Overwatch

Privacy, ethics and security report

Deliverable 6.3

Work package: **WP6**
Dissemination level: **PU**
Lead partner: ALPHA
Authors: **Elizabeth A. Nerantzis**
Due date: **31/10/2023**
Submission date: **31/10/2023**

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
Work Package	6
Dissemination Level	PU
Nature[1]	O
Author(s)	Elizabeth A. Nerantzis (ALPHA)
Co-Author(s)	ALPHA
Date	31/10/2023
Status	Draft
Revision	ENG
Reviewed by (if applicable)	Giuseppe Vella, Tommaso Nicoletti
Information to be used for citations of this report	Nerantzis E.A. (2023): Privacy, Ethics and Security report, D6.3, OVERWATCH. Horizon EUSPA Space 2021 Grant Agreement No 101082320.

Deliverable abstract	This is the first issue of the "Privacy, ethics and security report" deliverable of the OVERWATCH project. It provides and initial report 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	17/08/2023	ToC	E.A. Nerantzis
2	24/10/2023	Draft shared to ENG as peer reviewers	
3	27/10/2023	Implementation of received feedback	E.A. Nerantzis
4	30/10/2023	Final draft shared to Coordinator for EC submission	
5	22/01/2024	Addresses Reviewers comments	E.A. Nerantzis

List of authors, contributors and reviewers

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

Abbreviations

AI	Artificial Intelligence
AR	Augmented Reality
CEMS	Copericus 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

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].This document describes the ethical, privacy and security considerations as well as the respective procedures that are in place at a 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 will adopt for the relevant ethical issues, in particular for the human involvement. Two versions of this deliverable have been foreseen. This document represents the Issue 1 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 information on the ethical issues and assessment of potential threats related to privacy, ethics and/ or security that may have emerged during the project, with suggested countermeasures.	M36 (Oct 2025)

The OVERWATCH Ethics and Security Manager was identified and appointed.The ESM is responsible for providing advice and coordinating activities for what concerns the fulfilment of the ethical obligations of OVERWATCH. The ESM supporded by the appointed Data Manager for certain activities, 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.

In this context, the Privacy, Ethics and Security 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;
- EU Cookie Directive – Directive 2009/136/EC;
- EU Data Governance
- Charter of Fundamental Rights (CFR) of the European Union (2012/C 326/02)
- Council Framework Decision (2005/222/JHA).
- Future normative outlooks (e.g., the AI directive)

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 before they 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 into the 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, 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 ensures a 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.

Also, the "Expression des Besoins et Identification des Objectifs de Sécurité" (EBIOS) risk management approach for OVERWATCH data privacy and protection has been selected. - which follows the guidelines of Privacy-By-Design methodologies provided by the GDPR – and the related principles are described. In brief, this approach allows to analyse the risk posed to privacy by the processing of personal data (See section 3.6). This security approach 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 will be implemented as soon as 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: EU General Data Protection

Regulation (GDPR); EU Data Act, Charter of Fundamental Rights of the European Union on Human Rights; ePrivacy Directive; and the European Code of Conduct for Research Integrity (see section 3). Moreover, 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

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, there are in place 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 ethics risks related to the 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 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; 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 reports 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 pseudo-anonymization	Whenever possible data must be anonymised. 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'.

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.

	Following the recommendations of the GDPR, a Data Protection Officer will be appointed to direct and oversee all data protection activities. In OVERWATCH this figure is comprised in the Ethics and Security Manager figure. The ESM devises the policies and procedures that bring the organisation into compliance with the Regulation, monitors the implementation of those policies, ensures that all staff are fully trained in regard 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 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	Table 3-11 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. According to the EU GPDR, log audits must be collected and stored for a period of 1 year.

It is worth to be noted that the present analysis has been performed at very early stage of the project execution, advising on a set of countermeasures for risk mitigation that should be applied on the entire system implementation. For this reason, a key factor for the success of this methodology will be to iterate this process in order to have a constant check over the validity of the proposed Privacy- by-Design approach, in anticipation of any possible changes in the system design driven by technical or architectural needs and/or choices. At this stage, no major issues are present, especially in relation to the privacy and ethics requirements. For what concerns specifically the security requirements, so far, all identified risks are under control and possible actions are being implemented in order to minimise the impact of such risks. Moreover, it it is worth noting that all the above mentioned risks will be monitored and updated throughout the duration of the project, and presented in Issue 2, expected by M36, reflecting the evolution of the OVERWATCH project.

