation regarding these topics, and that will be further detailed within the context of the project:

- The EU General Data Protection Regulation (GDPR) is the main legal framework for the protection of personal data in the EU. It applies to any processing of personal data by EU entities or in the EU territory, regardless of where the data subjects are located. It grants data subjects various rights, such as the right to access, rectify, erase, restrict, object and port their data. It also imposes obligations on data controllers and processors, such as the duty to inform, obtain consent, ensure security, report breaches, conduct impact assessments and appoint data protection officers. The GDPR also regulates the transfer of personal data to third countries or international organisations, based on adequacy decisions, appropriate safeguards or derogations. The GDPR is directly applicable in all EU Member States since 25 May 2018 [RD02].
- The ePrivacy Directive is a specific legal instrument that complements and particularises the GDPR for the electronic communications sector. It regulates the confidentiality of communications, the use of cookies and other tracking technologies, the sending of unsolicited commercial communications and the processing of traffic and location data.
- The Charter of Fundamental Rights of the European Union is a legally binding document that enshrines the rights and freedoms of EU citizens and residents. It includes, among others, the right to respect for private and family life (Article 7), the right to protection of personal data (Article 8), the right to freedom of expression and information (Article 11), the right to education (Article 14), and the right to good administration (Article 41). These rights are relevant for research and innovation activities that involve personal data or affect other aspects of human dignity and autonomy [RD04].

- EU Data Governance Act (DGA) is a new regulation that aims to make more data available and facilitate data sharing across sectors and EU countries, in order to leverage the potential of data for the benefit of European citizens and businesses. It provides a framework for trustworthy data sharing that respects EU values and principles, such as data protection, privacy, security, transparency, accountability and democracy. The DGA improves data privacy and data security by introducing several measures and safeguards, such as: i) applying the GDPR to any processing of personal data within its scope and granting data subjects various rights and guarantees regarding their personal data; ii) regulating the re-use of certain categories of protected data held by public sector bodies that cannot be made available as open data and imposing technical requirements to ensure the privacy and confidentiality of data in re-use situations; iii) establishing a new category of data intermediaries that function as trustworthy organisers of data sharing or pooling within common European data spaces and requiring them to comply with high standards of transparency and accountability; iv) encouraging the sharing of data for altruistic purposes through a mechanism called data altruism and providing for rules and safeguards to ensure that data altruism is based on informed consent, respect for fundamental rights and ethical principles.The Data Governance Act entered into force on 23 June 2022 and is applicable since September 2023 [RD05].
- The Ethics Guidelines for Trustworthy AI are a set of non-binding principles and recommendations -however relevant- developed by a High-Level Expert Group on Artificial Intelligence appointed by the European Commission. They aim to ensure that AI systems are developed and used in a way that respects human values and fundamental rights, such as dignity, fairness, non-discrimination, privacy, transparency, accountability and democracy. The guidelines propose a framework for trustworthy AI based on four ethical principles (respect for human autonomy, prevention of harm, fairness and explicability) and seven key requirements: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being and accountability. They also provide an assessment list for self-evaluation of AI systems [RD06].

In this framework, data privacy, security, and ethics are addressed by OVERWATCH as a very important part of this human-centered approach and is based on software testing and validation operations involving adult human subjects.

All activities will comply with the established European and national rules on ethics, privacy and data security, and will be guided by well-established ethical and data protection principles,, such as informed consent, privacy by design and by default, and secure data management practices and data minimisation, ensuring that only the minimum amount of personal data necessary to achieve the project objectives is collected.

All activities will comply with applicable European and national rules on ethics, privacy and data security, and will be guided by well-established ethical and data protection principles, including informed consent, privacy by design and by default, secure data management practices, and data minimisation, ensuring that only the minimum amount of personal data necessary to achieve the project objectives is collected.

Moreover, addressing the FAIRness of data[4], the Council of the European Union emphasises that "the opportunities for the optimal reuse of research data can only be realised if data are consistent with the FAIR principles[5] (findable, accessible, interoperable and re-usable) within a secure and trustworthy environment" (Council conclusions on the transition towards an open science system). The FAIR principles are mentioned in the Communication "European Data Strategy (2020)" by the European Commission as a way to implement interoperability.

In this context, it is worth highlighing that specifically related to data security, the FAIR principles provide some guidance on how to improve the findability, accessibility, interoperability, and reusability of data, but they do not explicitly address data security issues. Yet, some of the FAIR principles can be interpreted and implemented in ways that enhance data security, such as:

- Assigning globally unique and persistent identifiers to data and metadata can help track and audit data usage and provenance, as well as prevent data loss or duplication.
- Using standardised and open protocols for data retrieval and access can help ensure data integrity and authenticity, as well as enable authentication and authorisation mechanisms when necessary.
- Applying clear and accessible data usage licenses to data and metadata can help define the rights and obligations of data providers and users, as well as protect data privacy and confidentiality.
- Following domain-relevant community standards for data and metadata can help ensure data quality and compliance with ethical and legal requirements.

However, data security also depends on other factors that are not directly covered by the FAIR principles, such as:

- The technical infrastructure and environment where data are stored, processed, and transferred, which should be secure, reliable, and resilient to threats and attacks.
- The organisational policies and procedures that govern data management and governance, which should be transparent, consistent, and enforceable.
- The human behaviour and culture that influence data practices and attitudes, which should be aware, responsible, and accountable.

Therefore, to assure data security in the framework of FAIR principles, one should consider not only the FAIR principles themselves, but also the broader context and implications of data stewardship. In light of this, the following strategies presented enable the involved organizations to strike a balance between data security and FAIRness of data, ensuring that data is both protected and accessible for research, innovation, and societal benefit.

3.1 Privacy requirements and considerations

Privacy is enabled by the protection of the personal data. There are several legal acts within the EU Law that address and regulate the issue of data protection. These are:

[4] In response to DRS, comment n.1.

[5] Source used: https://www.go-fair.org/fair-principles/

- General Data Protection Regulation – GDPR EU Regulation 2016/679);
- ePrivacy Directive - Directive 2002/58/EC (including EU Cookie Directive – Directive 2009/136/EC);
- EU Data Governance Act - Regulation (EU) 2022/868
- EU Data Act - Regulation (EU) 2023/2854
- Charter of Fundamental Rights (CFR) of the European Union (2012/C 326/02); and
- Artificial Intelligence regulatory framework (EU AI Act).

The next sections will present the relevant principles and information applicable within the context of the OVERWATCH project.

3.1.1 EU GDPR

The "General Data Protection Regulation (GDPR) - Reg. EU 2016/679" is a EU law which entered into force in 2016, directly applicable law in all Member States of the European Union on 25 May 2018, following a two-year transition period. The GDPR has replaced the previous Data Protection Directive (95/46/EC) and its national implementations. Being a Regulation, and not a directive, GDPR does not require any EU Member State to pass any enabling legislation through national law and is directly binding and applicable [RD02].

The GDPR lays down rules relating to the protection of natural persons with regard to the processing of personal data (Article 1) and applies to the processing of personal data (Article 2). The GDPR provisions do not apply to the processing of personal data of deceased persons or of legal entities. They do not apply either to data processed by an individual for purely personal reasons or activities carried out at home, provided there is no connection to a professional or commercial activity. When an individual uses personal data outside the personal sphere, for socio-cultural or financial activities, for example, then the data protection law must be respected. A list of key GDPR principles is summarised below.

List of key principles. The GDPR intends to protect personal data processed by legal entities. Therefore the main points worth highlighing are:

1)
   - It does not apply to personal data collected by individuals for their private use.
   - It does not apply to data that cannot be linked to individuals. For instance, data provided by a temperature sensor fixed on a monitoring pole/streetlight will not be considered as personal data (there is no link with a natural person), while the geolocation data and sensors data collected from a smart phone will be considered as a personal data, because they can be linked to a person.
2) The GDPR applies to the processing of personal data regardless of the means used, whether automated (e.g., a website, a network of sensors) or not automated (e.g., a filing system based on paper).
3) The GDPR has an extra-territorial reach, meaning that its rules apply not only to controllers or processors established in the European Union, but also to entities having their establishment in a third country, if they:
   - Offer goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union; or

- Monitor the data subjects' behaviour, as far as their behaviour takes place within the Union.

4) Personal data may only be processed where an appropriate legal basis under Article 6 GDPR applies. Consent of the data subject is one possible legal basis, where it is freely given, specific, informed and unambiguous; however, consent is not the only legal basis and may not be the most appropriate one in all circumstances. Depending on the context, personal data may also be processed where the processing:
   - is 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 (e.g. when transferring connected cars' data to an external provider of maintenance services, as agreed with the car's owner through a contract);
   - is necessary for compliance with a legal obligation to which the controller is subject (e.g. a Union, national or regional law setting out rules and obligations for cities within smart cities' programs);
   - is necessary in order to protect the vital interests of the data subject or of another natural person;
   - is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   - is 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 which require protection of personal data, in particular where the data subject is a child (the discipline of the legitimate interest still vary across EU Member States and needs a case-by-case assessment).
   - Consent should be free, unambiguous, informed, prior and demonstrable by the data controller, meaning that it must be documented somehow (also electronically, e.g. by means of a log).
5) In any event, data subjects must be informed about the processing undergone by their personal data before the processing starts or, when data are not collected from the data subjects themselves, within a reasonable period, in any event no later than the first communication or the first disclosure to the public, when such activities are foreseen.
6) Data protection principles (i.e., data minimization, purpose limitation, data accuracy, storage limitation etc.) must always be respected; a data controller may have a legal ground to process personal data (e.g., the data subject's consent), yet it may still run the processing in breach of one of the key data protection principles, which would make the personal data processing unlawful and, potentially, trigger a sanction by competent authorities. This is the essence of the principle of accountability.
7) Risky processing for the data subjects requires a Data Protection Impact Assessment (DPIA). In particular, the DPIA shall be carried out in the case of:
   - a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
   - processing on a large scale of special categories of data;

- a systematic monitoring of a publicly accessible area on a large scale. However, it is recommended to perform a DPIA before starting any data collection from data subjects in any pilots.

8) Clear procedures must be in place to ensure data subjects' rights, namely:
   - Right of access to their data and to receive any important information on what it is done with the data;
   - Right to rectification, when the personal data are processed in a non-accurate way;
   - Right to erasure, under certain conditions, in particular when data have been processed unlawfully or are no longer necessary;
   - Right to restriction, meaning the right to "freeze" data and obtain that they are not processed for a certain period of time, for example when the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data);
   - Right to data portability.
   - Right to object.
9) Procedures to handle and notify data breaches to data protection authorities and data subjects concerned must be in place.
10) Data collected on the data subject should be strictly necessary for the specific purpose previously determined by the data controller (the "data minimization" principle). Data that is unnecessary for that purpose should not be collected and stored "just in case" or because "it might be useful later". For example, if a large-scale event organizer needs generic data of people attending a concert, in order to issue tickets and organize the space in the venue, it would be not necessary and therefore disproportionate to collect information on the attendees' relatives in order to derive fine insights on the socio-economic cluster to which the attendees belong, which can then be used for targeted advertising.
11) Data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.
12) The purpose for which the data were collected or further processed determines the length of time for which the data should be kept. Once the data are no longer needed, they should either be deleted or kept in anonymous form if they serve historical, statistical or scientific uses.
13) In cases of secondary processing of research and scientific data previously obtained for other research purposes can be used in so far as they are not incompatible. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations.
14) GDPR does not concern the processing of anonymous information. According to Recital (26) of the GDPR, the principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer

identifiable.

As detailed above, the scope of application of this Regulation is about the protection of personal data. GDPR is very clear in the Recital (26) about the fact that anonymous information is not in the scope of this Regulation. Considering that:

- The OVERWATCH project gets inputs from research participants only on the basis of interviews, training sessions, and tests done under the scope of the OVERWATCH project[6];
- Data generated from such interviews, training sessions and tests will be processed following the GDPR principles, and according to the guidelines established by the D6.2 OVERWATCH Data Management Plan. Anonymization of data will be done whenever possible;
- GDPR is not applicable to anonymous information.

Yet, considering the importance of this topic in every Horizon Europe research and innovation project, the analysis conducted and detailed on this deliverable could represent the basis for any future further analysis should any new privacy requirement arises in the OVERWATCH context.

3.1.2 ePrivacy Directive

The **ePrivacy Directive** (Directive 2002/58/EC on privacy and electronic communications[7] and intended to be replaced by the ePrivacy Regulation, which remains under legislative negotiation and has not yet been adopted as of the date of this deliverable - concerns the processing of personal data and the protection of privacy in the electronic communications sector and deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies [RD06].

List of key ePrivacy Directive principles:

1. Where the e-Privacy Directive provides for a specific rule applicable to natural and legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks, it prevails over the general rule set out by the GDPR (Principle of Specialty)
2. Electronic Communication Services and Networks must be secured through appropriate technical and organizational measures (Security)
3. The confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, must be ensured (Confidentiality)
4. Storage of, or access to, information on users' terminal equipment requires the user's consent, unless such storage or access is either: (i) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) strictly necessary for

[6] In occasion of the pilots/ demonstrations, OVERWATCH generated data resulting through the use of the web-based dashboard, will be managed according to the procedures explicated in the D6.2 Data Management Plan, and in full observation of the GDPR regulation as well as ePrivacy directive and other relevant applicable regulations.

[7] Amended by Directive 2006/24/EC, Directive 2009/136/EC.

the provider of an information society service explicitly requested by the user to provide that service.

5. In other words, any website, or app should provide clear information on the cookies it deploys into the users' devices and collect the prior consent, where necessary.
6. Principles applicable to Traffic Data:
   - Traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication or for the purposes of processing subscriber's billing and interconnection payments (Traffic data erasure);
   - Traffic data can be processed for marketing and/or for the provision of value-added services only upon specific consent of the user concerned (Consent for Marketing purposes);
   - Specific information on traffic data processing and its duration must be provided (Specific Information);
   - Traffic data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (e.g. handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value-added service – Authorization profiles).
7. Principles applicable to Location Data:
   - Location data can be processed for the provision of value-added services only anonymously or upon specific consent of the user concerned (Consent for Location Data);
   - Users must be given the opportunity to easily refuse such processing at each connection (Updated Consent);
   - Location data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (Authorisation profiles).

3.1.2.1 The EU Cookie Directive

The EU Cookie Directive (Directive 2009/136/EC of the European Parliament and of the Council) is an amendment of the ePrivacy Directive (namely Directive 2002/58/EC) designed to increase consumer protection. The EU Cookie Directive requires websites to obtain informed consent from visitors before they store information on a computer or any web connected device. This is storage is mostly done by cookies, which can then be used for tracking visitors to a site. The EU Cookie Directive covers all forms of online tracking technology (like flash objects and device fingerprinting) so it doesn't just apply to cookies.

The previous privacy legislation required websites to give users information on how they could remove or opt-out of cookies, which was commonly placed in privacy policies that went mostly unread. With the EU Cookie Directive, the user of a site will now be required to opt-in when using a website containing cookies. So, the website must block cookies, until visitors have given their informed consent to their use.

The EU Cookie Directive is and will be used to protect the privacy of OVERWATCH's web-based communication channels, and serve as the basis for drafting the Privacy Policy of the OVERWATCH website (https://overwatchproject.eu/). It is worth to note that, generally, internet cookies are small

pieces of data stored on your computer or mobile device that are used to identify and track visitors. They perform important functions on a website, such as remembering logins and preferences. Cookies can also help measure web traffic and usage patterns.

As part of privacy legislation such as GDPR and ePrivacy, it is often required to display a cookie banner informing users about cookies, or consent must be obtained before tracking visitors' data. The Overwatch website (https://overwatchproject.eu/) uses Matomo (https://matomo.org/), in its cookie-less mode[8] and it is configured to automatically anonymise data avoiding to process any personal data. Hence, the cookie banner is not required, as the way we are using Matomo does not collect any personal data and, therefore, exempt from many countries' privacy regulations and user consent requirements.

Cookie-less tracking is an alternative form of tracking that uses methods such as counting the number of unique IP addresses or browser fingerprinting to identify users instead of cookies. This means that the websites can still track users even if they have disabled cookies in their browsers or if the user has deleted all the cookies from their browser history. At the most privacy-conscious end, we see cookie-less solutions such as Matomo using config_id to group different actions into "visits" during a short window of up to 24-hours.

In must be stressed that, cookieless analytics does not automatically fall outside the GDPR/ePrivacy framework, especially where technical information may still be used to single out users or group their actions. The need for consent or other safeguards is therefore assessed in light of the actual technical configuration and applicable national guidance.

3.1.3 EU Data Governance Act

The EU Data Governance Act (DGA) - i.e. "Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 Data Governance Act" - is a new regulation that aims to foster the availability and sharing of data across the EU, while ensuring high standards of data protection and privacy. The DGA applies to "data" — "any digital representation of acts, facts or information …" — in general, not just to personal data. It is the first of the European Union's new initiatives on "data" to get to the legislative finishing line [RD05].

The DGA impacts the management of personal data in several ways, such as:

- Give individuals more control over their personal data, providing them tools to manage the way their information is accessed. For example, individuals can consent to share their personal data for altruistic purposes, such as scientific research or social good, through recognized data altruism organizations. Individuals can also use data intermediaries, which are neutral and trustworthy entities that facilitate data sharing or pooling between data holders and data users, without accessing or reusing the data themselves.
- Encourage the wider re-use of data held by public sector bodies for purposes other than the ones for which the data was originally collected. It applies to both personal and non-personal data and imposes obligations on data sharing service providers (data intermediation services) and data altruism organizations. For example, the DGA requires these entities to comply with the GDPR and other relevant EU laws, to ensure appropriate safeguards for data protection and

[8] More information upon Matomo's cookie-less tracking is available here

privacy, to inform data subjects about the processing of their personal data, and to respect the rights of data subjects.

- Supports the development of common European data spaces in strategic sectors, such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills. These data spaces will enable the sharing and re-use of data across borders and sectors, while ensuring compliance with EU rules on data protection and privacy. The DGA will also facilitate the creation of codes of conduct and technical standards for data sharing within these data spaces.

In the context of OVERWATCH, the Consortium ensures full compliancy, also in view of potential new exploitation routes, especially in relation to new data intermediation services that could derive as an output of the project.

3.1.4 EU Data Act

The Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (the "Data Act") entered into force on 11 January 2024 and has been applicable since 12 September 2025 [RD19][RD20][RD21].

The Data Act is a horizontal regulation that establishes new rules governing who can access and use data generated by connected products and related services across all economic sectors in the EU. It applies to both personal and non-personal data, without prejudice to the GDPR, which remains the authoritative framework for personal data protection.The Data Act pursues four main objectives:

- **User access to IoT data (Chapters II-III):** It requires that connected products (defined as items that obtain, generate or collect data concerning their performance, use or environment and are able to communicate such data) should be designed to allow users to access the data they generate, and to share those data with third parties under fair, reasonable and non-discriminatory (FRAND) conditions. This obligation applies to products placed on the market after 12 September 2026.
- **Fairness in contractual terms (Chapter IV):** The Data Act introduces protections against unfair contractual terms unilaterally imposed by one party on another in relation to data access and use, particularly in business-to-business relationships.
- **Business-to-government data access in exceptional circumstances (Chapter V):** Under Article 14 and Article 15, public sector bodies may request access to data held by private entities where an exceptional need exists. This includes, in particular, situations of public emergency — such as natural disasters, pandemics or cybersecurity incidents — where the data is necessary to respond to the emergency and cannot be obtained through alternative means in a timely and effective manner. In non-emergency situations, access is limited to non-personal data and subject to additional safeguards.
- **Cloud switching and interoperability (Chapters VI-VIII):** The Data Act facilitates switching between data processing service providers (cloud, edge) by removing contractual, technical and organisational obstacles, and introduces interoperability requirements for data sharing across sectors and common European data spaces. Switching charges are being phased out and will be generally prohibited from 12 January 2027.

Although the Data Act was not yet applicable at the time of publication of D6.3 Issue 1, its provisions have since come into force and merit consideration in the regulatory landscape applicable to the OVERWATCH project. The relevance of the Data Act to OVERWATCH can be assessed along three dimensions:

First, **Chapter V on business-to-government data access during public emergencies** is of direct contextual relevance. The OVERWATCH platform is designed to support public authorities and emergency responders in disaster management scenarios, including floods and wildfires - precisely the types of events that the Data Act cites as examples of public emergencies justifying access to privately held data. While OVERWATCH itself is not a data holder subject to mandatory data sharing under Article 14, the regulatory framework created by Chapter V is significant for the operational environment in which the OVERWATCH solution is intended to be deployed. Public sector bodies using OVERWATCH may, in the future, invoke the Data Act as a legal basis for requesting access to privately held data to feed into the platform's decision-support tools. This means that the data governance logic of OVERWATCH should be designed to be compatible with the ingestion of data obtained under the Data Act's exceptional-need provisions, including compliance with the conditions laid down in Article 17 (justification and proportionality of requests), Article 19 (obligations on the receiving public body, including purpose limitation and deletion after use) and Article 20 (compensation to data holders). Where personal data are involved, invocation of the Data Act does not replace the need for an appropriate legal basis under the GDPR for any subsequent processing, and all GDPR principles and safeguards remain fully applicable.

Second, the **IoT data-sharing provisions** under Chapters II and III are potentially relevant in relation to connected devices that generate data within the OVERWATCH ecosystem. In particular, drones equipped with sensors, LiDAR and imagery capabilities, as well as augmented reality (AR) devices used by first responders, may qualify as connected products within the meaning of Article 2(5) of the Regulation. If such devices are placed on the EU market after 12 September 2026, they would be subject to the "data access by design" requirement under Article 3(1), meaning that they must be designed and manufactured in a manner that allows users to access the data they generate easily, securely and, where technically feasible, directly. At the current stage of the OVERWATCH project, this obligation does not apply, since the devices in use are either prototypes or pre-existing products. However, for any future commercialisation or procurement of connected devices within the OVERWATCH framework, compliance with these provisions would need to be assessed.

Third, the **cloud switching and interoperability provisions** under Chapters VI to VIII are relevant insofar as the OVERWATCH platform relies on cloud-based infrastructure and data processing services. The Data Act requires providers of such services to remove barriers to switching, ensure transparent contractual terms regarding portability, and comply with phased-in requirements for the elimination of switching charges. While these obligations are directed primarily at cloud service providers rather than at platform operators such as OVERWATCH, the consortium should be aware of the rights that the Data Act confers on its members as customers of cloud services, and should ensure that contractual arrangements with cloud providers are consistent with the new regulatory requirements.

Overall, the Data Act does not impose direct compliance obligations on the OVERWATCH consortium in its current research and development phase. However, its provisions, in particular those relating to

public emergency data access and IoT data sharing, are directly relevant to the operational and commercial context in which the OVERWATCH solution is intended to function. For this reason, the consortium will continue to monitor the evolving implementation of the Data Act, including any amendments introduced through the Digital Omnibus package [9]currently under legislative negotiation, and will take its provisions into account in the design of data governance mechanisms for future operational deployment.

3.1.5 Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights (CFR) of the European Union (2012/C 326/02) brings together in a single document the fundamental rights protected in the EU. The CFR contains rights and freedoms under six titles: Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice. Proclaimed in 2000, the Charter has become legally binding on the EU with the entry into force of the Treaty of Lisbon, in December 2009 [RD04]. The rights of every individual within the EU were established at different times, in different ways and in different forms. For this reason, the EU decided to clarify things and to include them all in a single document which has been updated in the light of changes in society, social progress and scientific and technological developments.

The CFR establishes:

- all the rights found in the case law of the Court of Justice of the EU;
- the rights and freedoms enshrined in the European Convention on Human Rights;
- other rights and principles resulting from the common constitutional traditions of EU countries
- and other international instruments.

The CFR sets out a series of individual rights and freedoms. The CFR is a very modern codification and includes 'third generation' fundamental rights, such as:

- data protection; and
- transparent administration.

Regarding the personal data protection, the articles 7 (respect for private and family life) and 8 (protection of personal data) of the Chapter state the following:

- “everyone has the right to respect for his or her private and family life, home and communications” (Article 7).
- “everyone has the right to the protection of personal data concerning him or her”, and that processing of such data must be “fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” (Article 8).

With reference to such relevant document, OVERWATCH aims to ensure compliance tending to the data protection and lawful use of data.

3.1.6 Council Framework Decision 2005/222/JHA

The Council Framework Decision (2005/222/JHA) of February 2005 addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service

[9] More information here: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

attacks. This Decision Framework seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can act against this form of crime. The Council Framework Decision was replaced by Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems [RD08]. It maintains existing offences and criminalizes new activities such as illegal interception and the usage of certain tools for committing offences. OVERWATCH will need to comply to this Directive, to address confidentiality, integrity, authentication and non-repudiation features of the platform.

3.1.7 Future normative outlooks

The European Commission's AI Strategy, first presented in 2018 [RD09], set the objective of making the EU a world-class hub for AI while ensuring that AI remains human-centric and trustworthy. This strategic ambition has since been translated into binding legislation through the adoption of the EU Artificial Intelligence Act [RD10][RD23], described below.

3.1.7.1 The EU Artificial Intelligence Act

The Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the "AI Act") was published in the Official Journal of the European Union on 12 July 2024 and entered into force on 1 August 2024. It constitutes the first comprehensive horizontal legal framework on artificial intelligence worldwide, and is directly applicable in all EU Member States.

The AI Act adopts a risk-based regulatory approach, classifying AI systems into four tiers according to the level of risk they pose to health, safety and fundamental rights:

- **Unacceptable risk (prohibited practices):** AI systems considered to pose an unacceptable threat to individuals are banned outright. These include, among others, social scoring systems by public authorities, real-time remote biometric identification in publicly accessible spaces (subject to limited exceptions for law enforcement), manipulation techniques that exploit vulnerabilities of specific groups, and AI-based emotion recognition in the workplace and educational settings. Prohibitions on these practices have been applicable since 2 February 2025.
- **High risk:** AI systems deployed in sensitive areas such as critical infrastructure, education, employment, law enforcement, migration and the administration of justice are classified as high-risk and are subject to strict requirements, including risk management systems, data governance, technical documentation, transparency, human oversight, accuracy and cybersecurity obligations. Providers of high-risk systems must undergo conformity assessments before placing such systems on the market.
- **Limited risk:** AI systems that interact with individuals (e.g. chatbots), generate synthetic content (e.g. deepfakes) or perform emotion recognition or biometric categorisation where such use is permitted under the AI Act, are subject to specific transparency obligations, ensuring that users are informed that they are interacting with an AI system or that content has been artificially generated or manipulated.

- **Minimal risk:** AI systems that do not fall within the above categories are not subject to specific regulatory obligations under the AI Act. Providers of such systems are encouraged to adhere to voluntary codes of conduct.

In addition to the risk-based framework, the AI Act introduces dedicated provisions for general-purpose AI (GPAI) models, requiring providers to maintain technical documentation, implement transparency measures, comply with copyright obligations and, for GPAI models with systemic risk, conduct model evaluations and ensure adequate cybersecurity measures. The obligations relating to GPAI models have been applicable since 2 August 2025.

Implementation timeline. The AI Act follows a phased implementation approach. The key compliance milestones are summarised as follows:

Date	Milestone
1 August 2024	Entry into force of the AI Act
2 February 2025	Prohibitions on unacceptable-risk AI practices become applicable
2 August 2025	GPAI model obligations and governance provisions become applicable; Member States designate national competent authorities
2 August 2026	Most remaining obligations become applicable, including requirements for high-risk AI systems (Annex III), transparency obligations, and the establishment of national AI regulatory sandboxes
2 August 2027	Full applicability, including obligations for high-risk AI systems that are safety components of products already subject to EU harmonisation legislation (Annex I)

Table 3-1 AI Act timeline and milestones

It should be noted that, as of the date of issue of this deliverable (April 2026), the European Commission's Digital Omnibus package (currently under trilogue negotiation between the Commission, the European Parliament and the Council) proposes to extend the compliance deadline for high-risk AI systems listed in Annex III from 2 August 2026 to 2 December 2027, and for product-embedded high-risk AI systems under Annex I to 2 August 2028. A political agreement is expected imminently; however, as the **Digital Omnibus has not yet been formally adopted**, the original deadlines remain the legally applicable reference at this stage. OVERWATCH will continue to monitor the outcome of the trilogue and adjust its compliance posture accordingly.

The AI Act establishes a multi-layered **governance architecture** at EU level, comprising:

- The **EU AI Office**, established within the European Commission, with supervisory and coordination responsibilities, in particular regarding GPAI models;
- The **European Artificial Intelligence Board (EAIB)**, composed of representatives of the Member States, to advise and assist the Commission and contribute to the consistent application of the Regulation;
- The **National Competent Authorities**, designated by each Member State for market surveillance and enforcement at national level; and
- The **Advisory Forum** and the **Scientific Panel of Independent Experts**, to provide technical and societal input into the regulatory process.

In the context of the OVERWATCH project, the AI Act is directly relevant so far as the platform integrates AI-based components for decision support purposes, including mapping analysis, predictive modelling and situational awareness tools.

As reported in the internal PES survey conducted under Task 6.3 (see Section 4), one consortium partner confirmed the presence of AI-based components within its contribution and, following an initial scoping assessment, indicated that these systems do not fall within the prohibited practices (Art. 5) or high-risk use cases (Art. 6 and Annexes) under the EU Artificial Intelligence Act. Additionally, the partner reported the application of confidence and uncertainty indicators as safeguards on AI-generated outputs.

While this preliminary classification appears reasonable on the basis of the information currently available, it should be regarded as provisional and subject to reassessment as the technical components mature and as the deployment context evolves. The AI Act's classification criteria depend not only on the technical nature of the AI system, but also on its intended purpose, the operational environment and the potential impact on the health, safety and fundamental rights of affected persons. Given that OVERWATCH is designed for use in emergency and crisis management contexts, particular vigilance is warranted, as future evolutions of the system's capabilities — or changes in the operational role assigned to AI-generated outputs — could shift the applicable risk category. In particular, should any AI component be deployed in a manner that materially influences operational decisions affecting the safety of persons or the allocation of emergency response resources, the classification may need to be reconsidered against the criteria for high-risk systems established in Article 6 and Annex III of the Regulation.