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 D6.3 “Privacy, Ethics and Security Requirements” – Issue 1:

Version	Content	Due date
Issue 1 (First Draft)	Guidelines and methodologies to ensure that privacy legislations are not infringed (such as the Directive 95/46/EC and the forthcoming General Data Protection Regulation) 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	M12 (Oct 2023)

	related to privacy, ethics and/ or security that may appear during the project, with suggested countermeasures to overcome them.	
Issue 2 (Final)	Updated information on the ethical issues and assessment of potential threats related to privacy, ethics and/ or security that may have emerged during the project, with suggested countermeasures.	M36 (Oct 2025)

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 draws the first conclusions of the the present issue.

2 OVERWATCH ethics and security manager

Due 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[2], 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 (DPO) 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 DPO, 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 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 delivered to the 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

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

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.

In case the ESM changes, the project coordinator will communicate such changes it to all interested parties in the shortest period.

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 ePrivacy Directive is currently under revision to align it with the GDPR and to extend its scope to new services and technologies [RD03].
- 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 for ethics, privacy and data security, translating into well-established ethical concepts and guidelines, such as informed permission, privacy by design and default, and safe data management methods and on only the bare minimum of personal data is collected in order to achieve the study goal.

Moreover, addressing the FAIRness of data, 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[3] (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.

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

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:

- 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
- Charter of Fundamental Rights (CFR) of the European Union (2012/C 326/02); and
- Council Framework Decision (2005/222/JHA); and
- Upcoming normative outlooks

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, and became 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 cannot be processed without a legal ground or the agreement of the data subject. This usually entails that the data subject has to give his/her consent to the processing of his or her personal data for one or more specific purposes; however, different legal grounds may apply, in different instances, which could exempt controllers or processors from collecting the data subject's consent. This holds true when personal data 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).

5) 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).
6) 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.
7) 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.
8) 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.
9) 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.

10) Procedures to handle and notify data breaches to data protection authorities and data subjects concerned must be in place.
11) 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.
12) 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.
13) 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.
14) 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.
15) 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[4];
- 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[5] and soon to replaced by the ePrivacy Regulation - 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. Access to, or storage of, information into the users' devices must be authorized by the users with a specific consent, unless it is "strictly necessary in order to provide a service explicitly requested by the subscriber or user" (so called "cookie law", Prior Consent). In other words, any website, or app should provide clear information on its the cookies it deploys into the users' devices and collect the prior consent, where necessary.
5. 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);

[4] 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.

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

- 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).

6. 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 (Authorization profiles).

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 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 the data intermediation services that could derive as an output of the project.

3.1.4 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 will ensure compliance tending to the data protection and lawful use of data.

3.1.5 Council Framework Decision 2005/222/JHA

The Council Framework Decision (2005/222/JHA) of November 2008 addresses the most significant forms of criminal activity against information systems, such as hacking, viruses and denial of service 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.This Directive 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 compliant to this Directive, to address confidentiality, integrity, authentication and non-repudiation features of the platform.

3.1.6 Future normative outlooks

As the EU is recognising the value of Artificial Intellingence, the European Commission designed a European AI Strategy which aims at making the EU a world-class hub for AI and ensuring that AI is human-centric and trustworthy. Such an objective translates into the European approach to excellence and trust through concrete rules and actions [RD09][RD10].

Currently, the Commission has proposed the first ever legal framework on AI, which addresses the risks of AI and positions Europe to play a leading role globally.

At this stage, the Proposal for a Regulation on artificial intelligence (AI act) was announced in April 2021. It aims to address risks of specific uses of AI, categorising them into 4 different levels: unacceptable risk, high risk, limited risk, and minimal risk.

The AI Act proposes to classify AI systems according to their level of risk for human safety, health, rights, and freedoms, and to impose different obligations on providers and users of AI systems depending on their risk category. The AI Act also proposes to establish a governance structure for AI at the EU level, involving national authorities, a European Artificial Intelligence Board (EAIB), European Union Agency for Cybersecurity - ENISA, and other relevant bodies. In doing so, the said Regulation will make sure that Europeans can trust the AI they are using and – at the same time - will be key to building an ecosytem of excellence in AI and strengthening the EU's ability to compete globally.

In the context of the OVERWATCH project, further evolutions of said regulation and related normative fram will be moritored and, if relevant, presented in the upcoming issue of the present deliverable.

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 through the use 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 tend to appear in the within the privacy- aware management of location information (e.g. drone multimedia information), providing safeguards for location privacy of on-site units against vulnerabilities for abuse. Taking as an example the location privacy, the drone location information is mandatory for the operability of the OVERWATCH service but, on the other hand, it should be disclosed with care 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 starting phases 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 to avoid the possibility that other third parties can learn an individual 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)[6] [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 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

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

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 goal of privacy by design is to prevent data privacy breaches and protect the privacy of individuals by default, by proactively incorporating data privacy safeguards into systems and processes[7]. In the context of OVERWATCH, it is the approach utilised for both the development of the platfom and the 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
1	Proactive not reactive; Preventativenot remedial	PbD anticipates and prevents privacy invasive events beforethey happen.

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

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 3-1 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 approach for data privacy and protection which follows the guidelines of Privacy-By-Design methodologies provided by the GDPR.This standard methodology, compliant with ISO 27005 [RD17], allows analysing the risk posed to privacy by the processing of personal data.

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.

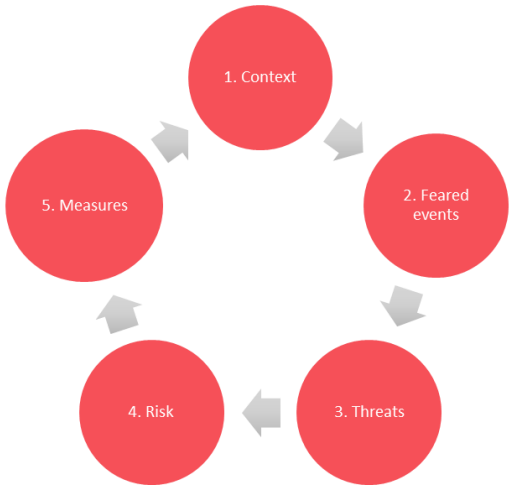

Figure 3-1 The five phases of the EBIOS Privacy By Design methodology

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 have restricted access permissions and anonymised information, whenever possible and if applicable. Therefore, it is fundamental in this context to devise data management mechanism that will ensure privacy and the non-disclosure of sensible 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.

Besides the idenfitied 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. The terms of reference will be developed and provided with Issue 2 of the present deliverable.

3.3 Ethical requirements and considerations

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. Certainly, OVERWATCH research involves voluntary participation of adults as research subjects, and hence a complete ethics self-assessment has been carried out in order to ensure that the proposal is compliant with applicable international, EU and national law. OVERWATCH designed solution will imply the collection and 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 an 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, Ethics and Security Manager 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, 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 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]). The management of such data will be regulated by a clear Term of Services, which must be read and accepted by all users, and which will follow the EU GDPR. 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 managed in strict accordance with EU GDPR, independently from the country where the data is generated, and OVERWATCH's Ethics and Security Manager will follow the procedures and make sure all the legislations are respected.

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 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (and subsequent modifications and supplements) 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	YES

anonymously? If that is not possible, will the research procedures guarantee that information will remain confidential?	
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.

3.3.3.1 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

mode8 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.

Nevertheless, should said regulatiorns be updated and, hence, new arrangements are required, the OVERWATCH consortium will make sure to be fully compliant to the updated regulatory framework.

3.3.3.2 Code of ethical conduct

The major ethical issue involves informed consent, confidentiality and OVERWATCH partner' access to sensitive material of persons and institutes/ organizations. The most essential safeguard is informed consent, including the Pilots and the participation in interviews and workshops/events of the project. The informed consent form for OVERWATCH is presented in Annex.

A basic principle in most, if not all, science is that the research and the participation must do no harm to the participants. This is often easy to understand and possible to imagine.

But the second most basic principle is that the research and the investigation must also do some good, and this is not only in some general sense, as a contribution to science and humanity, but also in the very specific case of a particular individual. This is often a neglected aspect, but in order to be an ethical researcher the researcher must also take this into consideration.

To this end, the OVERWATCH 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 GDPR (Regulation (EU) 2016/679, with regard to the processing of personal data [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 are in place. 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 to 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

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

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 sensible information that needs to be accessed by 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, sensible information will be treated differently for 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.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 to external users, such as web, mail, or FTP servers[9]. 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

[9] 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.

	provided information (e.g., this can be done via chatbot). 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 sensible 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 sensible 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 sensible 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 3-2 OVERWATCH primary assets description

Supporting assets

Supporting assets were identified and these could be systematically attacked by eternal/internal malicious persons/systems to attempt to 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 DPO, 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 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. According to the EU GPDR, log audits must be collected and stored for a period of 1 year.