In light of the above, the OVERWATCH consortium will continue to:

- monitor the evolving regulatory and interpretative framework under the AI Act, including the outcome of the Digital Omnibus trilogue and the publication of implementing guidance by the European Commission;
- reassess the risk classification of AI components as technical development progresses and as operational deployment scenarios become more defined;
- maintain the safeguards already in place (human validation and uncertainty indicators) and evaluate the need for additional measures, such as explicit disclaimers on the advisory nature of outputs, traceability of model assumptions, and formal human-in-the-loop validation procedures; and
- ensure that any future operational deployment of AI-enabled functionalities remains consistent with the four fundamental ethical principles identified in this deliverable, namely respect for human autonomy, prevention of harm, fairness, and explicability.

3.2 Privacy aspects of the OVERWATCH project

Privacy and data protection represent core values of the OVERWATCH project. In particular, the information gathered from the in-field operators via smart devices and services (e.g. AR device), which are transmitted in an online cloud-computing service platform and processed in the OVERWATCH Big Data Architecture represent key assets from the perspective of data protection.

So far, the main privacy challenges appear to relate to the privacy- aware management of location information (e.g. drone multimedia information), and to the need to provide safeguards for location privacy of on-site units against potential misuse or abuse.
Taking the location privacy as an example, the drone location data are necessary for the operability of the OVERWATCH service but, on the other hand, it should be disclosed with caution to reduce risk of unauthorized disclosure of on-site units' locations and/or related movement patterns.
These issues are potential risks in terms of privacy preservation that need to be handled from the early design stages of the project leveraging a well-defined Privacy-By-Design (PbD) [RD11][RD12] methodology respecting the claim/right of individuals, groups and institutions involved in the use of the system. Another potential issue is the need to prevent third parties from learning an individual's current or past location.
In order to meet these challenging goals and mitigate the privacy risk, technical mechanisms, also known as Privacy-Enhancing Technologies (PETs)[10] [RD14][RD15] have to be implemented: a set of compute tools, applications and mechanisms which, when integrated in services or applications, allow online users to protect the privacy of their Personally Identifiable Information (PII) provided. PETs are ICT measures protecting the privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system (IS). The main goals of PETs are the following:

- Increase the control over the personal data sent to, and used by, online service;
- Apply data minimisation techniques to minimise collected personal data;
- Choose the degree of anonymity for personal data (e.g., by using pseudonyms, anonymisers or anonymous data credentials);
- Choose the degree of unlinkability for personal data (e.g., by using multiple virtual identities);
- Achieve informed consent about giving their personal data to online service providers and merchants;
- Negotiate the terms and conditions for users of providing their personal data (data handling/privacy policy negotiation). In Privacy Negotiations, consumers and service providers establish, maintain, and refine privacy policies as individualised agreements through the ongoing choice amongst service alternatives;
- Provide the possibility to have these negotiated terms and conditions technically enforced by the infrastructures of the online service providers;
- Provide the possibility to remotely audit the enforcement of these terms and conditions for the online service providers;
- Perform data tracking: allow users to log, archive and look up past transfers of their personal data, including what data has been transferred, when, to whom and under what conditions;
- Facilitate the use of their legal rights of data inspection, correction and deletion.

In order to unleash the full benefit of a privacy and data protection methodology, PETs need to be rooted in a data governance strategy to be applied in practice during the whole project. For this reason, in OVERWATCH we propose the adoption of a Privacy-by-Design (PbD) approach, namely EBIOS, to

[10] Privacy-Enhancing Technologies are digital solutions that allow information to be collected, processed, analysed, and shared while protecting data confidentiality and privacy.

monitor all the design and development phases of the project. The term "Privacy by Design", or its variation "Data Protection by Design", has been coined as a development method for privacy-friendly systems and services, thereby going beyond mere technical solutions, addressing organisational procedures and business models as well. This concept founds is in line with the EU GDPR, and its main goals are:

- Unlinkability ensures that privacy-relevant data cannot be linked across domains that are constituted by a common purpose and context, and that means that processes have to be operated in such a way that the privacy-relevant data are unlinkable to any other set of privacy relevant data outside of the domain.
- Transparency ensures that all privacy-relevant data processing including the legal, technical and organisational setting can be understood and reconstructed at any time. The information has to be available before, during and after the processing takes place. Thus, transparency has to cover not only the actual processing, but also the planned processing (ex-ante transparency) and the time after the processing has taken place to know what exactly happened (ex-post transparency).
- Intervenability ensures intervention is possible concerning all ongoing or planned privacy-relevant data processing, in particular by those persons whose data are processed. The objective is the application of corrective measures and counterbalances where necessary.

One of the objectives of Privacy-by-Design is also to contribute to bridging the gap between the legal framework and the available technological implementation measures by providing a strategy to preserve privacy starting from the privacy principles of the legislation. For this reason, the proposed methodology will sketch a method to map legal obligations to design strategies, which allow the system designer to select appropriate techniques for implementing the identified privacy requirements.

3.2.1 Privacy requirements

Privacy by Design is an approach to system engineering that considers privacy throughout the whole design and implementation process. The purpose of data protection by design and by default is to prevent or mitigate data protection risks and to protect the individuals' rights and freedoms , by proactively incorporating data privacy safeguards into systems and processes[11]. In the context of OVERWATCH, it is the approach utilised for both the development of the platform and the related services.

The PbD framework employs an approach that is characterized by pro-activeness rather than reactiveness, anticipating and preventing privacy invasive events before they happen. Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred. It aims to prevent them from occurring.

In short, Privacy by Design comes before-the-fact, not after.The objectives of Privacy by Design - ensuring privacy protection and gaining personal control over one's own information and, for organizations, gaining a sustainable competitive advantage - may be accomplished by practicing the Seven Foundational Principles[RD11], which are reported into the following table:

#	Principle	Description

[11] In response to DRS, comment n.2.

1	Proactive not reactive; Preventativenot remedial	PbD anticipates and prevents privacy invasive events beforethey happen.
2	Privacy as the default setting	PbD delivers the maximum degree of privacy by ensuring that personal data are automatically protected in any givenIT system or business practice. If an individual does nothing,their privacy remains intact. No action is required on the part of the individual to protect their privacy — it is built intothe system, by default
3	Privacy embedded into design	PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
4	Full functionality – positive-sum, not-zero-sum	PbD seeks to accommodate all legitimate interests and objectives in a positive-sum win-win manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security – demonstrating that it is possible to have both.
5	End-to-end security – full lifecycle protection	PbD, having been embedded into the system prior to the first element of information being collected, extendssecurely throughout the entire lifecycle of the data involved - strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensuresa secure lifecycle management of information.
6	Visibility and transparency – keep it open	PbD seeks to assure all stakeholders that whatever the business practice or technology involved, its component parts and operations remain visible and transparent, to users and providers alike.
7	Respect for user privacy – keep it user-centric	PbD requires architects and operators to protect the interests of the individual by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Table 3-2 The Seven principles of Privacy by Design (PbD)

According to this vision, the privacy system must be user-centric, with the user at the centre of the entire system. This means that it is not sufficient a design that conforms to rule, if the user is not properly protected.

3.2.2EBIOS approach and principles

“Expression des Besoins et Identification des Objectifs de Sécurité” (EBIOS) is a risk management method used to identify, analyse and mitigate information security risks, and it is aligned with the ISO/IEC 27005 [RD17], risk management framework .

In OVERWATCH, EBIOS is used to support the operationalisation of the GDPR principle of data protection by design and by default, by enabling early identification of privacy-relevant assets, feared events, threat scenarios and proportionate mitigation measures throughout the system lifecycle

This security approach is made up of the following steps:

- Define the Context;
- Define the potential Feared Events;
- Define the scenarios of Threats;
- Analyse risks; and
- Identify measures for risk mitigation.

The approach has been implemented since the very beginning of platform development, as it allows to identify and treat risks before they become too difficult to mitigate[12].

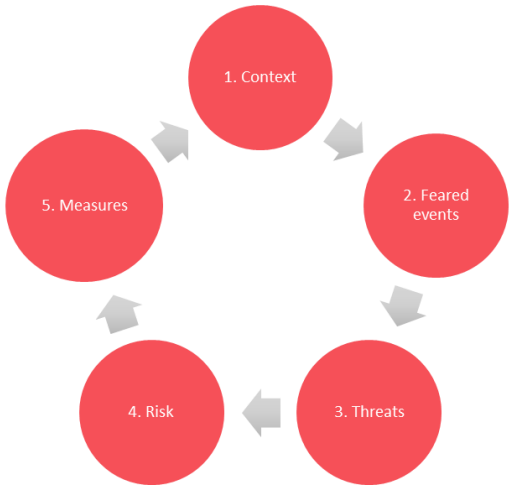


Figure 3-1 The five phases of the EBIOS Privacy By Design methodology

In this section, the context in which personal data are collected, stored and processed in OVERWATCH is described. In particular, users, primary and supporting assets will be identified in order to set the common ground for the adopted EBIOS privacy and data protection methodology.

One of the key objectives of the OVERWATCH project is to create a centralized platform together with a set of applications (i.e., OVERWATCH drone, AR) targeting mainly emergency practitioners (High-rank personnel authorised for the Emergency Control Room). In terms of security management, these users are expected to generate or receive data that are sensible, at different levels. These data are generated through the Report, which is a set of information including pictures, text, and metadata created by Authorised On-field Teams and/ or Drones.

The information collected in a report generated by first responders may require restricted access controls and should be anonymised , whenever possible and if applicable. Therefore, it is fundamental in this context to devise data management mechanism capable of ensuring privacy and the prevention of unauthorised disclosure of sensitive information.

From a more detailed perspective, there are privacy and security requirements that are shared by the identified class of users (i.e., first responders, public authorities/decision makers). It must be stressed that at this stage, access to the platform will be granted to a list of users (with credentials composed by an assigned alphanumeric ID and password), and hence with limited collection of data of personal information.

[12] In response to DRS, comment n.3.

Besides the identified categories of users, there are other potential users of the OVERWATCH solution that must be considered. It is possible that the technical solution for OVERWATCH will be accessible not only during an emergency event, for example to perform a particular kind of data analysis, to examine time-series of data, etc. In these cases, the system will probably be accessed by an internal user, such as an analyst, or a system administrator. The analysis of the context and requirements will be conducted applying a scenario-based approach. The context that is considered refers to users of the classes producing in-field reports. The following scenarios are foreseen:

- Emergency practitioners/On-field team: Appointed user by the authorised on-field team which is in charge of producing a report that contains accurate and quantitative information. The Reports are of primary importance for the Control Room.
- Data analysis: After an emergency, or during a pre-alert phase, a user would need to access a particular set of historical data (e.g., burned area delineation), joining them with other sources of information, to create a predictive model, etc. It might also be possible to analyse the information that has been created by the users via their reports, during an emergency, and use it to create other information levels: wildfire areas, flood areas, etc. It must be noted that according to the EU Data Protection Regulation, consent to collect and process personal data must now be explicitly obtained.

It is worth to be noted that all users must accept the terms of reference when accessing and using OVERWATCH product.

However, such acceptance should be understood as a contractual/access condition and must not be conflated with the GDPR legal basis for processing personal data. The project will identify and document the applicable lawful basis for each processing purpose.

3.3 Ethical requirements and considerations

The OVERWATCH consortium is fully aware that the project's activities may generate ethical, fundamental rights, privacy and data protection implications and is fully committed to comply to the highest standards at the European and International level. Indeed, the OVERWATCH Grant Agreement [RD01](Art. 14 and Annex 5 of the GA, under specific rules), explicitly mentions the project ethics requirement and the compliance with ethical principles and relevant legislations, while section 5 "Ethics self assessment" explains the actions that will be undertaken to monitor and manage ethical issues. These aspects affect specific activities, related to the engagement with end-users and stakeholders, as the involvement of humans in OVERWATCH is necessary for the co-design activities (i.e., user requirements), workshops, and professionals and volunteers for field validation purposes. Participation is voluntary and will be governed by documented procedures, including the provision of participant information, appropriate safeguards, and the collection and secure storage of any personal data where relevant.

OVERWATCH designed solution may involve the processing of personal data once operational, according to the content of the ethics review and ethics section of Description of Action). Their participation, including the collection of any personal data, is managed by the specific procedures and protocols and foresee several actions, starting from upfront consent for data collection and data processing up to the storage of data.

The management of such data will regulated by a clear Term of Services, which must be read and accepted by all users, and which will follow the EU GDPR (this will be enclosed in the forthcoming issue). Also, following the EU commission's guidelines, within the context of WP3, where the models are also established and developed, technical specifications for developing a robust AI are being incorporated. The ethical challenges, on the other hand, will be handled by innovation and AI professionals in T6.3 through an internal Ethics and Security committee that will be chaired by the Data Protection Officer of the project. AI will be in this project limited to mapping analysis, and the four basic principles (respect for human autonomy, prevention of harm, justice, and explicability) will be regularly reviewed in terms of ethics. A constant supervision of the development and use of AI, will prevent and minimise any risks, consequently maximising the benefits offered by AI systems during all its life cycle.

At this stage, the usage of AI in OVERWATCH has not raised any ethical concerns related to human rights and values, however all activities involving AI will be overseen by an internal ethics committee lead by the Ethics and Security Manager, which will perform their activities in WP6 under T6.3 - Security, privacy and ethics. AI projects and applications have exploded in popularity in recent years, making it one of the top strategic goals. Aside from the enormous potential of AI, there are also drawbacks, such as increased socio-economic inequality, malevolent use, and a reduction in work opportunities, to name a few. As the European Commission recently noted in the Ethics Guidelines for Trustworthy AI [RD06], it is critical to ensure its proper use while keeping its trustworthiness in mind. According to the guidelines the AI's trustworthiness is built on three pillars, that OVERWATCH will address and comply, i.e.:

- be legal, adhere to all applicable rules and regulations;
- ethical, adhere to ethical ideas and values;
- and will be robust, from both a technical and social standpoint.

These guidelines together with the implementation of an ‘ethics by design’ approach will ensure an ethically sound AI system.

Regarding human participation, the ESM has had / will have as objectives to oversee that all activities gathering, processing and analysing sensitive data, ensure that the established procedures are followed and fulfil all obligations with regard to confidentiality while ensuring the compliance with the regulation including the GDPR. When sensitive information is used by the project, the ESM will provide to the commission detailed information on privacy/confidentiality and how the data collection, storage, protection, sharing policies comply with national and EU legislation as well as how Informed Consent protocols were developed and implemented. Furthermore, a detailed assessment on possible unforeseen usage of data gathered during OVERWATCH will be provided, together with security measures to prevent improper use.

Ethical standards and guidelines present in Horizon Europe will be enforced throughout the project, all information regarding the purpose and procedure of the research will be clear and unmistakable to all human participants, as well as stress that their participation is on a voluntary basis. For those who choose to participate, will be informed of the purpose, duration and, procedure of the activity and their right to privacy. They will also be informed on how project privacy mechanisms will ensure privacy through anonymisation and data storage security. Regarding surveys no participant will be obliged to answer questions and will be made aware of their withdrawal rights which translate into withdrawal at any time and right to have any personal data, recordings or images destroyed.

OVERWATCH partners confirm that regarding human involvement in this proposal, all foreseen activities comply with relevant ethical codes of conduct in European Code of Conduct for Research Integrity as it will adhere to the principles for proper handling and management of research data.
Overall, the ethics dimension will be taken into consideration to meet the fundamental values: respect for human freedom, dignity, equality and solidarity, citizens rights, and justice.

3.3.1 Legal and ethical framework for the involvement of humans in OVERWATCH

For all activities funded by the EU, ethics is an essential part of research from the beginning to the end, and ethical compliance is pivotal to achieve real research excellence. Ethical research conduct implies the application of fundamental ethical principles and legislation to scientific research in all possible domains of research. In fact, ethics is given the highest priority in EU funded research: all the activities carried out under Horizon Europe (incl. previous H2020) must comply with ethical principles and relevant national, EU and international legislation, for example the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights. Research within the European Union must comply with:

- Ethical principles, i.e., Article 19 of Regulation (EU) 2021/695 establishing Horizon Europe;
- Applicable international, EU and national legislations (for example: the EU General Data Protection Regulation (GDPR), which replaced the former Directive 95/46/EC, and the Charter of Fundamental Rights of the European Union).

Specifically to the ethical principles, particular attention will be paid to the principle of proportionality, 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 the need to ensure high levels of human health protection. As for the applicable international, EU and national legislation, the OVERWATCH consortium will comply with the applicable legislations, in particular with reference to the following:

- Article 2(a) of EU Directive 95/46/EC (repealed by EU GDPR with Article 5 “Principles relating to processing of personal data”) establishes that personal data must be processed in accordance with certain principles and conditions that aim to limit the impact on the persons concerned and ensure data quality and confidentiality. Certain categories of data are more ‘sensitive’ than others (e.g., health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction) and these may only be processed according to specific rules.
- EU General Data Protection Regulation (GDPR), where personal data is “any information relating to an identified or identifiable natural person”. In particular:
    - Article 7 states the conditions in which consent must be given by the owner of the data in order for them to be treated.
    - Article 17 states the Right to erasure ('right to be forgotten'). This right entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure, as outlined in article 17 above, include the data no longer being relevant to original purposes for processing, or a data subject withdrawing consent. It should also be noted that this right requires controllers to

compare the subjects' rights to "the public interest in the availability of the data" when considering such requests.

- Article 8 of the Charter of Fundamental Rights on the protection of personal data, where everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.
- Article 5(3) of the European ePrivacy Directive states that "the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC and EU GDPR, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user." In short, Art. 5(3) requires that any "storing or retrieving" of information from a device of an end users should be subject to consent unless it is technically necessary to enable the intended communication to take place. This can be applied to a wide range of circumstances and applies to a range of different technologies and techniques for storing and retrieving information from a user's device (such as Cookies), so it is mandatory to obtain the necessary notifications/authorisations for collecting and processing the data (including specific authorisations, if applicable) and the free and fully informed consent of the persons concerned ('data subjects').
- The European Code of Conduct for Research Integrity [RD13] which establishes "A basic responsibility of the research community is to formulate the principles of research, to define the criteria for proper research behaviour, to maximise the quality and robustness of research, and to respond adequately to threats to, or violations of, research integrity." The Code of Conduct's purpose is to create awareness of this responsibility and to be a framework for self-regulation for the research community. It describes professional, legal and ethical responsibilities, and acknowledges the importance of the institutional settings in which research is organised. Therefore, this Code of Conduct is relevant and applicable to publicly funded and private research, whilst acknowledging legitimate constraints in its implementation.

3.3.2 Human participants in research activities and potential ethical concerns

OVERWATCH designed solution will imply the collection and the processing of personal data once operational (as stated in the Ethic section of OVERWATCH D6.2 Data Management Plan [RD07] and according to the content of the ethics review and ethics section of the proposal [RD01]).

Users will be required to accept the Terms of Service as a condition of access. For each processing purpose, the applicable lawful basis under Article 6 GDPR will be identified and documented, and where processing is based on consent, Article 7 GDPR conditions for valid consent will apply.
It is important to highlight that data regarding financial details, sexual lifestyles, ethnicity, political opinion, religious or philosophical conviction, and health will not be included in the Information Architecture of the solution, thus will not be treated.
Nevertheless, if the management of one or more of these types of data emerges during the requirement definition from end-users, such data will be handled under strict data minimisation and access control measures, and appropriate procedures will be applied to restrict, remove, or otherwise manage it in compliance with the GDPR and applicable national rule.
The main types of data generated by OVERWATCH are the following:

- Decision Support Tools
- Early warning & Risk maps
- Weather forecast maps
- Fire nowcasts and forecasts
- AR input data (sensor data for room tracking, head pose, audio stream, etc)
- Drone data (LiDAR, imagery, etc.)

Different features of the system will rely on location-based technologies to determine the position of people and "objects" (such as infrastructures, resources, vehicles, etc.), which is crucial for the implementation of the OVERWATCH products.
Key ethical issues concerning research activities are examined from the OVERWATCH point of view and include recruitment of participants, information to participants, informed consent and data handling during the planned research activities. The project activities will be carried out with regard to ethical implications and respecting the regulations expressed in international, European and national texts and codes of practices in force, in particular the General Data Protection Regulation (EU) 2016/679 (GDPR), which replaced the former Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Ethical, privacy, and data protection-related aspects will have a key role over all the operations involving personal and sensitive data from people, i.e., any data that can disclose a person's location, looks, etc. (e.g., collection, storage, analysis, transmission). This means that all the possible precautions for ethics and data management will be adopted in order to guarantee protection requirements (e.g., authorization/access control, message integrity and confidentiality).
The Ethics and Security Manager will be in charge of assuring that the ethical standards and guidelines of Horizon Europe and the European Commission, including data collection and processing, are rigorously applied regardless of the country in which the research is carried out. Furthermore, all research activity within OVERWATCH adheres to the European Code of Conduct for Research Integrity [RD13]. All OVERWATCH partners are required to act according to any national legislation and other data protection related regulations.

3.3.3 Ethical requirements

Since the early stages of the project an "ethical checklist" was used in order to assess the presence of possible issues, especially in beginning the research activity. It is the following:

Item	Check (Yes/No)
Is the proposed research adequately designed, so that it will be of informational value?	YES
Does the research pose risks of physical or psychological harm to participants by using deception, obtaining sensitive information or exposing them for risks in terms of safety and/or security hazards?	NO
If risks exist, does the research adequately control these risks by including procedures, such as debriefing, removing or reducing risks of physical harm, or obtaining data anonymously? If that is not possible, will the research procedures guarantee that information will remain confidential?	YES
Is there a provision for obtaining informed consent from all participants? Will the researcher provide sufficient information to potential participants so that they will be able to give their informed consent? Is there a clear agreement in writing (the informed consent form) between the researcher and the potential participants? The informed consent should also make it clear that the participant is free to withdraw from the study at any time.	YES
Will participants receive adequate feedback at the completion of the study, including a debriefing if that is necessary?	YES
Do I as researcher accept my full responsibility for the ethical and safe treatment of all participants?	YES
Have I as part of the project informed the Ethics Board about the ethical issues I have identified and of which I am aware?	YES

3.3.3.1 Code of ethical conduct

The major ethical issue involves informed consent, confidentiality and OVERWATCH partner' access to personal data and potentially sensitive or confidential information relating to individuals and organisations involved in the project.. Appropriate safeguards will therefore be implemented to ensure that participation is voluntary, informed and based on clear information regarding the purposes of the activities, the types of data collected, the expected use of such data, participants' rights, confidentiality measures and any potential risks. Informed consent will be obtained, where required, from participants involved in pilots, interviews, workshops and other project events. Participation is voluntary and participants are informed that they may withdraw at any time without negative consequences. The informed consent form for OVERWATCH is provided in Annex.

A fundamental ethical principle in research is that project activities must avoid causing harm to participants. This requires the identification and mitigation of potential risks, including risks related to privacy, confidentiality, misuse of information, reputational harm or undue pressure to participate.

At the same time, research activities should be designed to generate legitimate and proportionate benefits, either for participants, relevant stakeholders, the project community or society more broadly.

To this end, OVERWATCH project activities will be carried out in accordance with the applicable Horizon Europe ethical requirements, the Charter of Fundamental Rights of the European Union, relevant international and national ethical standards, and Regulation (EU) 2016/679 – i.e., the GDPR - where personal data are processed [RD01].

3.4 Security requirements and considerations

When collecting personal data, there are in place ethical and legal obligations to ensure that participants' information is properly protected . This is fundamental to safeguarding their rights and freedoms, and minimising the ethics risks related to the data processing. The EU GDPR requires all data controllers and processors to implement appropriate technical and organisational measures to ensure a level of data security that is commensurate with the risks faced by the data subjects in the event of unauthorised access to, or disclosure, accidental deletion or destruction of, their data (Art. 32 of the EU GDPR). As explained in D6.2 Data Management Plan deliverable [RD07], the data collected by OVERWATCH partners will be preserved in their own premises. Each partner has an accountable person for its data management and protection. Each OVERWATCH organisation has already in place high security measures and procedures aimed to avoid breaches in confidentiality and misuse of the collected data. The next section will focus on the assets that require definition and application of proper security and privacy management strategies.

3.4.1 Security aspects of OVERWATCH

Different categories of data that require the definition and the application of proper security and privacy management strategies have been identified.

Primary assets.

Primary assets required the definition and the application of proper security and privacy management strategies. The user data considered are summarized in the following table:

Primary Asset	Description
Personal Information data	This data refers to data related to the user profile. This includes possible personal data as well as the role of the user within the OVERWATCH platform (e.g., first responder). This is a sensitive information that needs to be accessedby a controlled set of users, with a specific set of permissions. To overcome possible issues, credentials will be given to the client with a set alphanumerical ID and password.
Location data	The geo-localisation reference (geographical coordinates) in the OVERWATCH data is key. This refers to all the information that are gathered from the users (via possible chatbot application) – possibly done by appointed authorised on-field agent - and collected in their report, sent to the OVERWATCH platform. This information must be collected at the highest level of precision possible but must be provided to users with a level of details that strongly depend on the role of the user that is receiving the information. On the other hand, sensitive information will be treated differentlyfor users with no permission grants on this information. Also, it must be stressed that the software will be deployed on client's premises and will leverage a DMZ (Demilitarised) network[13].In this context, a demilitarised network, is a security framework that isolates and protects an organization's internal network from untrusted external traffic, such as the internet. A DMZ typically contains servers and resources that provide services

[13] In response to DRS, comment n. 4.

	to external users, such as web, mail, or FTP servers[14]. A DMZ is separated from the internal network by a firewall or other security device that filters and controls the traffic between them. A DMZ can also have another firewall that protects it from the external network. This way, a DMZ can reduce the risk of an attacker gaining access to the internal network by compromising a server in the DMZ. The advantage of a DMZ is that it provides an extra layer of security for an organization's internal network by restricting access to sensitive data and servers. A DMZ enables external users to access certain services, such as web or mail servers, while creating a buffer between them and the private network. A DMZ also helps prevent network reconnaissance and enables access control by filtering and monitoring the traffic between the external and internal networks.
Multimedia data	Images may be collected and attached to generated reports in order to enhance the provided information. However, from the privacy and security management perspective, these data may include information that could be subject to non-disclosure restrictions. This is especially the case in which sensitive information(e.g., faces of people, cars' plate numbers) may be inadvertently revealed along with spatial-temporal geolocation inside frames or regions of the pictures, respectively. This represents a concrete risk that requires proper counter measures. Several solutions could be applied in this case to avoid or limit the risk. One possible solution is to adopt automatic image and video processing algorithms for an automatic identification and blurring of sensitive information (if required). While these techniques could avoid the disclosure risk completely in principle, it may also happen that important information for the management of the emergency would be automatically hidden without control. Therefore, in the OVERWATCH context, a more controllable solution would be preferable, with respect to a more accurate one. In this case, a warning message prompted to the user regarding the possible disclosure risk can represent a possible compromise, together with a mechanism to allow users to inform the data processor about an image/video that contains sensitive information.
Textual data inside the reports	Free textual information included by the user in the report to provide additional information about the occurring event.

Table 3-3 OVERWATCH primary assets description

Supporting assets

Supporting assets were identified and these could be systematically attacked by external/internal malicious persons/systems to attempt to compromise the privacy and protection of user's data. A list of OVERWATCH supporting assets is provided hereafter:

Potential measure	Description
Administration	Following the recommendations of the GDPR, a Data Protection Officer has been appointed to direct and oversee all data protection activities. Supporting the DATA MANAGER, in OVERWATCH, an Ethics and Security Manager figure was foreseen as well. The ESM devises the policies and procedures that bring the organisation into compliance with the

[14] A FTP - File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network.

	Regulation, monitors the implementation of those policies, ensures that all staff are fully trained with regards to protecting data, assigns responsibilities and handles the public's requests regarding their personal data. The ESM keeps management informed regarding their obligations under the Regulation and is the primary contact point for supervisory authorities. The ESM is also responsible for monitoring, notifying and otherwise communicating information about personal data breaches, and documenting public and regulators' requests regarding the removal, destruction and accessibility of data.
Authentication and Perimeter Security	Users need to reliably identify themselves and then have that identity propagated throughout the OVERWATCH platform to access resources. All the users involved in the creation of the report must be authenticated on the OVERWATCH platform. No anonymous report will be allowed. To this end, credentials will be provided to the client organisation, that will have a list of alphanumerical IDs and related passwords, distributed to authorised personnel. Since the OVERWATCH platform has been designed as a collection of additional services (e.g., AR, Drones), the main authentication mechanism that will be adopted will be based on a token- sharing authentication through active sessions. In more detail, each service communicating with the OVERWATCH platform is required to establish an encrypted communication session. Within the OVERWATCH ecosystem, standards such as OAuth2.0 and HTTPS will be used in order to provide secure Authentication and Authorization mechanisms.
Authorization - Restricted access to data and report information	Security administrators can define security policies at the database, table, column, and file levels, and can administer permissions for specific groups or individual users. Rules based on dynamic conditions such as time or location can also be added to an existing policy rule. A permission-based mechanism must be integrated into the OVERWATCH platform to implement different access level for the information provided. This requirement is particularly for report generated by first responders/ On-field Teams, whose access should be granted by the Control Room decision makers. First responders will have the possibility to create content where private content will be shared only within their organisation.
Secure communication & data transfer	All the information collected must be transmitted to the OVERWATCH platform on secure and trusted communication channels (e.g., based on HTTPS). The same also applies to data delivered to the users (e.g., through their chatbot app). The main focus is to avoid the leakage of information, as well as malicious sniffing of sensible data. To this end, proper set of certificates will be generated and used to establish secure communications on the channels. Therefore, the protocol adopted for data exchange in the communication between the OVERWATCH platform and services will be the HTTPS, that combines HTTP with SSL encryption, and the TLS.
Data backup and recovery	The table on "Selected risk-treatment measures" reports the risk treatment measures for OVERWATCH illustrated in section 3.4.2 describing how they are adopted to mitigate each of the presented risks and which is the effect in terms of re-estimation of severity and likelihood levels.
Secure data storage	The personal data gathered within OVERWATCH will be securely stored inside the OVERWATCH platform. The same strategy is also required for users' profile information and credentials, which will be stored in a separate system and database. No encryption is foreseen as the data storage is masked and only accessible by API access via the DMZ module.
Audit	Auditing is the monitoring and recording of selected user data actions. It can be based on individual actions, such as the type of query statement executed, or on combinations of

	factors that can include username, application, time, etc. Security policies can trigger auditing when specified elements are accessed or altered, including the contents within a specified object. Audit logs are retained for no longer than necessary for the purposes of accountability, security monitoring, and incident investigation, in line with the storage limitation principle. In the OVERWATCH project, the current operational retention period for audit logs is set to 1 year.