Table 3-3 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 3-4 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 3-5 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 3-6 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 from outside OVERWATCH consortium	• Software function creep • Hardware function creep (e.g., storage) • Phishing, man-in-the-middle attack	3. Significant	3. Significant	3. Significant

	• 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 • Acquisition of data sent over a Wi-Fi network, etc.	3. Significant	3. Significant	3. Significant

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 3-7 OVERWATCH likelihood matrix for feared events

3.4.2.1 Risk level analysis

The security of data is of outmost importance as it is directly correlated to data privacy and protection. In this direction, the assessment on 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.

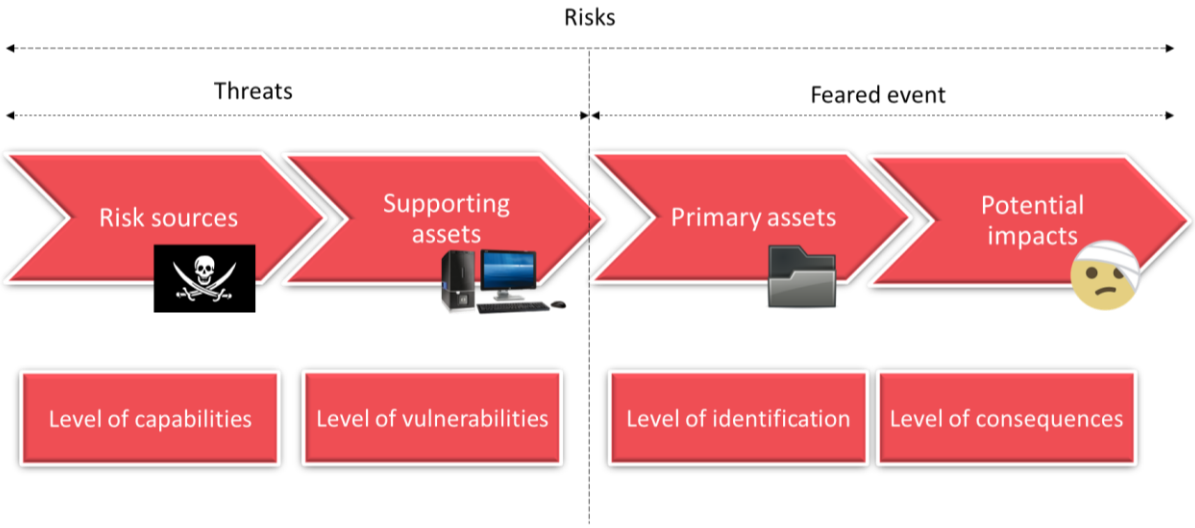

Figure 3-2 Risk components

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 the likelihood is equal to the likelihood value of the threats associated with the feared event. 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 3-8 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).