Table 3-4 OVERWATCH supporting assets description

3.4.2 Security measures implemented

Since the early stages of the project, a series of measures and actions were set in place and implemented to: identify events that could affect OVERWATCH data collection (such as feared events and threats); analyse the level of risk; identify the measures to be adopted for risk mitigation; identify measures on primary and secondary assets. A first list of feared events that that may affect the data collection, storage and processing operation in OVERWATCH was performed. Identifying feared events required assessing their potential impacts and consequences that each feared event could have on the identity of users and the privacy of data. To meet this goal feared events were ranked determining their *severity*, based on the level of identification of personal data and the prejudicial effect of these potential impacts.

The primary step consisted in the assessment of the level of identification of all personal data (identified beforehand) i.e., how easy is it to identify data subjects (identifiable individuals):

1. Negligible: Identifying an individual using his/her personal data appears to be virtually impossible.
2. Limited: Identifying an individual using his/her personal data appears to be difficult but is possible in certain cases.
3. Significant: Identifying an individual using his/her personal data appears to be relatively easy.
4. Maximum: Identifying an individual using his/her personal data appears to be extremely easy.

The second step, consisted in the estimation of the prejudicial effect of each feared event i.e., how much damage would be caused by all the potential impacts:

1. Negligible: Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.
2. Limited: Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.
3. Significant: Data subjects may encounter significant consequences, which they should be able to overcome albeit with serious.
4. Maximum: Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome.

The third step, verified the level of severity, which is determined by adding the respective personal data level of identification and prejudicial effects of potential impacts values obtained and locating the sum in the table below:

Level of Identification + Prejudicial effects	Severity
< 5	1. Negligible
= 5	2. Limited
= 6	3. Significant
> 6	4. Maximum

Table 3-5 Assessing the severity of each feared event

Feared Event	Level of identification of personal data	Most serious potential impact	Prejudicial effect of potential impacts	Maximum severity
Illegitimate access to personal data from outside OVERWATCH consortium	4. Maximum	• User account theft • Use of data for commercial purposes of for objectives outside the project scope	4. Maximum	4. Maximum
Illegitimate access to personal data from inside OVERWATCH consortium	4. Maximum	• User Account theft, • Use for scope outside the project • Use of data for commercial purposes of forobjectives outside the project scope	4. Limited	3. Significant
Disappearance of personal data	4. Maximum	• User must re-register • User lost his track history and acquired points	1. Negligible	2. Limited
Association user position through location data	3. Significant	• User location can be tracked • First Responders location can be tracked out of their work hours	3. Maximum	3. Significant
Association user-position through imagery data	3. Limited	• User location/habits can be tracked • Car plates can be identified	3. Maximum	3. Significant

Unwanted change of personal data	4. Maximum	• Faulty reporting errors by user	3. Significant	4. Maximum

Table 3-6 OVERWATCH severity matrix for feared events

In this context, the identification of threats was crucial, as they represent possible actions by risk sources that can lead to a feared event in OVERWATCH. To this end, a detailed and prioritised list of all threats has been identified and provided. As threats may affect the supporting assets, such supporting assets should be identified and estimated for each threat. In carrying out this activity three factors are considered: vulnerability of the assets, capabilities of risk sources and likelihood of the threat to actual happen.

First, the vulnerabilities of the supporting assets are estimated for each threat i.e. to what degree can the properties of supporting assets be exploited in order to carry out a threat:

1. Negligible: Carrying out a threat by exploiting the properties of supporting assets does not appear possible.
2. Limited: Carrying out a threat by exploiting the properties of supporting assets appears to be difficult.
3. Significant: Carrying out a threat by exploiting the properties of supporting assets appears to be possible.
4. Maximum: Carrying out a threat by exploiting the properties of supporting assets appears to be extremely easy.

Next, the capabilities of risk sources to exploit vulnerabilities (skills, available time, financial resources, proximity to system, motivation, feeling of impunity, etc.) are estimated for each threat:

1. Negligible: Risk sources do not appear to have any special capabilities to carry out a threat.
2. Limited: The capabilities of risk sources to carry out a threat are limited.
3. Significant: The capabilities of risk sources to carry out a threat are real and significant.
4. Maximum: The capabilities of risk sources to carry out a threat are definite and unlimited.

Finally, the likelihood of the threats is determined by adding the values obtained for the vulnerabilities of the supports and the capabilities of the risk sources and locating the sum in the table below:

Supporting asset vulnerability + Risk Source Capabilities	Likelihood
< 5	1. Negligible
= 5	2. Limited
= 6	3. Significant
> 6	4. Maximum

Table 3-7 Determination of likelihood for each threat

It is worth to note that, in this second issue, these items and related figures were re-assessed in order to assure that threats and related risks were adequately mapped and kept under control.

Feared Events	Most likely threats	Supporting asset vulnerabilities	Risk source capabilities	Maximum likelihood
Illegitimate access to personal data	• Software function creep	3. Significant	3. Significant	3. Significant

from outside OVERWATCH consortium	• Hardware function creep (e.g., storage) • Phishing, man-in-the-middle attack • Interception of Ethernet traffic • Acquisition of data sent over a Wi-Fi network, etc. • Unintentional disclosure of information • Information leakage during data exchange operations			
Illegitimate access personal data fro inside OVERWATC consortium	• Software function creep • Hardware creep • Assignment roles changes • Unintentional disclosure of information • Malicious generation of fake authenticated sessions • Unauthenticated access to OVERWATCH platform services	3. Significant	4. Maximum	4. Maximum
Disappearance personal data	• Software alteration • Hardware alteration or issues	2. Limited	3. Significant	3. Significant
Association use position throug locationdata	• Interception of Ethernet traffic • Data Information leakage during data exchange operations	3. Significant	3. Significant	3. Significant

	• Acquisition of data sent over a Wi-Fi network, etc.			
Association use position throug imagery data	• Interception of Ethernet traffic • Information leakage during data exchange operations • Acquisition of data sent over a Wi-Fi network, etc	2. Limited	2. Limited	1. Negligible
Unwanted change personal data	• Software function creep • Hardware function creep (e.g., storage)	3. Significant	3. Significant	3. Significant

Table 3-8 OVERWATCH likelihood matrix for feared events

3.4.2.1 Risk level analysis

The security of data is of utmost importance as it is directly correlated to data privacy and protection. In this direction, the assessment of potential risk in the OVERWATCH framework is described.

A risk is the result of feared events happening, that are generated by one or more threats; which may act through one or more supporting assets (e.g., system hardware, software component, communication channel), and which produces negative consequence on a primary asset (i.e., sensitive data). In brief, a risk consists of a feared event and all threats that may allow it to occur. The following figure summarizes in a visual way the concept of risk in data privacy and protection and the involved components.

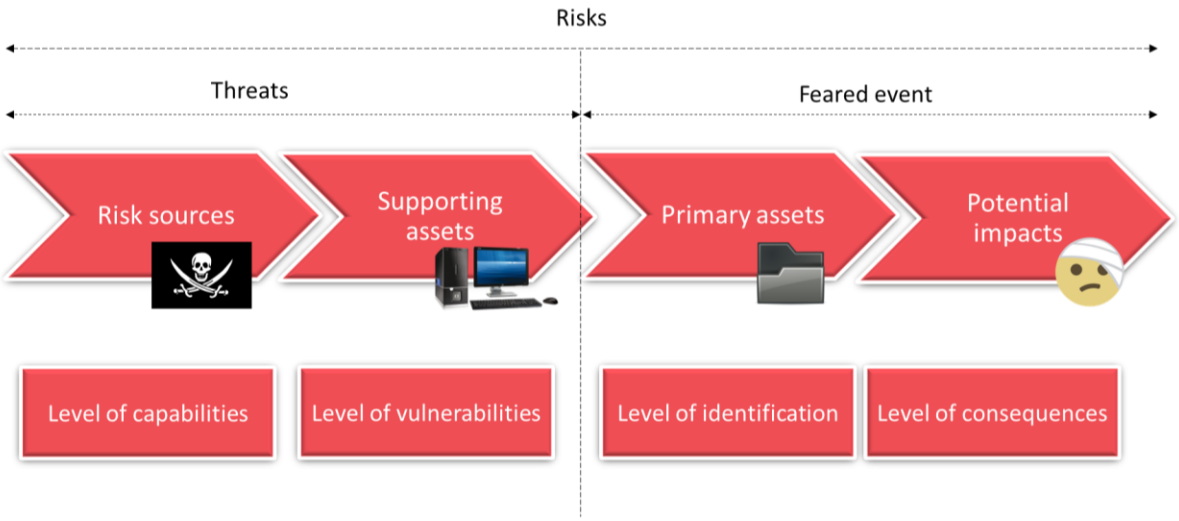


Figure 3-2 Risk components

Moreover, the risk level of each potential risk is determined as a function of risk severity and risk likelihood. While, the severity is equal to the severity of the feared event, while likelihood reflects the probability that relevant threats may successfully materialise through the identified supporting assets. Both these parameters are ranked in terms of the following classification: Negligible, Limited, Significant and Maximum. Hereafter, a list of potential privacy risks and the related severity and likelihood values for the OVERWATCH project are provided:

Risk #	Description	Severity	Likelihood
1	Illegitimate access to personal data from outside OVERWATCH consortium	4. Maximum	3. Significant
2	Illegitimate access to personal data from inside OVERWATCH consortium	3. Significant	4. Maximum
3	Illegitimate access to information collected in reports	4. Maximum	3. Significant
4	Loss of personal data	2. Limited	3. Significant
5	Loss of all/partial report information	4. Maximum	2. Limited
6	Association user-position through location data	3. Significant	3. Significant
7	Association user-position through imagery data	3. Significant	1. Negligible
8	Illegitimate change of personal data	4. Maximum	2. Limited
9	Disclosure of information from third-party sources with –non-disclosure constraints	4. Maximum	3. Significant

Table 3-9 OVERWATCH Privacy risk

After the potential risks are identified, a risk map is created based on severity of the feared event and the likelihood equal to the highest likelihood value of the threats is associated with the feared event (see figure below).

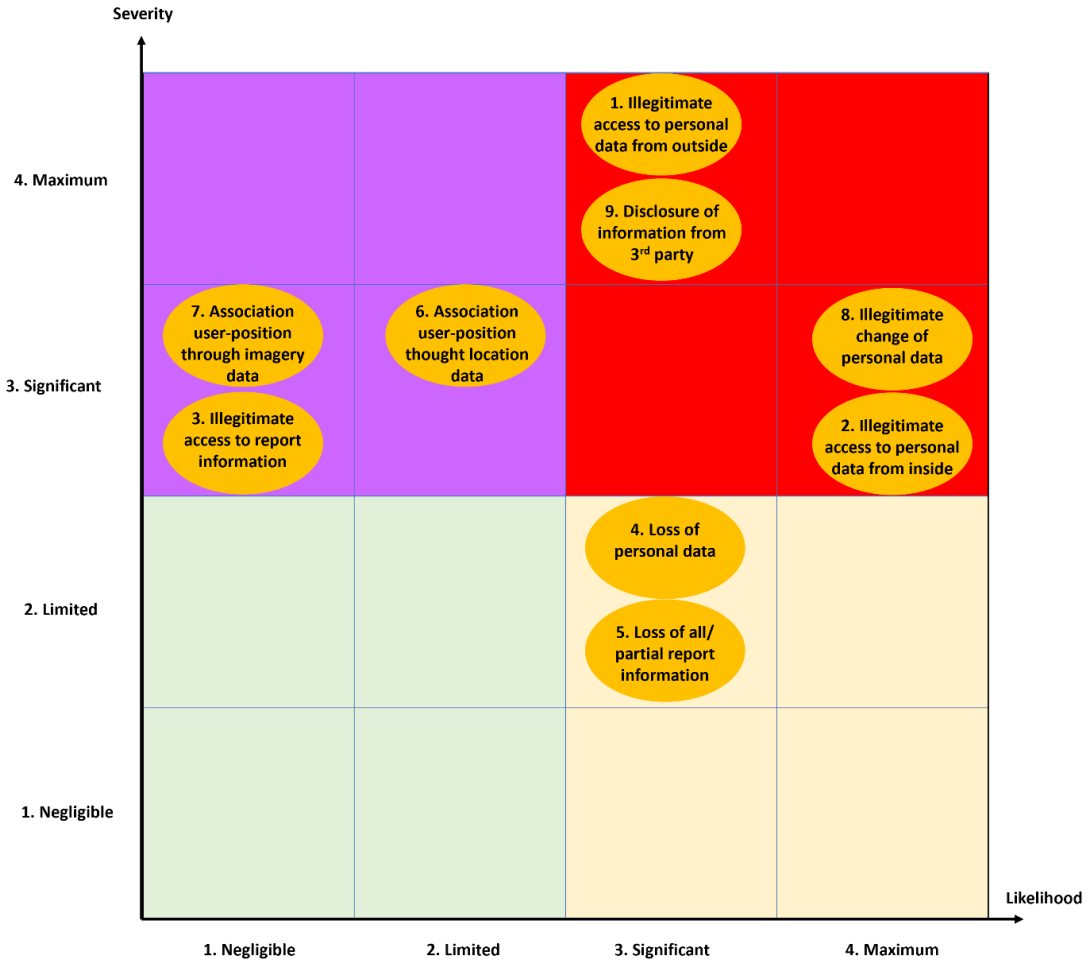


Figure 3-3 OVERWATCH risk map – BEFORE as presented in Issue 1

Where the envisaged processing is likely to result in a high risk to the rights and freedoms of natural persons, this risk assessment also informs the decision on whether a Data Protection Impact Assessment (DPIA) is required and supports its periodic review as processing evolve.
The ultimate goal of this 'exercise' is to build a protection system - compliant with the GDPR regulations and consistent with the OVERWATCH project technical requirements – that allows treating the risks identified in the previous step in commensurate manner. The used approach is based on the identification of measures, which can reduce the severity, and the likelihood levels of each risk until it can be considered acceptable for the system. As the project progressed, a new assessment of the risk level analysis was performed (Considering the feedback received from partners during the T6.3 activities).

3.4.2.2 Measures on primary assets

Potential measure	Description
Non-disclosure of personal and	Data related to the profile of the users must not be disclosed. These data will be only accessible to their direct owners and to users responsible for the management of the

location data	OVERWATCH platform. To prevent disclosure of unnecessary information (individual identity and location of an individual). The exact location of users will not be tracked to not disclose private information. Nonetheless, it is important that all the information provided in the report must be geo-localised. This requirement is directly connected to the previous one, i.e. non-disclosure of personal data. The approach adopted in OVERWATCH to avoid location tracking will be based a data separation technique that decouples the user personal data from the report's locations. User' personal data will be never displayed in the graphical interface, where the reports will be associated only with the user type (professional).
Data anonymization and pseudonymisation	Whenever possible data must be anonymised. In particular, while it is important to be able to retrieve the original user who did the original report, all the information gathered from generated report must be provided aggregated and in an anonymous form. Data anonymization techniques can be exploited in OVERWATCH encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Data minimization	Data minimisation at the earliest stage of processing is a core concept of privacy-enhancing technologies. In OVERWATCH only personal data necessary for the respective purpose of the project will be collected and processed. In the data collection stage and in the following processing stage, personal data treatment will be minimised as much as possible. Consequently, personal data will be erased or effectively anonymised as soon as it is not anymore needed for the given purpose.
Image objects detection and blurring	The detection of faces or other sensible objects (e.g., car plates) from images collected via the chatbot application and/or is another privacy issue that must be addressed. This aspect is still under discussion whether blurring is necessary as the type of client foreseen is to be found in the law enforcement and decision-making authorities. Yet, should it be required OVERWATCH will exploit one of the many open-source libraries and APIs for image detection and blurring that are still available on the market avoiding 'reinventing the wheel'.

Table 3-10 Potential measures for OVERWATCH primary assets

3.4.2.3 Measures on supporting assets

Potential measure	Description
Administration	To deliver consistent security administration and management, OVERWATCH will need a set of tools to define, administer and manage security policies consistently across the whole platform. Besides the technical aspects of risk mitigation, processes will also be inspected and detailed to identify the person/s who will be responsible for each task/activity/process. Where required, a Data Protection Officer (DATA MANAGER) is designated to advise on and monitor compliance with data protection obligations. The DATA MANAGER's contact details are published and communicated to the competent supervisory authority, and the DATA MANAGER acts as a contact point for the supervisory authority on issues relating to processing. An Ethics and Security Manager (ESM) supports the operational implementation of security and privacy policies, coordinates awareness and training activities, and facilitates internal workflows (e.g.,

	incident handling and evidence collection) in cooperation with the DATA MANAGER and relevant technical and management roles. In the event of a personal data breach, notification to the supervisory authority and, where applicable, communication to affected data subjects are handled by the controller in accordance with GDPR requirements, with the DATA MANAGER and ESM supporting the assessment, documentation, and mitigation actions.
Authentication and Perimeter Security	Users need to reliably identify themselves and then have that identity propagated throughout the OVERWATCH platform to access resources. All the users must be authenticated on the OVERWATCH platform. Moreover, user credentials must be stored securely. Since the OVERWATCH platform has been designed as a collection of remote services, the main authentication mechanism that will be adopted will be based on a token-sharing authentication through active sessions. In more details, each service communicating with the OVERWATCH platform is required to establish a trusted communication session. In the "handshaking" phase, when two services interact (e.g., AR, drones) for the first time, an encrypted token will be generated by the OVERWATCH platform and provided to each client service. This token will be used by clients to authenticate their requests. Similarly, the OVERWATCH platform will enable each client request only on the bases of a successful token verification.
Authorization - Restricted access to data and report information	Security administrators can define security policies at the database, table, column, and file levels, and can administer permissions for specific LDAP-based groups or individual users. Rules based on dynamic conditions such as time or geolocation can also be added to an existing policy rule. A permission-based mechanism may be integrated into the OVERWATCH platform to implement different access level for the information.
Secure communication anddata transfer	All the information collected in a report by a first-responder must be transmitted to the OVERWATCH platform on secure and trusted communication channels (e.g., based on HTTPS). The same also applies to data delivered to the users (e.g., through their chatbot app). The main focus is to avoid the leakage of the information, as well as malicious sniffing of sensible data. To this end, proper set of certificates will be generated and used to establish secure communications on the channels. The main protocol used for the data exchange will be the HTTP, since the OVERWATCH platform will expose data and functions through a series of RESTful services. Therefore, the protocol adopted for data exchange in the communication between the OVERWATCH platform and external modules will be the HTTPS, that combines HTTP with the SSL encryption. The same encrypted channel will be also used to exchange the token generated for authentication.
Data backup and recovery	2 reports the risk treatment measures illustrated in this paragraph and in section 3.4.2.2 describing how they are adopted to mitigate each of the presented list, and which is the effect in terms of re-estimation of severity and likelihood levels. Also, thanks to MinIO - single node multi drive - replicable and scalable on more logic file systems are enabled, allowing the data backup and recovery as well.
Secure data storage	The sensible information gathered from user-generated reports will be saved securely inside the OVERWATCH platform. The same strategy is also required for

	users' profile information and credentials. Different techniques can be adopted for these two categories of data. In the former case, a signature (hash) based encryption on the data could be applied. This is a one-way encryption strategy that would have the only objective of uniquely identify the user who created and/or validated the report data. On the other hand, two-ways encryption (i.e., encoding-decoding) can be adopted to securely store users' credentials. The same two-ways encryption strategy can be applied to data stored in the OVERWATCH platform data lake. More specifically, all the data collected from external sources that are under restricted privacy constraints outside the scope of the OVERWATCH project must be guaranteed.
Audit	Auditing is the monitoring and recording of selected user data actions. It can be based on individual actions, such as the type of query statement executed, or on combinations of factors that can include username, application, time, etc. Security policies can trigger auditing when specified elements are accessed or altered, including the contents within a specified object. Audit logs are retained for no longer than necessary for the purposes of accountability, security monitoring, and incident investigation, in line with the storage limitation principle. In the OVERWATCH project, the current operational retention period for audit logs is set to 1 year.

Table 3-11 Potential measures for OVERWATCH secondary assets

Selected risk-treatment measures	Risks								
	1.Illegitimate access to personal data from outside OVERWATCH	2.Illegitimate access to personal data from inside OVERWATCH	3.Illegitimate access to information collected in reports	4.Loss of personal data	5.Loss of all/partial report information	6.Association user-position through location data	7.Association user-position through imagery data	8.Illegitimate change of personal data	9.Disclosure of information from third-party sources
1. Administration	X	X	X	X	X	X	X	X	X
2. Authentication	X	X	X	X	X			X	X
3. Data Anonymization	X					X			
4. Data Minimization	X		X			X	X	X	X
5. Non-disclosure ofpersonal and location data	X		X			X			
6. Restricted accessto report information	X		X						X
7. Backup and Recovery				X	X			X	
8. Image objects detection & blurring							X		
9. Secure communication & data transfer	X		X						X
10. Secure storage	X			X	X			X	X
Residual severity	Significant	Limited	Significant	Negligible	Negligible	Significant	Limited	Limited	Limited
Residual likelihood	Limited	Significant	Limited	Negligible	Negligible	Limited	Negligible	Limited	Limited

Table 3-12 Selected risk-treatment measures

Coming to the results of the OVERWATCH risk analysis is clearly reported in Figure 3-4 showing the residual risk map after the inclusion of risk reduction measures on the OVERWATCH primary and the supporting assets.

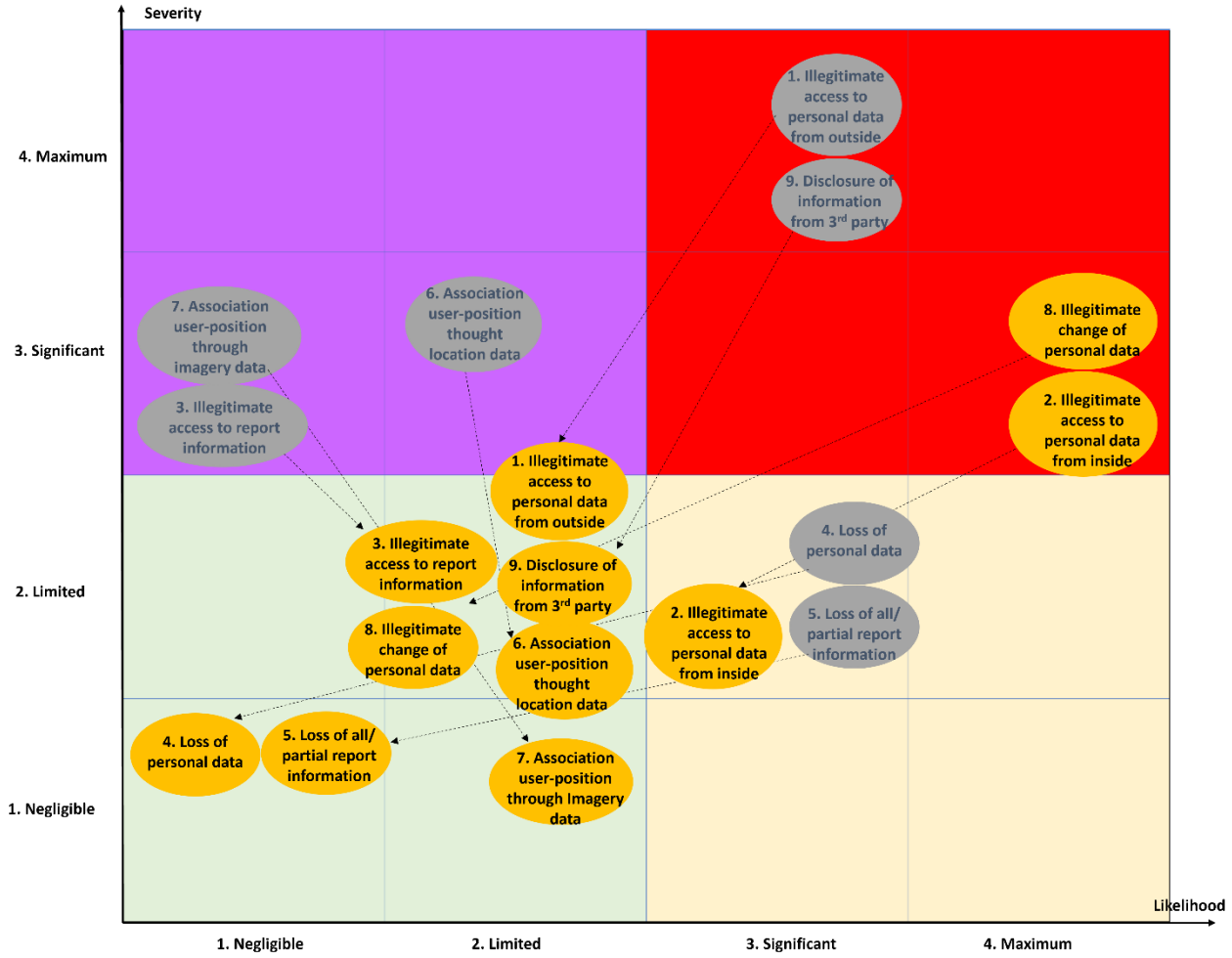


Figure 3-4 Residual risk map for OVERWATCH

The comparison between the risk map presented in Issue 1 and the updated assessment reflects a tangible and measurable improvement in the overall risk posture of the OVERWATCH project.
As shown in the figures above, the application of the risk treatment measures identified in Table 3-12, combined with the feedback received from the consortium partners during T6.3 activities, has resulted in a downward migration of the identified risks across the severity-likelihood matrix, bringing all nine feared events to a level that can be considered acceptable for the system in the current implementation context. In particular, risks that were previously positioned at the intersection of Maximum severity and Significant likelihood - such as Risk 1 (illegitimate access to personal data from outside the consortium), Risk 3 (illegitimate access to information collected in reports), and Risk 9 (disclosure of information from third-party sources subject to non-disclosure constraints) - have been repositioned following the application of the corresponding countermeasures, reflecting a reduction in their effective likelihood through the safeguards already in place. Similarly, Risk 2 (illegitimate access from inside the consortium), which presented a Maximum likelihood value in the original assessment, has been treated through internal access control and role-based authorisation measures, reducing its overall risk level. It is worth noting that this updated assessment does not indicate that all residual risk has been eliminated; rather, it confirms that the protection system built

around the OVERWATCH data architecture is functioning as intended and is proportionate to the nature and scale of the processing activities carried out to date.

4 Consortium Survey on PES Requirements

In light of the previous issue of this deliverable [RD18] and of the feedback and answers received from the consortium partners through the internal PES survey (see Annex 2), the present section provides an updated and more implementation-oriented view of the current status of the OVERWATCH project with regard to privacy, ethics and security requirements.
The purpose of this additional section is to complement the normative, methodological and risk-based analysis presented in Section 3 with direct evidence gathered from the partners involved in the development, integration and validation of the OVERWATCH solution. In more detail, the survey was used as a targeted assessment exercise in order to assess whether the assumptions, data flows, ethical safeguards, AI-related considerations and security measures described in D6.3 Issue 1 remain valid in the light of the practical activities carried out since October 2023.

The survey remained open for 98 days and collected 5 complete responses from designated representatives of consortium organisations involved in the technical and operational implementation of OVERWATCH. The average completion time was approximately 399 seconds (6 minutes and 39 seconds), reflecting the focused and structured nature of the instrument. The collected complete responses from designated representatives of consortium organisations involved in the technical and operational implementation of OVERWATCH. It is worth noting that the objective of the survey was not to establish a statistical sample for quantitative generalisation, but rather to provide a reliable and traceable internal snapshot of the current PES posture of the project, based on the direct reporting of the partners responsible for relevant technical components, demonstrations and field activities.
The questionnaire was organised around four thematic domains, namely: data flows and personal data processing; human involvement and ethical considerations; AI-based components and their preliminary qualification under the EU AI Act; and the evolution of the security posture since Issue 1.

4.1 Data flows and personal data processing

The first thematic domain of the survey addressed whether the data flows implemented in the project have changed since the publication of D6.3 Issue 1 and whether personal data has in fact been processed in the course of the activities carried out by the surveyed partners. On the question of whether any changes had occurred in the data flows described in the previous issue of the deliverable, all five respondents answered in the negative ("No"). This is a material and relevant finding, because it confirms that the data architecture and the related assumptions described in Section 3.2 of this deliverable remain valid at the present stage of project execution. More specifically, no respondent indicated the introduction of additional or unforeseen exchanges of information that would require the privacy analysis to be reopened or substantially revised. This stability is particularly important in the case of OVERWATCH, where the interaction between first responder reports, drone feeds, AR devices, server-side processing and visualisation tools had already been assessed under the Privacy-by-Design approach selected for the project. The absence of changes therefore supports the view that the design choices made at the outset have been sufficiently robust and that the initial conceptual modelling of the relevant information flows has remained aligned with the reality of implementation.

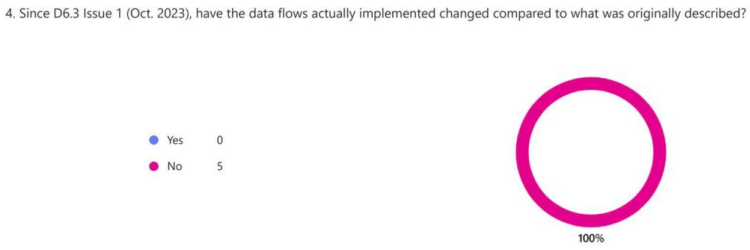


Figure 4-1 Data flows since D6.3 Issue 1

With regard to actual personal data processing, the responses are equally clear. All five respondents confirmed that their organisation has not processed personal or potentially identifiable data in practice, even incidentally (100% of responders replied "No"). This answer is further supported by the follow-up question on the categories of data that may have been involved. No respondent selected images or videos containing individuals or vehicles, geolocation data, user or operator identifiers, system or access logs, or derived personal data. Instead, all five respondents confirmed that no personal data has been processed. Taken together, these responses indicate that, at the time of the survey, the activities performed by the surveyed partners remain outside the scope of practical personal data processing. This outcome is coherent with the principles of data minimisation and privacy by default that underpin the PbD framework described in Section 3.2.1, and it also reflects the fact that the project is still in a controlled implementation phase in which operational deployment involving real-world personal data remains limited or absent. In practical terms, this means that the legal triggers associated with real processing operations under the GDPR have not yet been activated in relation to the surveyed activities.