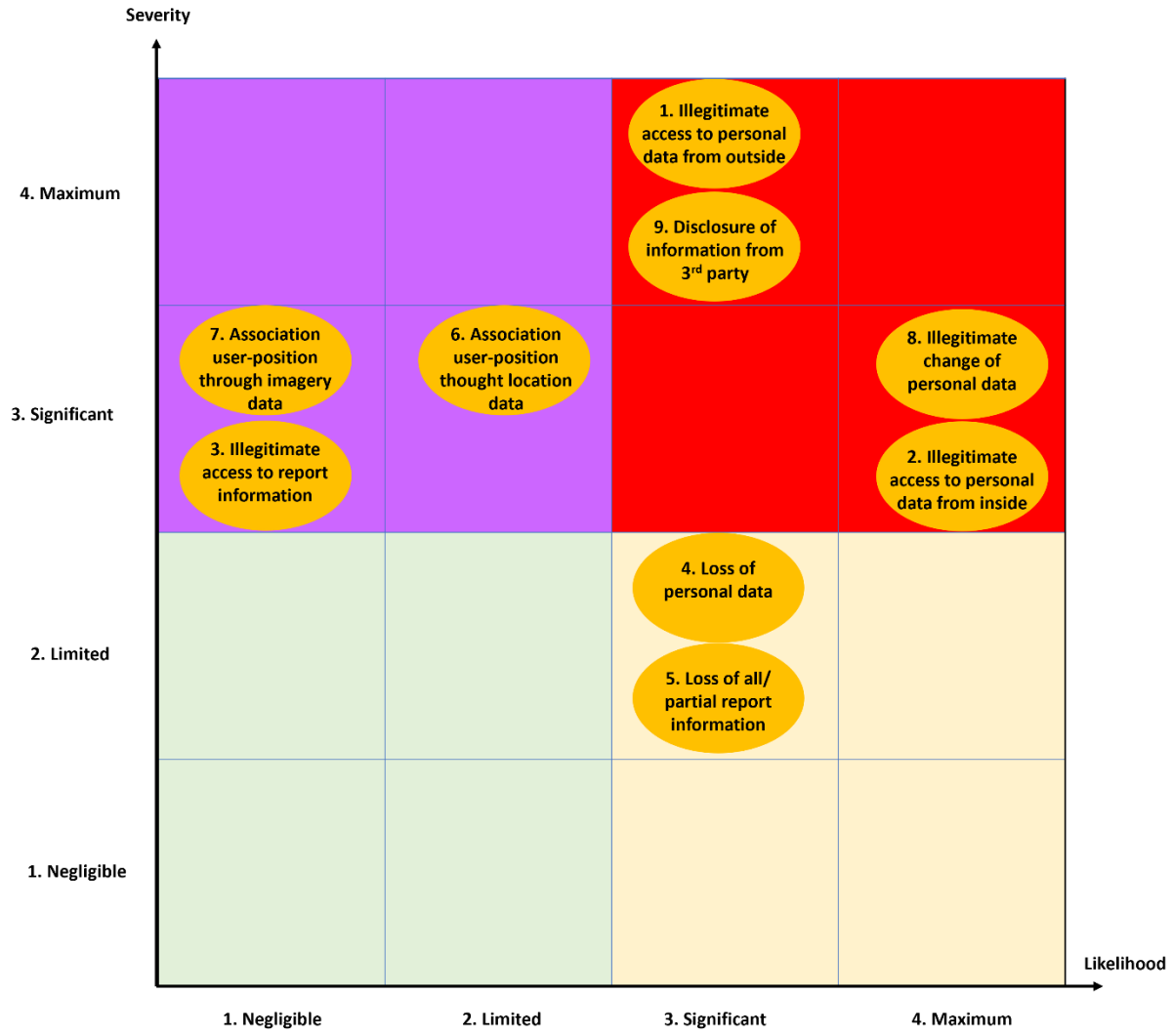

Figure 3-3 OVERWATCH risk map

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.

In the following sections, a list of Privacy-Enhancing Technologies (PETs) is provided that will be included in the design of the OVERWATCH system in order to enhance data protection and mitigate users' privacy risks.

3.4.2.2 Measures on primary assets

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 reports locations. User' personal data will be never displayed in the graphical interface, where the reportswill be associated only with the user type (professional).
Data anonymization and pseudo-anonymization	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 3-9 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. Following the recommendations of the GDPR, a Data Protection Officer will be

	appointed to direct and oversee all data protection activities. In OVERWATCH this figure is comprised in the Ethics and Security Manager figure. The ESM devises the policies and procedures that bring the organisation into compliance with the Regulation, monitors the implementation of those policies, ensures that all staff are fully trained in regard 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 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 3-11 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. According to the EU GPDR, log audits must be collected and stored for a period of 1 year.

Table 3-10 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 3-11 Selected risk-treatment measures

Coming to the results of this first 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.

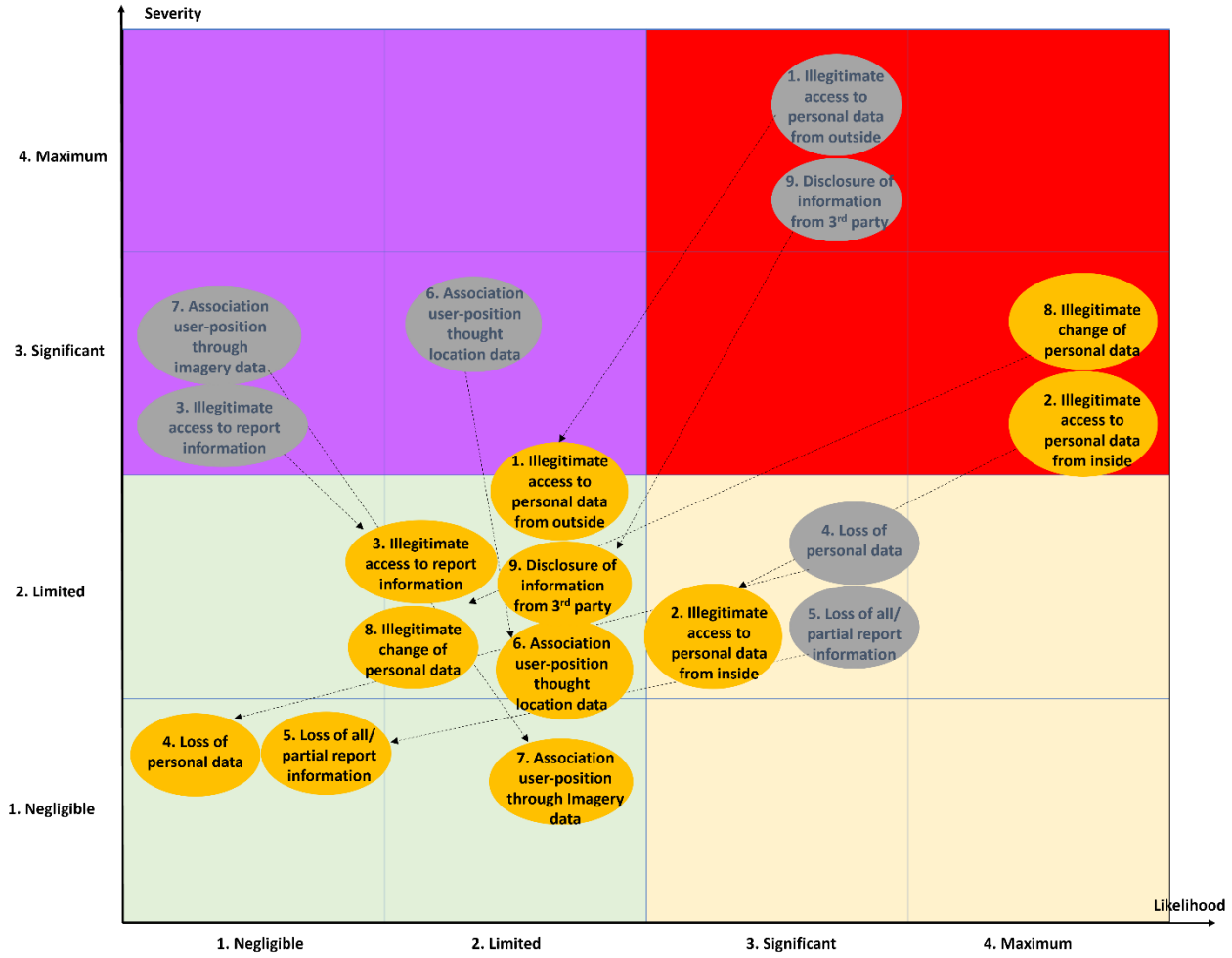

Figure 3-4 Residual risk map for OVERWATCH

So far, all identified risks are under control and possible actions are being implemented in order to minimise the impact of such risks. Moreover, it it is worth noting that all the above mentioned risks will be monitored and updated throughout the duration of the project.

4 Conclusions

The present “Privacy, Ethics and Security Report” document is the first issue of the deliverable and reports a detailed analysis of privacy, ethics and security requirements for OVERWATCH.

In particular, as seen, privacy and data protection issues together with ethics and security issues may potentially affect the OVERWATCH system at the level of primary assets (data) and supporting assets (Software and hardware architecture).

A clear methodology based on the EBIOS approach has been identified to support the project during the whole system design phase of the OVERWATCH platform. The described methodology is fully compliant to the directive of the General Data Protection Directive (GDPR) and the fundamental principles of Privacy-by- Design.

It is worth to be noted that the present analysis has been performed at very early stage of the project execution, advising on a set of countermeasures for privacy risk mitigation that should be applied on the entire system implementation. For this reason, a key factor for the success of this methodology would be to iterate this process in order to have a constant check over the validity of the proposed Privacy- by-Design approach, in anticipation of any possible changes in the system design driven by technical or architectural needs and/or choices.

At this stage, no major issues are present, especially in relation to the privacy and ethics requirements. For what concerns specifically the security requirements, so far, all identified risks are under control and possible actions are being implemented in order to minimise the impact of such risks. Moreover, it it is worth noting that all the above mentioned risks will be monitored and updated throughout the duration of the project.

Finally, a new update is expected (Issue 2) by M36 and will present revised information, in view of the evolution of the OVERWATCH project.

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

Annex

Informed consent Templates

These templates were developed and designed in order to be adapted to best serve the occasion of the OVERWATCH event and/or workshops. Every time a partner decides to host an event/workshop it fills in the highlighted yellow parts tailoring to the scope of the event itself.

Informed Consent Model for OVERWATCH workshops

This general informed consent model is designed to support OVERWATCH researchers in the deployment of an informed consent procedure that intends to comply with the ethical standards acknowledged by the European Commission in Horizon Europe projects regarding research with human participants when inviting them to participate in a OVERWATCH WORKSHOP, which may imply participation in several activities (surveys, interviews, focus groups).

The template is designed for the participation of adults (18 years old or more) able to give consent and will have to be adapted if the participation or younger people and/or vulnerable groups is sought, both in terms of "H" and "POPD".

Support of ethics experts and data protection officers or legal departments must in any case be sought to adapt the model to the specific cases and to legal and organizational compliance with applicable data protection laws and policies.

INFORMED CONSENT

Project Acronym	OVERWATCH
Project Name	Integrated holographic management map for safety and crisis events
Grant Agreement no.	101082320
Start date of the project	01.11.2022
End date of the project	31.10.2025
Financed by	EUROPEAN COMMISSION - EUSPA
Programme	Horizon Europe
Website	www.overwatchproject.eu

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

INTRODUCTION

You have been invited to participate in the [NAME WORKSHOP] of the OVERWATCH project.
The Workshop aims at providing different stakeholders the possibility of participating in the OVERWATCH project by bringing together the scientific community, emergency managers, civil protection and first responders. The OVERWATCH project is funded by the EU and has the objective to develop an integrated holographic management system for response, recovery and mitigation of emergencies and disasters, by enabling the authorities to quickly deploy and manage air, water and ground assets and personnel through decision support tools integrated in an immersive and

decentralized command platform. This system will be supported by combining several services already offered by EGNSS and Copernicus Emergency Management and Security (for example and HAS and SAR) with digital technologies, artificial intelligence, drones, 5G, augmented reality which will provide the required performance to make this system a valuable resource for emergency practitioners.

The Workshop is part of the definition of the OVERWATCH user requirements and has the objective of identifying the main top-down user requirements, taking stock of existing frameworks dealing with multi-hazard contexts for Disaster Risk Management.
Before deciding on participation, please read this document carefully. The document is divided in three sections:

1. **Project Information Sheet**, including the information about the aims of the project, the scope and terms of your participation, the general privacy policy regarding your personal data and the organisation responsible and contact researcher(s).
2. **Complete Privacy Policy Information,** regarding the details of the processing of your personal data.
3. **Informed Consent Form,** to consent on participation and on the processing of your personal data under the above conditions if you wish to participate.

Please read the document and ask any questions you may have to be completely sure to understand all the proceedings and implications of your participation.

INFORMATION SHEET

Always review and adapt information in this document to assure that it is written in language and terms that can be fully understood by participants.

PURPOSE

Participation in the [NAME WORKSHOP] of the OVERWATCH project. The Workshop is part of the OVERWATCH (Integrated holographic management map for safety and crisis events) project (www.overwatchproject.eu), funded by the European Commission/ EUSPA, and running from 01/11/2022 to 31/10/2025.

Short summary of the project's objectives: OVERWATCH aims to develop an integrated holographic management system for response, recovery and mitigation of emergencies and disasters, by enabling the authorities to quickly deploy and manage air, water and ground assets and personnel through decision support tools integrated in an immersive and decentralized command platform. All the developments of the project will be demonstrated with in-field events in Portugal and in Poland. You will find complete and updated information about the project in www.overwatchproject.eu

Purpose of the WORKSHOP: The workshop is structured upon an interactive framework in which international organizations, national governments, local governments, emergency managers, technical experts will interplay with OVERWATCH project partners to provide substantial feedback on the user requirements through stocktaking and discussing of existing frameworks dealing with multi-hazards contexts for disaster risk management. The feedback will guide all OVERWATCH developments and will overcome potential regulatory, economic and technical barriers.

Scope and terms of your participation: If you wish to participate, you will be invited to respond to a **questionnaire and participate in focus groups** in the course of the Workshop. The foreseen location of the activities is [include location].

Participation in all WORKSHOP activities will be entirely voluntary.

The information obtained in these activities will be processed and studied and integrated in the project conclusions, including scientific publications and public reports that will be available in the project website (www.overwatchproject.eu). The information will be separated from your personal data, and processed to be aggregated and anonymised: i.e. It will not include any personal data that could lead to identifying you, your personal details or your opinions or any other person. The information will normally be captured by written, however, some activities may require audio recording, which will always be transcribed before processing. Once transcribed, the recording will be deleted.

The information will be stored in the OVERWATCH project archive hosted in the data platform of the project and managed by a Data Management Plan by the Data Manager of the project Mr Federico Monteforte (ITHACA) with guarantee of compliancy from the Ethics and Security Manager, Ms Elizabeth A. Nerantzis (ALPHA).

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

Your role is crucial since you will contribute to complete the user requirements; produce the set of requirements for OVERWATCH developments and their integration with internationally recognized resources and tools.

No particular risks, discomforts or disadvantages are foreseen for participants in principle. However, in case you experience any negative effect of your participation, please contact the responsible researches detailed here below.

Your participation is entirely voluntary, and you can decide to withdraw your participation at any moment you would like to, without any consequence at all.

The project study is expected to conclude by October 2025. Personal data will be held for a period of no longer than 4 years after the completion of the OVERWATCH project. [*Date of the expected approval of the final reports of the project where the deliverables related to the study will be approved by the EC/EUSPA].*

PRIVACY POLICY:

Your personal data (basic contact data) will be processed by [*NOTE: insert name of partner who will collect and manage the personal contact data*] only for the purposes of conducting the [NAME WORKSHOP] within OVERWATCH project and will not be disclosed to any external sources.

In case that you are asked in the course of any activity (e.g. an interview) about demographic parameters such as your age range, gender, educational background or job type, such data will be stored separately from your contact data. Information recording methodologies in activities have been designed to avoid or minimize the reception of incidental personal data. In addition, all information will be processed to anonymise (by erasing, pseudonimising, fictionalisating or generalising) any incidental indirect personal identifier registered during the activity (e.g. your work place and position or any incidental identifier of a third person named in the course of a conversation) before using it for the research.

Video-recordings and photographs taken during meetings, photo sessions and interviews may be published on the OVERWATCH and the partners' web sites, **only if you have expressly agreed in the form below (see point 3.).**

Data will be used in accordance with the EU General Data Protection Regulation (GDPR) and [*NOTE: INSERT NATIONAL LEGISLATION OF THE PARTNER IN CHARGE OF COLLECTING DATA*], both available at [INSERT LINK].

You have the right to request access, modification and cancellation of your data, as foreseen by the GDPR.
Complete Privacy Policy Information is available here [INSERT LINK] and will be handed to you with a leaflet you may consult at any time.

CONTACT PERSONS FOR QUESTIONS OR CLARIFICATIONS:

[*NOTE: insert name of partner who will collect and manage the personal contact data data*] is the organisation responsible of the [NAME WORKSHOP].

The contact researcher(s) you can contact regarding your participation:

1. [researcher Name & surname] via email [xxxxx@YYYY.ZZZ]
2. [researcher Name & surname] via email [xxxxx@YYYY.ZZZ]

COMPLETE PRIVACY POLICY INFORMATION

[*NOTE: insert complete privacy policy information from the partner that will collect and manage the personal data, according to its organisational procedures, the GDPR standards and the applicable legislation: applicable international, EU and national law (in particular, the GDPR, national data protection laws and other relevant legislation). When necessary, please adapt the short «Privacy Policy » notice in the previous section].*

INFORMED CONSENT FORM

[*NOTE: the consent form has to be inserted at the end of the information documents (Information sheet and Complete Privacy Policy Information) and kept together. It is necessary to keep the 3 sections together to be able to demonstrate that the consent has been given in relation to the specific information provided in the 2 preceding sections. Participants must receive the information on their participation in the project and at least the short notice on Privacy policy. The complete privacy policy information should be made available to participants both in paper and in electronic form (e.g. via a link).*

Consequently, at least the Information Sheet must include a reference (version XXX, date XXX) matching the version referenced here below in the consent box.

A copy of the documentation should be given to the participant.]

CONSENT FOR THE VOLUNTARY PARTICIPATION IN THE PROJECT

I am 18 years or older and I am competent to provide consent	☐
I confirm that I have been fully informed about the aims and purposes and conditions my participation in the [NAME WORKSHOP] within the OVERWATCH project and I have read and understood the Information Sheet (version XXX, date XXX). I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.	☐
I understand that there is no compulsion to participate and that, if I choose to participate, I may at any stage withdraw my participation.	☐
I agree to participate in the [NAME WORKSHOP] within the OVERWATCH project.	☐

CONSENT FOR THE PROCESSING OF PERSONAL DATA

I declare that I have read and understood the information on data protection and that I have been able to solve any doubts with the help of the OVERWATCH team, who has provided all the explanations I have requested.	☐
I give my consent to the processing of my personal data as explained in the privacy information, in relation to my involvement in the OVERWATCH project.	☐
I agree that my image and voice may be recorded in the OVERWATCH project videos (e.g. at meetings, workshops, interviews, etc.) and that such videos be published on the project's and on the partners' websites.	☐

Name	Date	Signature
…… ……	…… ……	…… ……

Information sheet – Alternative for 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

Ethics and Security Manager
Name: Elizabeth A. Nerantzis
Email: en@alphacons.eu

Post Address: ITHACA S.r.l.
via P.C. Boggio 6, 10138 Torino (TO) - Italy

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.