This conclusion is confirmed by the responses relating to GDPR role qualification and DPIA obligations. All five respondents indicated that their organisation currently has no GDPR role in relation to the surveyed activities, and all confirmed that a Data Protection Impact Assessment is not required at this stage (100% of respondents replied "Not required"). This means that, based on the information reported by the partners, no organisation currently acts as Data Controller, Data Processor or Joint Controller in relation to personal data within the scope of the activities covered by the survey. Whilst this does not exclude the possibility that such roles may arise in later phases of the project, especially in the context of external demonstrations, pilot use or operational exploitation, it confirms that the current implementation context remains limited in terms of personal data exposure. It is worth noting, however, that the absence of current GDPR obligations should not be interpreted as a reason for inaction. On the contrary, it provides the consortium with an important preparation window during which governance measures, allocation of responsibilities and internal procedures can be clarified before the relevant obligations become operationally applicable.

Concerning data lifecycle governance, the survey reveals a more differentiated picture. Four out of five respondents reported that no specific measures are currently implemented in this area, whilst one respondent indicated that concrete measures are already in place, namely defined retention periods, role-based access control, deletion procedures after pilots or demonstrations, and anonymisation or pseudonymisation practices. At the present stage, this variation does not amount to a compliance problem, precisely because no actual personal data processing has been reported by the respondents. Nevertheless, it does point to an uneven level of organisational maturity across the consortium with regard to the operational management of data over time. This finding is relevant because such measures are closely connected to the lifecycle protection principle of Privacy-by-

Design and to the EBIOS-based logic of anticipating risk before processing begins. As the project moves closer to pilot demonstrations and potentially more operational settings, the consortium would benefit from progressively harmonising a minimum set of lifecycle governance practices across partners, drawing, where appropriate, on the measures already identified in the existing security and privacy treatment framework of this deliverable.

Figure 4-2 Questions 5 to 8 - Personal data processing, GDPR role qualification and DPIA status.

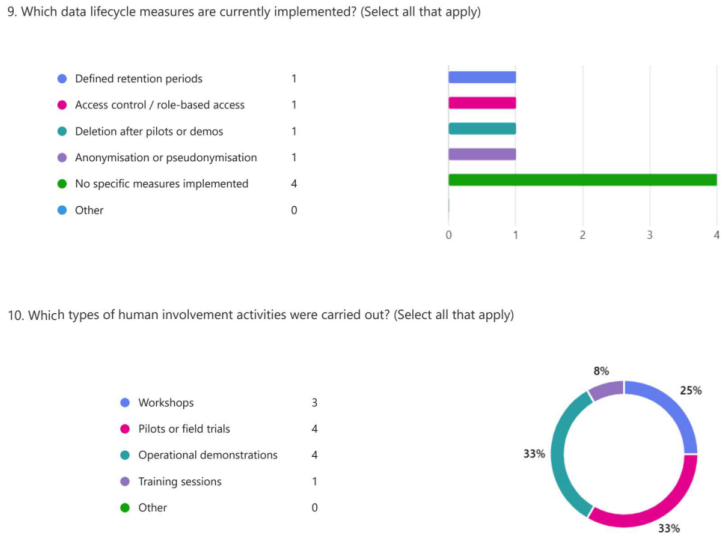


Figure 4-3 Questions 9 to 12 - Data lifecycle measures, human involvement activities and ethical sensitivities.

4.2 Human involvement and ethical considerations

The second thematic domain of the survey focused on the extent of human involvement in OVERWATCH activities and on whether any ethical concerns or sensitivities have emerged during the implementation of the project. The responses indicate that human participation has already occurred across several types of activities. Four respondents reported pilots or field trials, four reported operational demonstrations, three reported workshops, and one reported training sessions. This is an important finding, because it confirms that the project has already moved beyond purely internal technical development and has entered into forms of interaction that involve users, practitioners or stakeholders in real or quasi-real operational settings. In the context of OVERWATCH, such forms of engagement are ethically relevant because they may involve observation, participation, feedback collection, or the use of tools and procedures that affect human actors in emergency response scenarios. The survey results therefore provide practical confirmation that the ethical governance mechanisms described in Section 3.3 are not merely theoretical but are directly relevant to ongoing project execution.

On the specific question of informed consent and participant information, one respondent confirmed that informed consent forms and information sheets were used where required, whilst the remaining four selected "Not Applicable" and none selected "No". This is a reassuring result. It does not indicate any case in which formal consent documentation should have been used but was omitted. The "Not Applicable" responses are consistent with the nature of some of the activities reported, such as internal workshops, demonstrations among project staff, or technical sessions that do not involve external participants acting as research subjects. At the same time, this result confirms the practical utility of the informed consent templates provided in the Annex to this deliverable.

The fact that such templates already exist and have been used where appropriate places the consortium in a relatively strong position to manage future external trials and demonstrations in a compliant and ethically sound manner. In other words, the framework described in Issue 1 appears not only conceptually adequate but was also operationally usable.

The survey further indicates that no ethical concerns or sensitivities have emerged during the activities conducted so far. All respondents answered "No" to this question, and all responders also indicated that they do not foresee significant ethical risks in the future operational or commercial use

of the solution. More in detail, no respondent identified concerns related to function creep, misuse by third parties, diminished human oversight, or societal and reputational issues. This finding is positive and broadly consistent with the ethical checklist and governance approach already established within the project. However, it should be interpreted with a degree of caution. Ethical risks in projects such as OVERWATCH often emerge progressively, especially when tools move from controlled testing environments towards more realistic operational deployment. For this reason, the absence of concerns at the current stage should be seen as a positive interim status rather than as a final conclusion. It remains advisable that the consortium continues to monitor the four fundamental ethical principles identified in the deliverable, namely respect for human autonomy, prevention of harm, fairness, and explicability, in order to ensure that possible concerns are captured early as the platform matures.

4.3 AI-based components and EU AI Act considerations

The third thematic domain of the survey addressed the presence of AI-based components within the contributions of the surveyed partners and their preliminary categorisation under the EU AI Act. One respondent confirmed that its contribution includes AI-based components used in decision-support contexts, whilst the remaining four respondents indicated that they do not have AI components within the scope of their contribution. This is fully consistent with the architecture and functional orientation described in the previous issue of the deliverable, where AI-related functionalities are presented as tools supporting situational awareness and analytical assistance rather than as systems taking autonomous operational decisions. In this respect, the survey results suggest that AI within OVERWATCH remains limited in scope, targeted in use, and still embedded within a broader human-centred operational setting. This matters, because the risk and compliance implications of AI depend heavily not only on the presence of algorithmic elements, but also on the function they perform, the data they use, and the degree of human oversight that remains in place.

As regards the preliminary qualification of the identified AI component under the EU AI Act, the respondent concerned classified it as minimal risk, whilst the remaining responses were not applicable. On the basis of the information available through the survey and the functional description already included in this deliverable, this appears to be a reasonable preliminary position. Nonetheless, this should not be treated as definitively settled. The regulatory treatment of AI systems depends on concrete deployment context, intended purpose, user environment and the potential impact on health, safety and fundamental rights. Since OVERWATCH is linked to emergency and crisis management scenarios, future evolutions of the relevant components could attract closer regulatory attention if their role becomes more operationally influential. It is therefore advisable that the consortium continues to monitor both the maturation of the technical components and the development of interpretative guidance under the EU AI Act framework.

With regard to safeguards applied to AI-generated outputs, the respondent with AI in scope indicated the use of human validation before operational use and the provision of confidence or uncertainty indicators. No respondent selected restrictions based on user role or context, active monitoring of AI performance, or explicit disclaimers on the advisory nature of outputs. Three respondents selected the option indicating that no specific safeguards are implemented, which is understandable given that most of them reported no AI components at all. The safeguards that were identified are relevant and aligned with the principles of human oversight and explicability already described in the current deliverable. However, the survey also suggests that the consortium would benefit from a more explicit and shared minimum governance baseline for AI-enabled functionalities, even if these functionalities

remain limited in number. Such a baseline could include common wording on the advisory role of outputs, traceability of model assumptions, explicit human-in-the-loop validation procedures, and internal criteria for determining when a reassessment under the AI Act may be required. Introducing such a baseline would not be an excessive burden; it would be a sensible anticipatory measure consistent with the project's preventive approach to ethics, privacy and security.

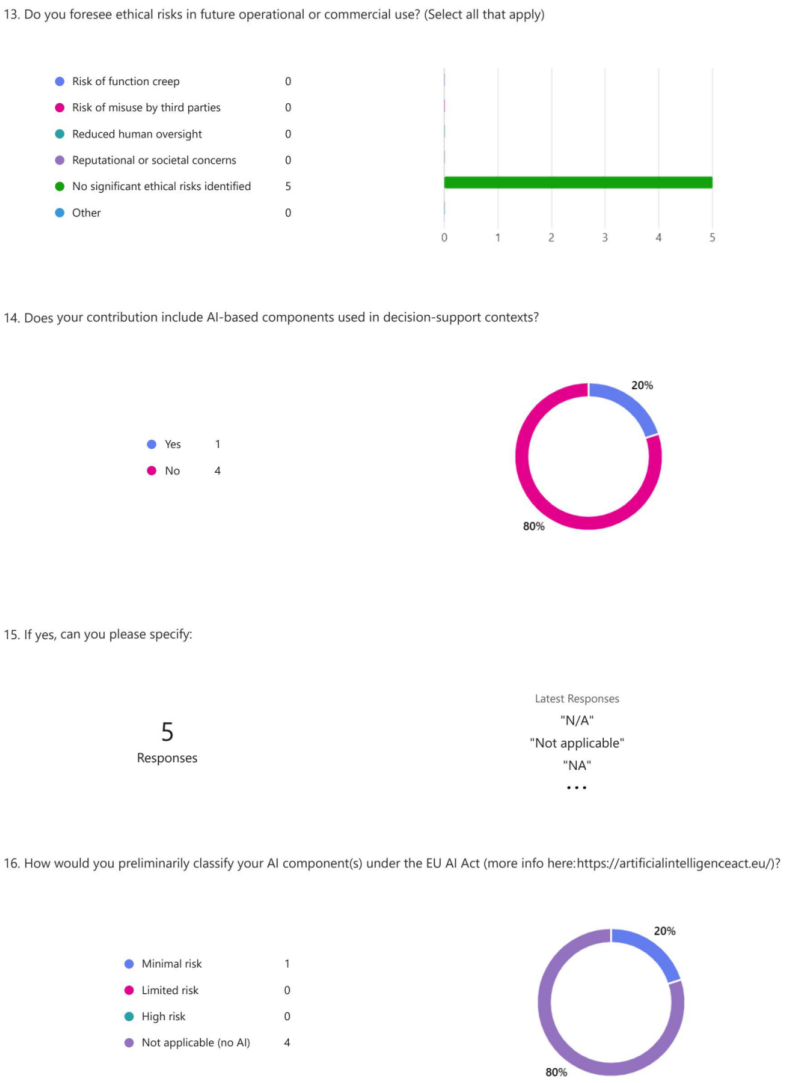


Figure 4-4 Questions 13 to 16 - Future ethical risk outlook, AI components and EU AI Act classification.

4.4 Security posture and evolution since Issue 1

The fourth thematic domain of the survey focused on whether any security issues had been identified, since the publication of D6.3 Issue 1 [RD18], and whether any security measures had been added or modified during the intervening period. The overall picture is reassuring.

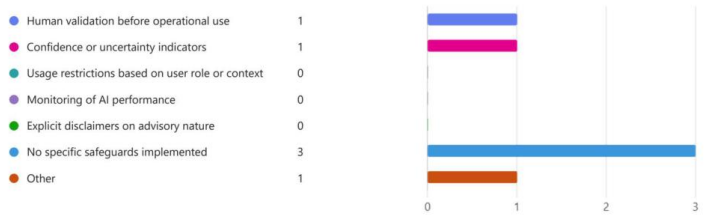
Four out of five of respondents reported that no threats or vulnerabilities had been identified since Issue 1. No respondent reported unauthorised access attempts, authentication or authorisation weaknesses, misconfiguration issues, or availability and resilience problems. These results suggest that the technical and organisational security measures already described in Section 3.4 have remained broadly effective under the current implementation conditions. This is an important point, because the security architecture of OVERWATCH relies on a combination of software components, interfaces, service communications and distributed assets, meaning that even minor weaknesses could have a disproportionate impact if not properly controlled. The absence of reported incidents

or vulnerabilities therefore indicates that, at least within the scope covered by the survey, the baseline protections remain adequate.

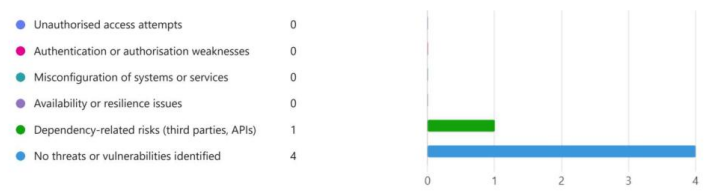
At the same time, one respondent reported dependency-related risks linked to third-party components or APIs. This is not a marginal point. In a distributed and service-oriented environment such as OVERWATCH, dependency risks are a realistic and foreseeable part of the security landscape. The platform relies on interoperable modules and, in some cases, on externally sourced services or datasets. This means that the security posture of the system is influenced not only by what the consortium develops directly, but also by the robustness, integrity and update practices of external components on which some functionalities depend. The identification of this risk therefore adds credibility to the survey, because it reflects a realistic implementation concern rather than an artificial picture of zero exposure. It is also consistent with the threat scenarios and treatment logic already set out in Section 3.4 and in the related risk tables. In practical terms, this issue should continue to be monitored through configuration control, dependency management, secure communication practices and audit procedures, rather than being treated as an isolated observation.

On the question of updates to security measures, four respondents reported that no changes had been made since the previous issue, whilst one respondent reported improvements in authentication and authorisation, encryption and secure communications, and monitoring and audit logging. Although no further descriptive detail was provided in the free-text follow-up, these three areas correspond closely to the core technical safeguards already emphasised in the current deliverable. This means that the reported improvements are not random or disconnected actions, but rather developments that appear to strengthen exactly the areas that had already been identified as important for the protection of both primary and supporting assets. In particular, stronger authentication and authorisation measures reduce the risk of improper access, improved encryption strengthens confidentiality in transit, and enhanced audit logging supports traceability, accountability and incident review. The finding therefore suggests that at least one partner has continued to evolve its security posture in a direction fully consistent with the risk treatment logic of D6.3. This is a positive sign, because it indicates that the deliverable has not remained a static compliance document, but has continued to function as a practical reference framework for ongoing technical improvement.

17. Which safeguards are currently applied to AI-generated outputs? (Select all that apply)



18. Have any of the following security issues been identified since Issue 1? (Select all that apply)



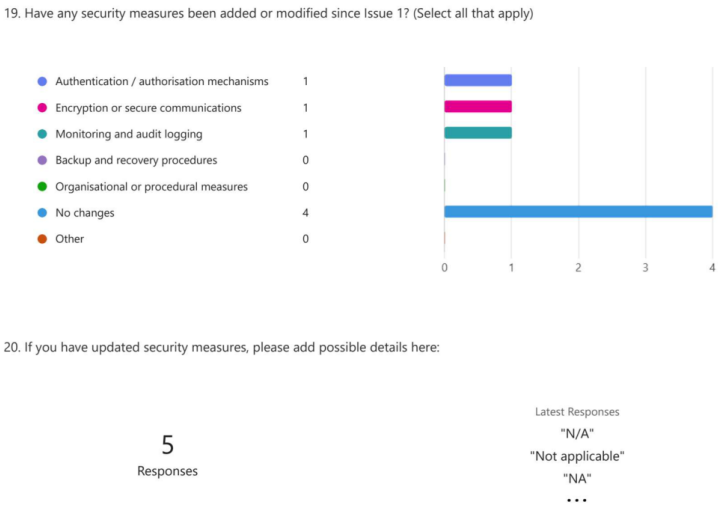


Figure 4-5 Questions 17 to 20. AI output safeguards, security issues identified and security measure updates.

4.5 Key findings and implications for Issue 2

The findings of the internal PES survey provide a coherent and overall positive picture of the present status of the project. In summary, the main conclusions that can be drawn are the following:

The data flows implemented since Issue 1 have remained unchanged, which confirms the continued validity of the privacy analysis and design assumptions already described in the current deliverable. No surveyed partner has processed personal or potentially identifiable data in practice to date, and no GDPR roles or DPIA obligations are currently triggered within the scope of the activities covered by the survey.

The maturity of data lifecycle governance measures is uneven across the consortium, which is not yet problematic but should be addressed before more operational and data-intensive phases begin. Human involvement is already substantial across pilots, demonstrations, workshops and training activities, and the ethical governance mechanisms already defined by the project appear to be functioning effectively.

AI-based components are present only in a limited part of the surveyed contributions and are currently viewed as minimal risk; however, their future classification and governance should remain under review as technical maturity and deployment context evolve.

The security situation remains under control, with no major issues reported, one realistic dependency-related risk identified, and targeted improvements in core security safeguards already implemented by one partner.

In particular, the survey results reported in this section support the view that, at the current stage, no major issues are present, in particular in relation to privacy and ethics requirements. For what concerns security requirements, the identified risks remain under control and the measures in place continue to be consistent with the risk treatment approach already described in this deliverable.

5 Conclusions

The present document has reported on the ethical, privacy and security requirements and considerations applicable to the OVERWATCH project, providing guidelines, methodologies and practical measures to support the consortium in maintaining compliance with the applicable European and national legal framework throughout the full duration of the project.

In particular, the privacy analysis conducted in the context of Task 6.3 has confirmed that the Privacy-by-Design approach selected for OVERWATCH, structured around the seven principles of PbD and implemented through the EBIOS risk management methodology, provides a solid and coherent basis for the protection of personal data across all relevant processing contexts.
The ethical framework established since the early stages of the project, including the appointment of the Ethics and Security Manager, the adoption of the ethical checklist, and the development of informed consent templates for human participants, has similarly proved adequate and operationally functional, as confirmed by the results of the internal PES survey reported in Section 4.
With regard to security, the risk assessment carried out in Section 3.4 has enabled the consortium to identify relevant feared events and threat scenarios, assess their potential severity and likelihood, and define a coherent set of risk treatment measures for both primary and supporting assets, as summarised in the risk-treatment table in Section 3.4.
With regard to security, the risk assessment carried out in Section 3.4 has allowed the consortium to identify the feared events and threat scenarios most relevant to the OVERWATCH system architecture, to evaluate their likelihood and potential severity, and to select a coherent set of risk treatment measures for both primary and supporting assets, as summarised in Table 3-12.
The internal PES survey further confirms that the security posture of the consortium has remained stable and consistent with the risk treatment framework described in this deliverable, with no major incidents reported and targeted improvements already implemented by at least one partner in the areas of authentication, encryption and audit logging.
At this stage, no major issues are present in relation to privacy and ethics requirements, whilst the one security-related dependency risk identified through the survey is fully consistent with the scenarios already anticipated in the risk analysis and is addressed through the measures already in place.
Overall, it can be concluded that the OVERWATCH project has adequately addressed the privacy, ethics and security dimensions within the scope of this deliverable, and that the governance structures, risk treatment measures and ethical safeguards currently in place provide a coherent and proportionate response to the risks and obligations identified.

Looking ahead, the consortium recognises that the regulatory landscape within which OVERWATCH operates has evolved significantly since the beginning of the project and will continue to do so. The entry into force of the EU AI Act and the full applicability of the EU Data Act, together with the ongoing legislative negotiations on the Digital Omnibus package and the continued maturation of the European data strategy, mean that the compliance requirements applicable to platforms such as OVERWATCH will become progressively more detailed and more demanding. At the same time, the transition from a controlled research and development environment towards potential operational deployment will bring the project closer to real-world data processing scenarios in which the legal triggers under the GDPR, the AI Act and the Data Act may become fully operative. The OVERWATCH consortium is well positioned to manage this transition. The Privacy-by-Design methodology, the EBIOS risk management framework, the ethical governance structures and the security measures documented in this deliverable were deliberately designed to be adaptable rather than static, and the internal PES survey has confirmed that they have functioned effectively throughout the project lifecycle. The consortium therefore concludes this deliverable with reasonable confidence that the foundations laid are not only adequate for the current phase of the project, but also sufficiently robust and forward-looking to support the responsible evolution of the OVERWATCH solution beyond the scope of this grant agreement.

References

ID	Title	Revision	Access Date
[RD01]	OVERWATCH Grant Agreement	-	2023
[RD02]	Data Protection in the EU, European Council of the European Union. Source: link	-	2023
[RD03]	ePrivacy Directive, European Data Protection Supervisor. Source: link	-	2023
[RD04]	The Charter of Fundamental Rights of the European Union, Aid, Development cooperation, Fundamental rights, European Commission website. Source: link	-	2023
[RD05]	The EU Data Governance Act explained, European Commission. Source: link		2023
[RD06]	The Ethics Guidelines for Trustworthy AI, Shaping Europe's digital future, European Commission. Source: link	-	2023
[RD07]	D6.2 OVERWATCH Data Management Plan. Source: link	-	2023
[RD08]	Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Source: link	-	2023
[RD09]	Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe. April 2018. Source: Link	-	2023
[RD10]	Proposal for a Regulation laying down harmonised rules on artificial intelligence, Policy and Legislation. Publication 21 April 2021. Source: link	-	2023
[RD11]	Ann Cavoukian. Privacy by Design – The 7 Foundational Principles, January 2011. (Revised version). Source: link	-	2023
[RD12]	Privacy and Data Protection by Design, EU Agency for Cybersecurity- ENISA, 2015. Source: link ENISA	-	2023
[RD13]	European Code of Conduct for Research Integrity. Source: link	-	2023
[RD14]	Ronald Hes and John J. Borking. Privacy-enhancing technologies: The path to anonymity. Technical report, Registratiekamer, 1995	-	2023

[RD15]	Emerging privacy-enhancing technologies. Current regulatory and policy approaches, OECD, 2023. Source: link	-	2023
[RD16]	EBIOS approach. Source: link	-	2023
[RD17]	ISO/IEC 27005:2018. Source: link	-	2023
[RD18]	D6.3 Privacy, Security, Ethics requirements - Issue 1	-	2023
[RD19]	Data Act full text: Regulation (EU) 2023/2854. link	-	2026
[RD20]	European Commission, Data Act explained (fact page). link	-	2026
[RD21]	European Commission, Data Act policy page (confirms 12 September 2025 applicability). link	-	2026
[RD22]	Article 15 (exceptional need) link	-	2026
[RD23]	AI Act full text (Official Journal): Regulation (EU) 2024/1689, published 12 July 2024. link	-	2026
[RD24]	European Commission, AI Act implementation timeline (AI Act Service Desk). link	-	2026
[RD25]	European Parliament, AI Act implementation timeline briefing (EPRS, 2025). link	-	2026
[RD26]	EU Artificial Intelligence Act Implementation Timeline (Future of Life Institute tracker) link	-	2026

Annex

1 Information sheet – Online forms

Thank you for your interest in participating in the OVERWATCH project (www.overwatchproject.eu). Before you agree to take part, the person organising the research must explain the project to you and you should read the Information Sheet of the project provided. If you have any questions arising from the Information Sheet or explanation already given to you, please ask the researcher before you decide whether to join in. Please note that the general information regarding any personal data will be not disclosed. Moreover, our research will present only aggregated data (not individual results) and your personal data will remain confidential.

Should you have any additional questions related to how we manage your data please contact our Data Manager and, as well, our Ethics and Security Manager:

Data Manager
Name: Federico Monteforte
Email: federico.monteforte@ithacaweb.org
Post Address: ITHACA S.r.l.
via P.C. Boggio 6, 10138 Torino (TO) - Italy

Ethics and Security Manager
Name: Elizabeth A. Nerantzis
Email: en@alphacons.eu
Post Address: ALPHA CONSULTANTS SRL,
Viale Cirene 7, 20135 Milano (MI) – Italy

Participant's Statement

I declare that: *Please initiate all boxes*

I have read the notes written above and read the OVERWATCH Information sheet, and understand what the study involves. I have been given the opportunity to ask questions and have had them answered to my satisfaction.	☐
I understand that my participation is voluntary and that I am free to withdraw at any time without giving a reason immediately without consequences.	☐
I have been given the information about the expected duration of the subject's participation and that personal data will be held for a period of no longer than 4 years after the completion of the OVERWATCH project.	☐
I consent to the processing of my personal information the OVERWATCH project, which will remain confidential.	☐
I agree that the research projects named above have been explained to me to my satisfaction and I agree to take part in this study.	☐
I understand that the information I have submitted will be published, as a report, scientific publication or other dissemination and communication outputs. Confidentiality and anonymity will be maintained and it will not be possible to identify me from any publications.	☐

I agree that my non-personal research data may be used by others for future research. I am assured that the confidentiality of my personal data will be upheld through the removal of identifiers.

I understand that such information will be treated as strictly confidential and handled in accordance with the provisions of the EU General Data Protection Regulation (Reg. 2016/679). ☐

Signature Checkbox Date

This project has received funding from the European Union's Horizon Europe programme (CALL:HORIZON-EUSPA-2021-SPACE) under grant agreement no. 101082320.

2. Internal Consortium PES survey

Privacy, Ethics and Security - PES update survey

The aim of this survey is to collect information to update the Deliverable D6.3 - Privacy, Ethics and Security Report (Issue 2). Please answer on behalf of your organisation. The questionnaire should take no longer than 20 minutes.

In accordance with Regulation (EU) 2016/679 (GDPR), all personal data collected in the context of this activity will be processed lawfully, fairly, and solely for specified and legitimate purposes. Data processing will be limited to what is strictly necessary, and appropriate technical and organisational measures will be applied to ensure confidentiality and security. Any information enabling the identification of interviewees will be removed at the earliest possible stage. The **final output will contain only anonymised and aggregated data,** ensuring that individuals are no longer identifiable in accordance with Recital 26 GDPR. Personal data will be retained only for the duration necessary to fulfil the purposes of the activity and will then be securely deleted or anonymised.

Should you have any question please contact the OVERWATCH Ethics and Security Manager (ESM): en@alphacons.eu. For general Data Protection Issues please contact OVERWATCH Data Protection Officer (DATA MANAGER): federico.monteforte@ithacaweb.org

* Required

Privacy and Data protection (GDPR)

4. Since D6.3 Issue 1 (Oct. 2023), have the data flows actually implemented changed compared to what was originally described? *
   - ☐ Yes
   - ☐ No
5. Has your organisation processed personal or potentially identifiable data in practice, even incidentally?
   - ☐ Yes

- [ ] No

6. If personal data was processed, which of the following types were involved? (Select all that apply)
   - [ ] Images or video containing people or vehicles
   - [ ] Geolocation data
   - [ ] User or operator identifiers
   - [ ] System or access logs
   - [ ] Derived or inferred personal data
   - [ ] No personal data processed
   - [ ] Other

Please specify if "Other" _____

7. Based on implemented processing, how does your organisation currently qualify its role under GDPR? *
   - [ ] Data Controller
   - [ ] Data Processor
   - [ ] Joint Controller
   - [ ] No GDPR role (no personal data processed)
   - [ ] Not yet assessed
   - [ ] Other

Please specify if "Other" _____

8. What is the current status of any Data Protection Impact Assessment (DPIA) related to your activities? *
   - [ ] Not required
   - [ ] Completed
   - [ ] Ongoing
   - [ ] Planned
   - [ ] Not assessed yet

9. Which data lifecycle measures are currently implemented? (Select all that apply)
   - [ ] Defined retention periods
   - [ ] Access control / role-based access
   - [ ] Deletion after pilots or demos
   - [ ] Anonymisation or pseudonymisation
   - [ ] No specific measures implemented
   - [ ] Other

Ethics & Human involvement

10. Which types of human involvement activities were carried out? (Select all that apply)
    - [ ] Workshops
    - [ ] Pilots or field trials
    - [ ] Operational demonstrations
    - [ ] Training sessions
    - [ ] Other

11. Where human involvement occurred, were informed consent forms and participant information sheets used? *
- [ ] Yes
- [ ] No
- [ ] Not Applicable

12. Did any ethical concerns or sensitivities emerge during project activities?
- [ ] Yes
- [ ] No

13. Do you foresee ethical risks in future operational or commercial use? (Select all that apply)
- [ ] Risk of function creep
- [ ] Risk of misuse by third parties
- [ ] Reduced human oversight
- [ ] Reputational or societal concerns
- [ ] No significant ethical risks identified
- [ ] Other

Artificial Intelligence and Decision Support ethics

14. Does your contribution include AI-based components used in decision-support contexts?
- [ ] Yes
- [ ] No

15. If yes, can you please specify: *

16. How would you preliminarily classify your AI component(s) under the EU AI Act (more info here: https://artificialintelligenceact.eu/)?
- [ ] Minimal risk
- [ ] Limited risk
- [ ] High risk
- [ ] Not applicable (no AI)

17. Which safeguards are currently applied to AI-generated outputs? (Select all that apply)
- [ ] Human validation before operational use
- [ ] Confidence or uncertainty indicators
- [ ] Usage restrictions based on user role or context
- [ ] Monitoring of AI performance
- [ ] Explicit disclaimers on advisory nature
- [ ] No specific safeguards implemented
- [ ] Other

Security and Risk management

18. Have any of the following security issues been identified since Issue 1? (Select all that apply)

- ☐ Unauthorised access attempts
- ☐ Authentication or authorization weaknesses
- ☐ Misconfiguration of systems or services
- ☐ Availability or resilience issues
- ☐ Dependency-related risks (third parties, APIs)
- ☐ No threats or vulnerabilities identified

19. Have any security measures been added or modified since Issue 1? (Select all that apply)

- ☐ Authentication / authorisation mechanisms
- ☐ Encryption or secure communications
- ☐ Monitoring and audit logging
- ☐ Backup and recovery procedures
- ☐ Organisational or procedural measures
- ☐ No changes
- ☐ Other

20. If you have updated security measures, please add possible details here: