TeamAware

TEAM AWARENESS ENHANCED WITH ARTIFICIAL INTELLIGENCE AND AUGMENTED REALITY

Deliverable D2.5

Legal and Ethical Principles and Guidelines

Editor(s):	Gemma Galdon Clavell, Nour Salih, Marta Burgos
Responsible Partner:	Eticas Research and Innovation
Status-Version:	Draft / Final – v1.0
Date:	31/01/2022
Distribution level (CO, PU):	Public

Project Number:	GA 101019808
Project Title:	TeamAware

Title of Deliverable:	Legal and Ethical Principles and Guidelines
Due Date of Delivery to the EC:	07/03/2022

Workpackage responsible for the Deliverable:	WP2
Editor(s):	Eticas Research and Innovation
Contributor(s):	Johanniter, SIMAVI, CERTH/ITI, THALES, FRAUNHOFER, AVISA, DUNE, AIT
Reviewer(s):	All partners
Approved by:	All Partners
Recommended/mandatory readers:	WP2-WP14

Abstract:	Legal state-of-the-art around events, risks and threats affecting first responders, including data protection and security requirements for the TeamAware system.
Keyword List:	Ethics, data privacy, right to privacy, fundamental rights.
Licensing information:	The document itself is delivered for the European Commission being public.
Disclaimer	This deliverable reflects only the author's views and the Commission is not responsible for any use that may be made of the information contained therein

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	**Modified by**
v0.1	02/11/2021	First draft version	ERI
v0.2	25/01/2022	Comments from Johanniter	ERI
v0.3	27/01/2022	Formatting and partner contributions	ERI
V0.4	27/01/2022	Last edits and submission	ERI
V1.0	07/03/2022	Version submitted	SIMAVI

Table of Contents

List of Figures

List of Tables

Terms and abbreviations

AB	Advisory board
ADS	Acoustic Detection System
AMS	activity monitoring system
AR	Augmented Reality
AVS	acoustic vector sensors
CCTV	Closed circuit television
CDS	Chemical Detection System
CFR	Charter of Fundamental Rights
CICIS	Citizen Involvement and City Integration System
COILS	continuous outdoor/indoor localisation system
D	Deliverable
DMP	Data Management Plan
DPM	Data Management Plan
DPO	Data protection officer
EC	European Commission
EU	European Union
GA	Grant Agreement
GDPR	General Data Protection Regulation
GDPR	General Data Protection Regulation
IMS	Infrastructure Monitoring System
LEA	Law enforcement agent
M	Month
NGO	Non-governmental organization
TMS	Team Monitoring System
UAV	Unmanned aerial vehicle
USAR	Urban Search and Rescue
VSAS	Visual scene analysis system
WP	Work Package

Executive Summary

TeamAware is a research and development project lasting 36 months and is developed by 24 partners from 13 European countries. The TeamAware project seeks to enhance crisis management, flexibility, and reaction capability of first responders from different sectors through real-time, fused, refined, and manageable information by using highly standardized augmented reality and mobile human machine interfaces.

The TeamAware project is divided into fifteen Work Packages (WPs). This document constitutes the Deliverable 2.5 “Legal and Ethical Principles and Guidelines”.

The main objective of this deliverable is to establish the ethical and legal principles that will be followed throughout the different stages of the TeamAware project. For this purpose, an analysis of the main legislation in relation to data rights and privacy and fundamental rights has been carried out, also taking into consideration the possible participation of vulnerable populations in the drills. The deliverable is structured as follows: An overview and systems developed in TEAMAWARE, the EU legal framework concerning TEAMAWARE design and implementation, and overview of the principles of INSARAG guidelines aimed at First Responders, Research considerations and Conclusions.

1 Introduction

This deliverable lays out the necessary legal and ethical guidelines to follow for TeamAware. It also provides more fleshed out details of topics touched in previous submitted deliverables (D15.3) for ethical requirements in WP15 such as consent, basis for processing, third countries, data protection and human rights. It will discuss in detail the legal framework under which partners will be collecting and processing data, especially personal data.

The deliverable is structured as follows: An overview and systems developed in TEAMAWARE, the EU legal framework concerning TEAMAWARE design and implementation, and overview of the principles of INSARAG guidelines aimed at First Responders, Research considerations and Conclusions.

2 TeamAware Overview and systems

The events, dangers, and threats that affect first responder teams are divided into two categories by TeamAware: surrounding and in-team situational awareness. TeamAware's situational awareness focuses on events, hazards, and threats that surround first responders, such as injured persons, victims, building risks, fire, smog, hazardous chemicals, biological toxins, radiation-leakage, explosion, and so on. TeamAware focuses on the location, vital status, and body posture of first responders for in-team situational awareness. Furthermore, the TeamAware solution will be created by combining the in-depth experience of field first responders.

The design of TeamAware, as shown in Figure 1, is based on the operational and strategic idea, needs, and use-cases determined with the help of first responders.

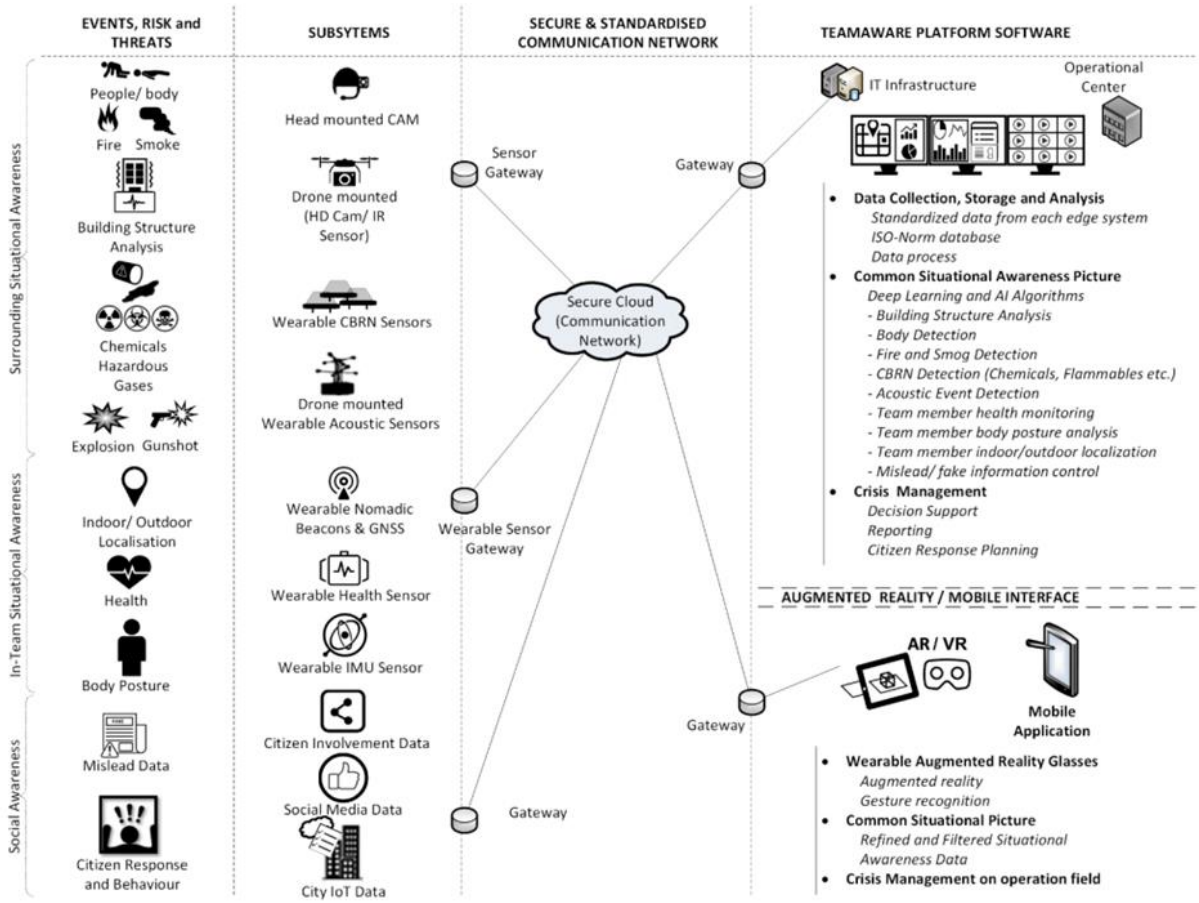

Figure 1 TeamAware Design

Surrounding situational awareness: there are numerous types of sensor subsystems that can identify multiple dangers and hazards surrounding the responder team in the context of surrounding situational awareness. Depending on the use-cases, surrounding situational awareness **subsystems will be wearable, portable, or drone-borne.** They'll use available network or portable gateways to connect to the cloud based TeamAware platform.

Head-mounted cameras, drone-borne HD cameras, and infrared (IR) sensors will be used to **identify and detect injured persons, victims, fire, smog, and building damage.** While **head mounted cameras** will be utilized to analyse the incident from a place where first responders can safely function, **drone-borne cameras** will be used to analyse occurrences in areas where first responder teams are unable to reach owing to obstructions, fire, and other factors. Along with the head-mounted and drone-borne cameras, TeamAware will be able to communicate with the current and available **indoor and outdoor IP CCTVs** in the vicinity of the incident. The victims will be identified using a **visual scene analysis system (VSAS)**, which will also detect anomalies such as smoke, fire, and anomalous heating. Images and videos taken by drone mounted cameras and head mounted cameras will be used to monitor infrastructure: **Infrastructure Monitoring System (IMS)**. IMS will be used to recognize and detect ruin and building damage, as well as identify rubble, conduct energy asset inspections, and assess building risk.

There will also be a **wearable chemical detection system (CDS)** with chemical dispersion model and decision assistance that can function in cooperative and independent modes. The chemical sensors will be worn by first responders to monitor air quality and potential hazards such as dangerous gases, explosions, and so on. In more detail, quantum dot inks are used to print sensors in fabrics as wearable sensors that provide an optical signal when chemical agents are present. CDS will be used to detect air quality, oxygen levels, hazardous gases (ammonia, chlorine, hydrogen cyanide, phosphine, and sulphur dioxide), and flammable gases (ammonia, chlorine, hydrogen cyanide, phosphine, and sulphur dioxide). In addition, CDS will give chemical intensity and a chemical dispersion map.

An **acoustic detection system (ADS)** will be used as an extra subsystem to identify and locate explosions or gunshots near first responders. In the operations, ADS will identify and locate explosions, gunshots, and snipers, as well as human sounds and whistles.

In-team situational awareness: The continuous outdoor/indoor localisation system (COILS), as well as health and body posture monitoring subsystems, will make up the in-team situational awareness system. The in-team situational awareness system will be a wearable system with wearable gateways connecting it to the cloud-based TeamAware platform. Taking into account that the in–team situational awareness will connect with the cloud, cybersecurity measures will be considered in order to protect the localisation data.

During operations, a fully integrated real-time indoor/outdoor localisation system is necessary to locate responders in hazardous and dangerous situations. Indoor, underground, and, in general, in all locations where GNSS is unavailable, unreliable, or intermittent, GNSS receivers will be used, while wireless beacons, RF transceivers, and inertial measurement units (together with innovative multisensory fusion techniques) will be used. Health monitoring and body motion capturing devices will also be part of the **activity monitoring system (AMS).** The first responders' vital signals will be monitored by the health monitoring subsystem. Body motion capture will track a first responder's location and orientation in order to detect action such as standing motionless, moving, holding a hose, or lying on the ground. The **team monitoring system** will be built by COILS and AMS (TMS).

Citizen involvement and a city integration system will form the basis of the social situational awareness system (CICIS). To inform first responders, CICIS will use citizen answers from the event scene, social media data, and data from city IoT devices. In the current era, social media is a popular means of

disseminating information; hence, it is feasible to receive up-to-date and mainly trustworthy information from social media (supported by scene photos, videos, and various user statements). It is critical to ensure citizens' security and safety at the scene of an event; as a result, citizen response planning and behavioural analysis of citizens in the event of an incident will be examined in CICIS.

Communication Network: In terms of system compatibility, the TeamAware platform will integrate each system. On a message communication bus, standardisation and communication mechanisms for data collecting from diverse sensors will be defined. This protocol will be compatible with both 5G and ad-hoc sensor networks, as well as adaptable to new network types, allowing for the integration of new sensor systems. The TeamAware system solution will allow interconnectivity and interoperability of operation centres. Smart sensor systems and user interfaces supplemented with augmented/virtual/mixed reality data will require real-time data workflow management and real-time communication, which will be provided by a network solution. Wearable gateways with secure connections will send the data acquired from diverse sources to the cloud. The network architecture will be scalable and optimized to connect a variety of wearable, portable, and drone-borne sensors of various sorts and numbers. In fact, a disaster might bring the communication infrastructure to a halt. As a result, the communication network solution will be redundant and versatile, allowing it to connect subsystems to the secure cloud using both 5G and ad-hoc mesh networks. As a result, each sensor system's bandwidth will be adaptable to network capacity by switching to low resolution (critical data) mode.

TeamAware Platform Software: The data received from multiple sensor systems will be analysed in order to monitor and manage the first responder's surroundings as well as their activity. To connect measurements and data from diverse sources, the software will use sensor fusion supplemented with artificial intelligence, notably deep-learning algorithms. The "Common Situational Awareness Picture" will be generated by the information fusion stage. This information will be used by the responders for situational awareness and decision-making. In addition, first responders will be able to manage events and processes, assign assignments to other guards and agencies, and do basic information management system functions. Even if the infrastructure fails, the TeamAware platform will continue to run as a cloud service. Data collection, storage, and analysis, internet of things (IoT), sensor network administration, map, decision support, and decision-making software will all be available on the TeamAware platform. The software will create a "Common Situational Awareness" image that includes the following elements:

- **Surrounding situational awareness:** Body and victim detection, fire and smoke detection, infrastructure and building damages monitoring, air quality monitoring, chemical detection, explosions and gunshot detection
- **In-team situational awareness:** Indoor/ outdoor localisation, vital signal monitoring, body motion analysis
- **Social situational awareness:** Citizen sourced data, social media sourced and validated data, city IoT sensors

TeamAware Human Machine Interfaces (HMI): The "Common Situational Awareness Picture" will be presented to operators in the central office as well as responders in the field via the TeamAware platform's operation center. In depth, the dense data will be processed and filtered to provide clear and manageable data that will be displayed on the user interface. The displays will use an augmented

reality/mobile interface to create a user experience that is both intelligible and standard (ISO 9241). Because there are various and heterogeneous data sources deployed in the field, the user interface will present a dynamic option, allowing operators to select the right data for the right application by integrating disparate sources. In a restricted setting, it will be critical to develop a system that can operate in low-quality transmission or even in a disconnected state.

2.1 Data life cycles of systems and WPs

2.1.1 WP1 Project Management and Coordination

The first work package of TeamAware holds all the administrative and organizational tasks and deliverables for the project to develop as necessary. It holds all information on all partners, including data related to mailing lists, contact information, roles and responsibilities, etc. All the information created and used for this WP will follow DMP guidelines for data life cycle management as established already in D1.3 'Data Management Plan v1'.

2.1.2 WP2 System Architecture Specification and Design

Information for WP2 will be updated in D1.7 'Legal, Ethical and Societal Issues Handbook v2' to be delivered in month 30.

2.1.3 WP3 Visual Scene Analysis System

The main objective of Visual Scene Analysis System (VSAS) is to provide vision-based solutions that will help First Responders (FRs) before or during their interventions. The VSAS provides vision-based solutions that will be deployed on two different subsystems: the "head mounted camera" subsystem (called the "helmet" subsystem) and the "UAV mounted camera" subsystem (called the "UAV payload" subsystem). These subsystems will be linked through dedicated radios to a ground subsystem acting as a gateway.

The basic technical functionalities of the VSAS are presented in the table below. A part of them will be embedded on the helmet subsystem or on the UAV subsystem and will target several scenarios as synthesized here:

Table 1 Basic technical functionalities, subsystems, and targeted scenarios

Basic technical functionalities	Subsystem			Typical scenario(s)
	Helmet	UAV	On ground	
Localisation in GNSS-denied environments	X	X		FRs localisation to get a good situation awareness, FRs guidance
Piloting assistance		X		Building exploration to collect information, to detect victims…
Semantic mapping	(X)	(X)	X	Building exploration to collect information, to detect victims, to help for FRs deployment…
Victim detection and localisation	(X)	(X)	X	Indoor victims rescue

Software systems: Data analytic is performed to detect and localise victims to improve the rescue operations. The VSAS system will be also used to locate the LEA agent during the operations. Other softwares (i.e., semantic mapping) concern the detection of relevant environmental information suitable to organise the rescue operations.

Data Cycle for software development and deployment purposes

- **Data collection**: Data that will be collected can be divided into non-personal data and personal data. Non-personal data are photos and videos that reveal information about shape, colour, decoration of the environment and existing datasets used to train the vision algorithms. Further, the pilot development includes a preliminary step which implies the collection of **video/images** that could have personal information. In this case the aim is to make, where possible, the personal data anonymous, such that it cannot be related to an identifiable legal person. This data will be collected, used, and stored for the development of the VSAS with the purpose to train suitable algorithms (i.e., the ones listed in Table1). The data will represent 1-10 individuals involved in the TeamAware project and it may reveal some personal data (i.e., face imagery), without the aim to identify legal persons. Informed consent will be signed by individuals involved in the personal data collection from the TeamAware project in order to protect their privacy.

  The not-anonymised data used for the training part will be stored on a dedicated server (dedicated PC) for the whole project duration and destroyed after the project duration.

- **Data Cycle in the Analytics**
  1. **Data understanding** — This phase includes exploratory data analysis that allows to figure out which subsets are useful for the modelling and which hypothesis have to be explored.
  2. **Data preparation** — This can be considered to be the most time-consuming phase as it involves rigorous data cleaning and pre-processing as well as the handling of missing data.
  3. **Modelling** — The pre-processed data are used for model building in which learning algorithms are used to perform the analysis.
  4. **Evaluation** — In performing the 4 aforementioned steps, it is important to evaluate the results and review the process performed to determine whether the originally set of objectives (KPIs, technical performances etc..) are met or not. If deemed appropriate, some steps may need to be performed again. Rinse and repeat. Additionally, in this evaluation phase, some findings may ignite new project ideas for which to explore.
  5. **Deployment** — Once the model is of satisfactory quality, the model is then deployed. In the operational phase, the camera images are not going to be stored and a particular attention will be paid to the actual flows of these data in order to protect the privacy (the characteristics of the network and authentication procedures are currently under definition on WP9). Especially considering the fact that a part of the footprints (restricted to the not embedded analytic see "Table 1 – on the ground functionalities") are going to be combined and exchanged locally on the TeamAware platform/network, that could introduce the risk of unauthorised collection of data.

For the embedded functionalities (Table 1) on Drone and UAV, data is only kept during runtime, and thus disappears on power-off.

2.1.4 WP4 Infrastructure Monitoring System

Information for WP4 will be updated in D1.7 'Legal, Ethical and Societal Issues Handbook v2' to be delivered in month 30.

2.1.5 WP5 Chemical Detection System

Information for WP5 will be updated in D1.7 'Legal, Ethical and Societal Issues Handbook v2' to be delivered in month 30.

2.1.6 WP6 Acoustic Detection System

This work package is related to the development of an acoustic detection system capable of recognizing sounds such as gunshots, explosions and human screams.

The data collection will be conducted under the premises of CERTH/ITI. In particular, data related to human speech (e.g., screams and shouts) will be collected and the following researchers will participate in the data collection:

- Theoktisti Marinopoulou
- Anastasios Vafeiadis
- Antonios Lalas

Speech recognition will not be performed. On the contrary, the magnitude spectrogram representations of the screams or the word "help" will be extracted and fingerprinting will be performed for the audio-based event detection.

Regarding the acoustic data from explosions and gunshots, **public datasets will be used.** More specifically, the MIVIA Audio Events Dataset and the UrbanSound8K will be used for the event of a gunshot. Sound events from explosions will be extracted from the AudioSet dataset. AudioSet is made available by Google Inc. under a Creative Commons Attribution 4.0 International (CC BY 4.0) license. The UrbanSound8K dataset is offered free of charge for non-commercial use only under the terms of the Creative Commons Attribution Non-commercial License (by-nc), version 3.0: http://creativecommons.org/licenses/by-nc/3.0/. Finally, part of the MIVIA Audio Events Dataset,, which will be used for the TeamAware project, is licensed under the CC BY license (CC BY 4.0).

Additionally, two public datasets will be used to test the performance of the algorithm of sound event localization (direction of arrival, azimuth and elevation). The TAU-NIGENS Spatial Sound Events 2021 that is available under the Creative Commons Attribution Non-commercial 4.0 International and the DREGON dataset that is publicly available for personal, educational and academic use only.

In the case where the on-board first-person view camera will be used to extract features of the detected objects and set bounding boxes of the target, the video feed will be available only via the local Wi-Fi network that is established by the DJI Matrice 200 v2 drone. Events such as the shouts for help can be detected via a person waving their hands. Events such as gunshots could also be detected via the body pose of a person carrying a gun. During the data collection, all the

videos will be stored locally on computers at the CERTH premises; a blur effect will be applied to the faces of the participants and finally, at the classification stage only integer values of the body pose will be used to detect the event. In the case of the "explosion" class the FLAME dataset will be used that is licensed under the Creative Commons Attribution.

Following the data lifecycle management, as depicted in Figure 1, all the acoustic data will be stored in the internal storage of the single-board computer (SBC) that will be used for the deployment of the algorithms. In particular, a Raspberry Pi 4 SBC and two microphone arrays, namely ReSpeaker Mic Array v2.0 and MATRIX Creator, will be used for the creation of the dataset. In the case where the 32 GB of the SBC internal storage will not be enough, the dataset will be stored in a network drive that can be accessed only by the users involved in the TeamAware project and from the CERTH premises. As part of the audio data might contain speech signals, all the wav recordings will be pseudo-labelled. The spectrogram features (either as PNG files or NumPy arrays) will be extracted from the raw audio recordings to train the algorithms. The dataset will not be shared publicly. It could be available to an internal partner (e.g., MicroFlown for the completion of WP6) of the project after a request. All the raw audio recordings will be archived after the end of the project and destroyed after 5 years based on the current GDPR.

During inference, only stream packets of audio (numerical arrays with amplitude information) will be processed in real-time. In the case where a cloud connection is needed to communicate with the TeamAware platform, a text file containing all the metadata (timestamps with audio event detected, azimuth, elevation, and direction of arrival) will be sent.

The data collection with the array of acoustic vector sensors (AVS) will be performed either in the company or for gunshot or explosion detection (if it's needed) in a military training ground close to AVISA, where such events take place every day. In AVISA, we have some datasets on incoming small arms fire and blasts/ explosions that can be used for initial tests by CERTH. If we need to capture new datasets, we go to the military training ground and we will deploy our array on the ground or on a drone and record the data. Since we are designing and developing an array of AVS to be used in the ADS system in WP6, some data captures would be used for design and development of the prototype array by AVISA. Besides, some other data recording will be arranged using the prototype array according to the requirements of algorithm development and the captured data would be used by CERTH for the algorithm development and required analysis in the process of the ADS development.

For data collection of explosions and gunshots using the array of AVS in AVISA, some data can be captured using one or more loudspeakers that play the explosion or gunshot sounds (from audio files in the public data sets used by CERTH). The array can be also installed on a drone hovering/flying in one of the rooms in our company while the audio files will be played from the loudspeaker on the ground in different places. The drone equipped with the prototype array can be used for recording the data in a military training ground if it's needed. The array would be covered by a properly designed wind cap for data captures outdoors. In all these tests, the audio files will be recorded on a memory on the drone or on a laptop and later, the data will be used for analysis and processing required in the TeamAware project.

People who will involve in the data captures from AVISA will be:

- Edwin Jansen

- Michael Maassen

Figure 2 Data life cycle

2.1.7 WP7 Team Monitoring System

The WP7 includes the use (joint or separate) of the COILS (continuous outdoor indoor localisation system) and the AMS (activity monitoring system); therefore, the following sections will separately deal with them.

The fundamental framework of the data collection in the WP7 of TeamAware can be split into the basic tasks in which the project can be in contact with humans and their personal data, as defined by the Regulation (EU) 2016/679.

COILS: personal data management

As stated in GA, on the one hand TeamAware needs the involvement of humans for the system on-field demonstrations; on the other hand, it is of paramount importance to stress that for the development and test of the WP7-COILS, no personal information about the humans directly involved in the trials will be ever asked, gathered, recorded, and stored in any phase relevant to the demonstration activities. Indeed, the individuals involved in the on-field demonstrations will be personnel belonging to the end-users' organisations partners in TeamAware and DUNE has and will not have any direct relationship with their personal (identifiable) data, both in the development phase and in the testing/demonstration phase of the COILS. Before, during and after the execution of the trials, the DUNE personnel will never collect any information about the involved people.

From a technical point of view, in a multi-user scenario, each human involved will be equipped with a system (the COILS system) that will automatically associate (with no interaction with other people and no personal data collection) each user with a Bluetooth address string (e.g., "C6:76:99:B4:77:08") that is the identifier of the device. The data elaborated by the COILS (i.e., the geo-location of the device worn by the user) are sent to the Incident Command System as strings of positions associated to the aforesaid Bluetooth address, with no relationship with any personal data of the user wearing the said device. Paradoxically the COILS system cannot

distinguish between a COILS equipped by a human or a by a dog. It is worth stressing that any association between the provided Bluetooth string and the real personal data of the operator wearing the system could (and probably will) be performed at the Incident Command System side, but such an association is performed by other TeamAware systems, well outside the COILS.

In addition, the use of the COILS does not need any videorecording or photos of the participating individuals; therefore such information will not be collected (by the WP7-COILS activities) before, during or after the on-field demonstrations. Should third parties (e.g., the cooperating Organisations themselves) perform such or similar activities, they will do it outside the scope of the COILS activities, with no liability of DUNE about the possible infringement of the privacy of the participating individuals.

AMS: personal data management

Data lifecycle can be evaluated in two different collections of AMS data. One of them is the previously collected anonymous/simulated (synthetic) health and posture data to be used to train neural networks –which will be stored for unlimited time since it does not contain any personal information and will be either collected from a large number of unknown (anonymous) users or synthetic data.

The second of them is collected during operation (Figure 1), which is the online representation of rescuers' postures and anomalies within them. This data can be paired with the rescuer's sensor set ID since it is important to know which user (to be called with ID) is hurt or has an anomaly during the operation. This data can be either deleted after a while (<5 years) or after the operation duration (to be used in training phase, possibly) and stored.

Figure 2 shows the data lifecycle of the AMS, orange boxes show the path of previously collected training data, green boxes show the path of the data collected during the operation (contains ID of set) and blue boxes show the common process for both data.

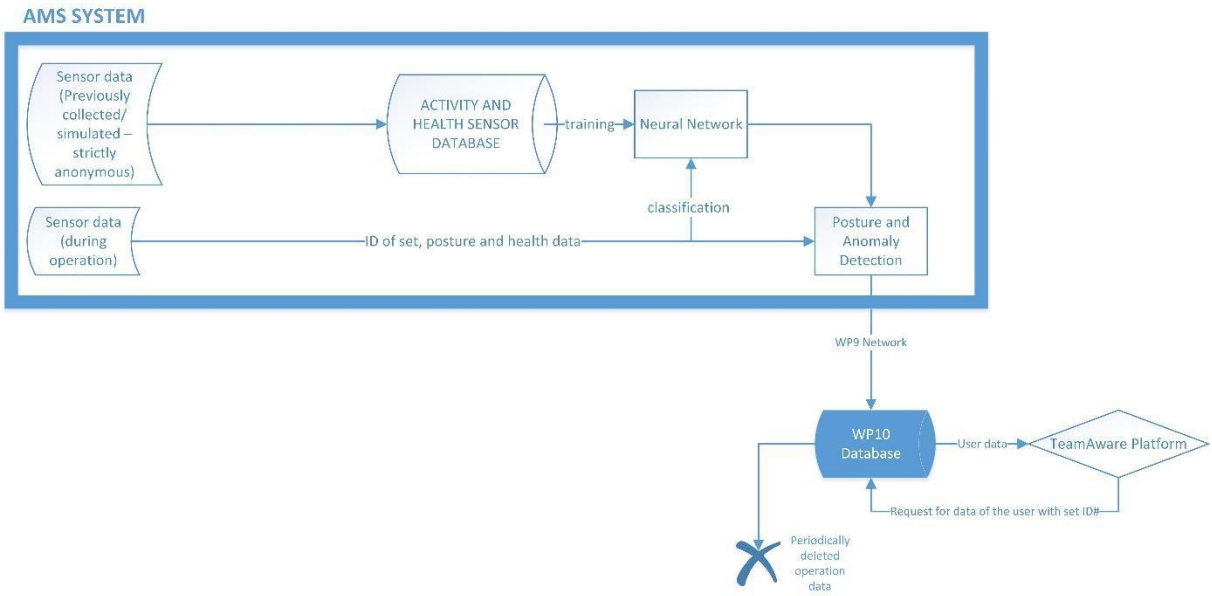

Figure 3 AMS system data and process flow

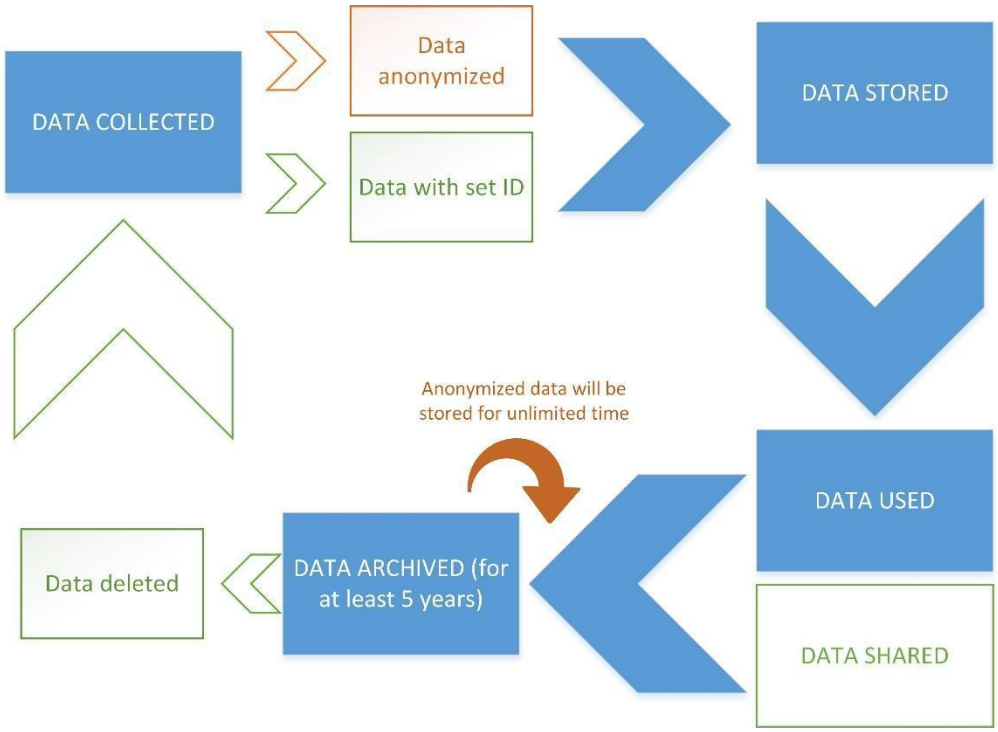

Figure 4 AMS system data lifecycle

2.1.8 WP8 Citizen Involvement and City Integration System

Information for WP8 will be updated in D1.7 'Legal, Ethical and Societal Issues Handbook v2' to be delivered in month 30.

2.1.9 WP9 Secure and Standardised Communication Network & WP10 TeamAware AI Platform Software

WP9 will be centered around the interoperability services among Operation Centres which will be developed, connection with existing first responder operation centres, secure and cloud-based communication channels and a network architecture design which will be scalable and optimised to connect different types and numbers of wearable, portable, and drone-borne sensors. While WP10 will mainly implement the software architecture designed in WP2 and subsequently work very closely with WP9 to deploy the associated technologies and interfaces provided. For this they will need to catalogue and organise all the georeferenced and heterogeneous data from various information systems to provide decision support for responders, disaster managers and coordinating bodies and provide stakeholders with end-user friendly risk warning mechanisms and risk mitigation strategies.

In WP9 "collection/creation" of data happens outside WP9, except for the user accounts that are handled in the "identity and access management" component, all other data is generated by WPs where systems are being developed. Once WP9 receives information from other WPs the data is stored in the data storage layer of the interoperable architecture which will allow dynamic

integration of the assets into the system. Similarly, the data analytics layer of the architecture is where the data will serve its main purpose, especially in line with WP10 data fusion. While within the interoperable architecture sharing happens on several layers: “manage dispatching”, “cross-centre message exchange” and “sensor gateways”.

When it comes to archiving and destroying there is nothing specified yet, however WP9 is studying the use of the data storage layer as a possible solution for archiving. As far as destroying data there are no protocols in place yet at this early stage but requirements are being considered to end up with a design that explicitly states where and how long certain data is allowed to be stored/archived or to which extent the data transferred is considered privacy relevant.

It is also important to consider that Interoperability services are “using” the data in a way, what they do is to transform the data from one format to another and send it to the next stage. They have no way of identifying what the data is and they do not store it. Virtualization and deployment is where all of this takes place.

For WP10, led by Fraunhofer, where the implementation on knowledge from the previous WPs will come the data life cycle can be explained as follows:

- **Creation or detection of data**
  - Within WP10, we have 2 kinds of Data in regards of data creation
    - **Sensor Data:** This Data will be created by the sensor in previous WPs and then sent to WP10. We have no control over the creation of this data, WP10 will simply use the incoming data.
    - **Fused Data[1]:** This Data is created within WP10 by fusing the incoming sensor data to create new data points for higher information gain.

- **Storage**
  - WP10 stores all the data which is created either by WP10 itself or any of the connected sensor systems. This might include personal data if it is either gathered by sensors in any way or generated by the data fusion.

- **Use**
  - The collected data is used within WP10 for further computational purposes as well as display purposes for operational team members. This might include personal data if it is either gathered by sensors in any way or generated by the data fusion.

- **Sharing**

[1] For the fused data, there is a possibility that this data might contain personal information about the first responders integrated within the TeamAware system. This will become clearer as the development of systems advances and any relevant information will be updated accordingly in D1.7.

- The data is shared within the whole TeamAware system. This might include personal data if it is either gathered by sensors in any way or generated by the data fusion.

- **Archiving**
  - By direct end-user request, the accumulated data can be archived completely as a file. WP10 does not provide any functionality to automatically archive the data over a prolonged period of time.
  - The life span of the data within the WP10 system is limited to the deployment scenario. As soon as the scenario ends, the user has the opportunity to store the data in a file.

- **Destroying**
  - The WP10 system will delete the stored data after the scenario has been ended by the user.

2.1.10 WP11 TeamAware AR/Mobile Interfaces

Information for WP11 will be updated in D1.7 'Legal, Ethical and Societal Issues Handbook v2' to be delivered in month 30.

2.1.11 WP12 Integration and Test

WP12 does not foresee any data handling issues that will be different from what the systems will have already specified before integration and testing of the platform begins. WP12 will not interfere in sub-systems data life cycles.

2.1.12 WP13 Demonstration and Validation

Information for WP13 will be updated in D1.7 'Legal, Ethical and Societal Issues Handbook v2' to be delivered in month 30.

2.1.13 WP14 Dissemination, Exploitation and Communication

Information for WP14 will be updated in D1.7 'Legal, Ethical and Societal Issues Handbook v2' to be delivered in month 30.

2.1.14 WP15 Ethics requirements

WP15 does not process any personal information as it consists of delivering a series of ethical requirements to the commission. Nevertheless, it will follow internal DMP processes and any due action will be taken regarding storage, archiving and deletion.

3 EU Legal framework concerning TeamAware design and implementation

TeamAware protocols and methods will be heavily geared at strengthening and improving first responder awareness communication and knowledge systems during crisis and emergency management. These toolkits are specifically designed to satisfy the interests and needs of cops, medical personnel, and emergency responders who are the first to respond in an emergency. However, as stated in the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union (2016/C 202/02), the data transfers that this entails must be particularly respectful of fundamental rights to privacy and personal data protection.

To begin, the European Union's Charter of Basic Rights recognizes personal data protection as a fundamental right in Article 8 (Title II: Freedoms), as well as the right to respect for private and family life in Article 7.

Users of the TeamAware tool kits must be able to exercise these rights in relation to the data they share with the system under these coordinates. The importance of the right to non-discrimination is emphasized in the European Union's Charter of Fundamental Rights (CFR), the European Convention on Human Rights, and the Universal Declaration of Human Rights. Many of the possible collectives employing TeamAware toolkits, including persons with disabilities, may face discrimination as a result of their features.

Vulnerable populations include the elderly, pregnant women, juveniles, children, people with disabilities, migrants and displaced persons and religious minorities, all of whom are protected by international human rights accords.

The right to the integrity of the person (Article 3 CFR) is another right to consider within TeamAware, as the usage and administration of TeamAware technologies and suggestions might have an impact on users' physical and mental well-being. This problem necessitates that IT administrators raise user knowledge of these dangers. Furthermore, the rights to liberty and security are framed in Article 6 CFR, which can be affected by the usage of TeamAware if its technologies are misused. It should also be taken into account that TeamAware has potential implications in terms of the freedom of expression and information (Art 11 CFR) and the right to environmental protection (Art 37 CFR).

Furthermore, documents such as the European Union's Charter of Fundamental Rights, the European Convention on Human Rights, and the Universal Declaration of Human Rights demand specific public protection and ensure that disadvantaged social groups are treated equally. Among these precautions, public institutions should take the lead in involving marginalized groups based on their socioeconomic or cultural circumstances. TeamAware will answer to these demands in the field of first responders by developing particular guidelines for vulnerable groups, should they be considered an affected group, which will introduce new mechanisms for ensuring their active inclusion and equal security standards with individuals who do not belong to these groups. TeamAware must, however, pay close attention to how the toolkits integrate specific technologies and procedures for such purposes without exposing these social groups to new hazards.

3.1 Human Rights

Right to integrity

Because of the nature of live-action field exercises, the right to integrity, as described below, is relevant when considering that the field exercises carried out within TeamAware will expose research participants to conditions that may have a negative impact on their bodily and mental integrity:

Charter of Fundamental Rights of the European Union

Article 3:

1. Everyone has the right to respect for his or her physical and mental integrity.

    a. In the fields of medicine and biology, the following must be respected in particular:
    b. the free and informed consent of the person concerned, according to the procedures laid down by law;
    c. the prohibition of eugenic practices, in particular those aiming at the selection of persons;
    d. the prohibition on making the human body and its parts as such a source of financial gain;
    e. the prohibition of the reproductive cloning of human beings.

The relevance of human rights is highlighted within TeamAware due to the presence of persons from vulnerable groups. Because of their vulnerability, these people require particular attention and care in order for their human rights to be respected. Along these lines, D1.3 (Data Management Plan) and the ethical requirement deliverables from WP15 are targeted at putting in place mechanisms to ensure that their involvement in TeamAware's research activities does not jeopardize their human rights protection. This involves specific environmental and safety considerations, which will be represented in the aforementioned deliverables and monitored by ETICAS as fieldwork activities progress.

Right to privacy

The following definitions from several international instruments are relevant to properly comprehend what the right to privacy comprises and how TeamAware's research efforts may affect it:

Universal Declaration of Human Rights. **Article 12:**
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks

The right to privacy is a conditional right, which means that it can be violated for valid reasons and in a proportional manner. In the second paragraph of the European Convention on Human Rights, this is hinted at. As a result, TeamAware shall handle the personal data of research participants in a proportional manner and in accordance with data protection laws.

Charter of Fundamental Rights of the European Union.
Article 7:
Everyone has the right to respect for his or her private and family life, home and communications.
Article 8:
1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of 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. 3. Compliance with these rules shall be subject to control by an independent authority.

If not extensively discussed in this area, the right to personal data protection is also worth highlighting. This article emphasizes the idea of purpose limitation as well as two of the European Union's data protection rights, namely the right of access and correction. The General Data Protection Regulation, which is the EU's principal regulatory framework on the subject, explains the right to data protection in depth.

European Convention on Human Rights.
Article 8:
1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Additionally, the consortium has recognized non-discrimination as a core objective in TeamAware when it comes to the handling of personal data of study participants who belong to vulnerable groups of the population. Different international legal documents have defined the right to non-discrimination in the following ways:

Charter of Fundamental Rights of the European Union.
Article 21. Non-discrimination:
1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. 2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.

European Convention on Human Rights **Article 14. Prohibition of discrimination:**
The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.
Article 1. General prohibition of discrimination (Protocol No. 12):
1. The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. 2. No one shall be discriminated against by any public authority on any ground such as those mentioned in paragraph.

Universal Declaration of Human Rights **Article 7:**
All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

This project has carefully analysed all the possible consequences of the processing of sensitive information for members of the aforementioned collectives. In fact, one of the project's main goals is to give practitioners useful insight into how to cope with vulnerable persons in the event of an emergency. The recommendations in this deliverable will help to avoid any potential discriminatory treatment during the research.

Among the vulnerable groups slated to participate in the field drills there are expected to be disabled some individuals considered part of the elderly group. Prior to that, however, it is vital to analyse how vulnerable groups are legally classified in order to provide some solid criteria for categorizing people. De facto, however, certain vulnerable groups, such as children or people with a certain disability, cannot participate in the simulation, because it must always be given that the person frees themselves in an emergency.

Members of religious minorities

It's difficult to discover a legal definition of what constitutes a religious minority, most likely due to the difficulties of defining such a term.

The Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities

Article 1
1.States shall protect the existence and the national or ethnic, cultural, religious and linguistic identity of minorities within their respective territories and shall encourage conditions for the promotion of that identity. 2. States shall adopt appropriate legislative and other measures to achieve those ends.
Article 2
1. Persons belonging to national or ethnic, religious and linguistic minorities (hereinafter referred to as persons belonging to minorities) have the right to enjoy their own culture, to profess and practise their own religion, and to use their own language, in private and in public, freely and without interference or any form of discrimination.

Because international law lacks a clear definition of what constitutes a religious minority, we can state that for the purposes of TeamAware, religious minorities are individuals who practice a faith other than the majority of the population of the country in question. Religious minorities, as stated in the above Declaration, have the freedom to practice their religion and participate in society without being discriminated against. As a result, TeamAware will need to make sure that this is the case and make an effort to incorporate these considerations into the project's toolkits and outcomes.

The elderly

Charter of Fundamental Rights of the European Union **Article 25**
The Union recognises and respects the rights of the elderly to lead a life of dignity and independence and to participate in social and cultural life.

Even though there is no legal definition of "elderly," Eurostat considers those above the age of 65 to be elderly. The TeamAware project will follow a similar path.

One of the key goals of TeamAware is to build response procedures that take into account the requirements of vulnerable individuals, hence the confluence of TeamAware and human rights is particularly essential. Not only must research activities be carried out in a manner that ensures that these are respected, but the project's deliverables (including the many toolkits generated as part of it) must also ensure that vulnerable people's rights are protected whenever it is relevant for the system or subsystem.

In line with this, the Recommendation No R (87) 21 of the Committee of Ministers to Member States on Assistance to Victims and the Prevention of Victimisation establishes the following:

Paragraph 4:
"ensure that victims and their families, especially those who are most vulnerable, receive in particular [...]emergency help to meet immediate needs [...]"

When it comes to vulnerable groups, TeamAware takes two approaches to guaranteeing their human rights. To begin with, the TeamAware toolkits are designed to improve the efficiency of first-responder actions during emergency situations involving these groups. Second, this deliverable and all WP15 deliverables will contribute to put in place safeguards to ensure that their participation in TeamAware's research activities is in accordance with human rights.

3.2 Data protection

This section will define and analyse key data protection regulations in order to frame their consequences for TeamAware's design and deployment. The focus of the investigation is on the GDPR, which reflects the most recent data protection standard and covers TeamAware's main requirements for lawfully processing personal data.

Articles 2 and 3 of the GDPR respectively establish the material and territorial scopes of the regulation.

The General Data Protection Regulation (EU GDPR)

Article 2

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:
   a) in the course of an activity which falls outside the scope of Union law;
   b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;
   c) by a natural person in the course of a purely personal or household activity;
   d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. 2Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

The TeamAware collaboration is made up of organizations based largely in European Union or European Economic Area (EEA) nations that will process personal data belonging to data subjects based in those areas for research purposes. The exception to that are Sabanci University (SU), Havelsan Hava Elektronik Sanayi Ve Ticaret (HAVELSAN), Ambulance and Emergency Physicians Association (AAHD), SRDC Yazilim Arastirma Ve Gelistirme Ve Danosmanlik Ticaret Anomin sirketi (SRDC) and Bursa Buyuksehir Belediyesi (BBB), five partners that are based in Turkey, a country that is not currently a member of the European Union. Nonetheless, because the personal data it may process as part of TeamAware belongs to data subjects whose data is being monitored for research purposes within the Union, even these partners must comply with the GDPR (Article 3.2). Furthermore, the joint controller's agreement requires this partner to achieve the minimum requirements set forth in it, ensuring a minimum level of compliance.

In light of these considerations, the GDPR, as well as its national implementation in the various member states, is the primary applicable legislation in terms of personal data.

Personal data

As previously stated, the protection of personal data is regarded as a basic right in the European Union, with the GDPR serving as the primary legal foundation. Given that TeamAware processes personal data, this right must be defined. To begin with, personal data is defined as follows in article 4:

The General Data Protection Regulation (EU GDPR)

Article 4 (1):

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Data subjects are natural persons to whom data can be attributed and who are the subjects of the GDPR's data protection rights. For the legal examination of TeamAware's outcomes and research method, correctly determining what data are personal data for data subjects is critical. Any information that identifies or allows for the identification of natural persons is considered personal data. The GDPR provides a few examples but does not provide a complete list. This is because even data that appears to be unproblematic in terms of data privacy has been shown to allow for the identification of persons (Narayanan and Shmatikov, 2008).

The TeamAware consortium will be processing mainly data coming from:

- Representatives and contact points from members of the AB's.
- Research participants involved in the field exercises carried out within the project, some of them belonging to vulnerable categories of the population.
- Databases publicly available whenever possible.
- Data generated during testing such as environmental and structural shapes, colors, decorations, etc.

Table 2 Data collected in TeamAware

WP	Type of data	Partner responsible
WP1	Personal contact information	SIMAVI
WP3	video/images that could have personal information (ie. identifying facial or body features)	THALES
WP6	Audio files with human voices	AVISA
WP7	Health and posture data	DUNE
WP8	Twitter usernames, geolocation markers, descriptive information regarding situations or people	INNOVA
WP13	Personal data for demonstrations	RAN
WP14	Personal contact information	JOAFG

There are a lot of techniques to protect data in order to reduce the risks associated with managing the above data, such as the danger of misuse. One of these is pseudonymization, which is defined under the GDPR as:

Article 4(5):

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person

Pseudonymisation ensures that a database can re-identify an individual with less information about them. Depending on the database's criticality, this technical method of data protection may be sufficient. It is important to note, however, that pseudonymized data is still personal data and is subject to the GDPR.

The GDPR, on the other hand, does not regard anonymized data to be personal data. It is defined as follows:

Recital 26:

> [...] The principles of data protection should therefore 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. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Anonymisation entails modifying a personal data dataset in such a way that it is theoretically impossible to re-identify individuals. A dataset can be altered in a variety of ways, including grouping persons based on common qualities, eliminating fields, replacing fields with false data that is comparable, making the data less exact, and so on. Anonymisation must be separated from pseudonymisation, with the key difference being the inability to re-identify someone.

The technical and organizational mechanisms used to protect data subjects' and study participants' rights and freedoms are discussed in D1.3 (Data Management Plan v1). This process is particularly significant because it involves changes in the legal status of data (Recital 26 GDPR), but it is also one of the most important security measures for sensitive data that TeamAware and its data life cycle must carry out. Furthermore, with the exception of prior approval obtained via the use of informed consent, it is necessary to anonymize personal information before disclosing it to other parties.

Each member of the consortium that must adopt anonymisation and pseudonymisation measures has been tasked with implementing such measures and will share finalized details that will be reflected in D1.8 (Data Management Plan v2).

Special categories of data

As previously stated, some of TeamAware's activities necessitate the processing of sensitive personal data. Article 9.1 GDPR defines the categories of personal data that are considered sensitive:

> **Article 9.1**
>
> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

However, data belonging to the sensitive categories established in Article 9.1 GDPR can be processed in cases where the conditions established in Article 9.2 apply:

> **Article 9.2:**
>
> 2. Paragraph 1 shall not apply if one of the following applies:
>
> a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
>
> b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social

protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject;

f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

In light of these observations, the processing of sensitive personal data is not forbidden, but it is subject to additional precautions. In all circumstances, sensitive data utilized for research reasons will be treated with informed consent in TeamAware. Furthermore, according to Article 9.2 g) GDPR, this sort of

processing must be "proportionate to the goal sought, respect the essence of the right to data protection, and provide for appropriate and particular safeguards to safeguard the data subject's fundamental rights and interests." In summary, the TeamAware project's management of special categories of data must be based on one of the aforementioned requirements, and their controllers/processors must implement special security measures for their treatment, which may include anonymization, encryption, strong user authentication, backup solutions, or data erasure.

It is unclear at this stage of the project what is all the sensitive data that will be collected since there may be new information brought up as the systems develop. However, we can give an overview of the known sensitive data that will be collected so far.

Table 3 Sensitive data in TeamAware

WP	Type of sensitive personal data	Partner responsible for collection	Partners with which data will be shared	Purpose for data processing	Basis for processing
WP3	Biometric data	THALES	TREE, EUCENTRE	The biometric data, although not used for identification purposes, will be processed in order to provide First responders with information otherwise not available about possible victims in an emergency site.	Legitimate interest
WP7	Health data	DUNE	HAVELSAN	This data will provide vital information on First Responders who may be injured or in a life threatening situation.	Consent

The purpose for which these data are gathered is especially important, especially in terms of adhering to the principle of data minimisation, which requires controllers to only collect the minimum amount of personal data required to achieve their goals. In this vein, determining the aim for collecting and processing all forms of data collected within the project to guarantee that no additional personal data is collected and processed is especially crucial when dealing with personal data belonging to special

categories. Moreover, TeamAware partners will use publicly available data whenever possible as a risk mitigation measure.

Roles involving personal data

It is indeed critical to understand the roles and duties of the various players in the GDPR as well as the TeamAware project.

In data operations involving personal data, the data controller plays a critical role because it is the entity that bears much of the responsibility for what happens to that data. A controller is defined in Article 4(7):

Article 4(7):
'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
Article 24:
1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 24 still does not provide a full description of the controller's responsibilities. Also significant are the following:

Transparent information, communication, and modalities for the exercise of the rights of the data subject (Article 12 GDPR);

Data protection by design and by default (Article 25 GDPR);

Obligation to only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject (Article 28 GDPR);

- Records of processing activities (Article 30 GDPR);
- Security of processing (Article 32 GDPR);
- Notification of a personal data breach to the supervisory authority (Article 33 GDPR);
- Communication of a personal data breach to the data subject (Article 34 GDPR);
- Data protection impact assessment (Article 35 GDPR);
- Prior consultation (Article 36);
- Designation of the data protection officer (Article 37 GDPR);

- Transfers subject to appropriate safeguards (Article 46)

The requirement to preserve records of processing activities is not always applicable. Article 5 of the GDPR outlines the following scenarios in which the requirement to retain records will apply:

> *The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.*

As a result, at the very least, the partners who will process personal data from special categories will be required to preserve records of the processing activities involving special categories data..

The repercussions of not adhering to the controller regulations are outlined in Articles 82 to 84. Data subjects who have had their data protection rights violated as a result of the controller's failure to comply have the right to compensation. In addition, administrative fines and penalties may be imposed for infractions of the regulation.

The controller isn't always the only one who handles personal information. Personal data can also be processed on behalf of the controller by other companies. Processors are what they're called, and they're defined as follows:

Article 4(8):
'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
Article 28.2:
The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
Article 28.3:
Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.
Article 29:
The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.
Article 30.2:
Each processor and, where applicable, the processor's representative shall maintain a record of all categories

of processing activities carried out on behalf of a controller, containing:
a. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
b. the categories of processing carried out on behalf of each controller;
c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
d. where possible, a general description of the technical and organisational security measures referred to in Article 32(1)

The articles above define the major responsibilities of data processors. In general, data processors are responsible for assisting the controller in complying with the GDPR, including not processing data for purposes or in ways other than those specified by the controller, keeping records of their processing activities, and generally abiding by the terms agreed upon with the controller.

According to article 37.1 of the GDPR, in certain instances involving the processing of a certain amount of personal data or where the processing is carried out by a specific type of entity, the entity must appoint a Data Protection Officer (DPO):

Article 37.1:

The controller and the processor shall designate a data protection officer in any case where:

a. The controller and the processor shall designate a data protection officer in any case where:

b. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

c. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

d. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Article 39:

1. The data protection officer shall have at least the following tasks:

    a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

    b. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of

personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

d. to cooperate with the supervisory authority;

e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

As part of the TeamAware data governance, the consortium had established in the GA that controllers would be appointed for each of the participating organisations in the following manner:

To ensure compliance with national regulations, a data controller will be appointed for each participating partner, acting as an interface with the relevant Data Protection Authority when required. The partners in charge of exercises that will be developed in Turkey and Romania in which volunteers' participation is envisaged, will obtain the approval for the personal data management from their respective National Data Protection Authorities prior to the activities described in the WP.

It should be noted, however, that controllers are not a compensated position. As a result, all partners who are required to do so have selected a DPO, and those who are not required to appoint a DPO have supplied their data protection policy for the project, as specified in D15.3 (POPD - Requirement No. 3 [M5]). Each participating organization has appointed a DPO through a DPO statement. D15.3 contains a list of DPOs who have been appointed, as well as their DPO statements and contact information. The DPOs are in charge of ensuring GDPR compliance inside their organizations and assisting data subjects in exercising their data protection rights.

Legal basis of processing

Processing personal data is only lawful if it is based on one of the following justifications:

Article 6:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
   a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   b. 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;
   c. processing is necessary for compliance with a legal obligation to which the controller is subject;

d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing 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;
f. processing 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.

* Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

The GDPR emphasizes the importance of consent. Indeed, in many circumstances, personal data processing is not permitted unless consent is given; consent thus serves as the primary key to personal data processing. Because people's consent has been abused in the past, the GDPR strengthened the idea to ensure that consent is informed and explicit.

Article 4(11):

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

Article 7:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Within TeamAware, the processing of personal data will be justified solely on the basis of informed consent, which will be provided by study participants in accordance with the procedures and using the tools described in D15.1.

Informed consent sheets and forms will be critical in this regard, as they must be developed in such a way that consent is effectively given freely and informedly. To be allowed to do so, they will need to include everything listed in Article 13 of the GDPR.

Article 13

1. 1.Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
    a. the identity and the contact details of the controller and, where applicable, of the controller's representative;
    b. the contact details of the data protection officer, where applicable;
    c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
    d. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
    e. the recipients or categories of recipients of the personal data, if any;
    f. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
    a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
    b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
    c. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
    d. the right to lodge a complaint with a supervisory authority;
    e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
    f. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

Principles

The motives behind the data protection law that has proliferated in recent decades are to process personal data in a fair and respectful manner that respects the data subjects' fundamental rights. The Organization for Economic Cooperation and Development established the first ethical principles to follow

in 1980, and they have served as a foundation for subsequent legislation. These principles are also reflected in the GDPR, which includes the following:

Article 5.1 (a):
processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); Lawful processing is that which is carried out on some of the basis for processing established in Article 6.1 GDPR. As for the principles of fairness and transparency, they require that the data subject be informed of the existence of the processing operation and its purposes (see Article 60). Therefore, they have to do with informed consent.
Article 5.1 (b):
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); The principle of purpose limitation implies that data must be collected in order to fulfil certain goals. This is also related to informed consent since data subjects must be informed of the purposes for which their data are going to be processed in order for consent to be considered truly informed and lawful (see Articles 13 and 14 GDPR).
Article 5.1 (c):
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); The principle of data minimisation establishes that the data collected from data subjects must be kept to a minimum. In other words, no more data should be collected than what is strictly necessary in order to achieve the purpose of the processing.
Article 5.1 (d):
accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
Article 5.1 (e):
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

Data must be accurate and reflect reality, and it must be appraised in light of the processing's goals. The rights of the data subject, who can ask the controller to erase or amend the data it has about them, are the fundamental way in which this principle is applied in the GDPR (Articles 16 and 17 GDPR).

Personal data should not be stored for any longer than is necessary to achieve the purposes for which they were gathered in the first place, according to the principle of storage limits. The period can be extended if the data is processed for one of the purposes listed in Article 89 GDPR (public interest, scientific or historical research, or statistical purposes), which may be the case for TeamAware because raw data sets may be collected and shared with other researchers for research purposes. That does not, however, absolve the controller from implementing technical and organizational safeguards to protect the data subject's rights and freedoms.

The approved data retention time that was contained in the DMP for TeamAware was five years after the project ended. Furthermore, partners are recommended to erase data as soon as they no longer require it, in order to minimize threats to study participants' data protection rights. The storage limitation concept requires controllers to explain their data retention time based on its utility.

Article 5.1 (f):

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

The principle of accountability ensures that the GDPR's other principles have teeth by requiring those who are responsible to be held accountable if they are not compliant. The GDPR's punishments and costs (see Articles 83 and 84 GDPR) were designed to offer positive reinforcement for good behavior. The TeamAware consortium has opted to establish itself as a joint controller by signing a joint controller's agreement outlining the roles and duties of the various partners.

In terms of processors, partners are urged to only work with processors who provide adequate data protection guarantees. As stipulated by the GDPR, the relationship between a consortium member and processors must be governed by a contract.

When processing personal data, the processing entity should follow all of these principles. When building a system or service that needs the use of personal data, the GDPR requires the data controller to consider data protection by design and by default, as stated in article 25 of the GDPR.

It is worth noting that this deliverable, as well as the rest of WP15, are targeted at adhering to the principles of data protection by design and default, as they strive to raise awareness of the project's possible issues. This Deliverable also aims to address them early on in order to raise the degree of legal compliance and ethical awareness in accordance with the "data protection by design and by default" approach. This includes personal data collection limitations and a clear and accessible explanation of the goals and processes underlying the acquisition of personal data from both end-users and research participants.

Other relevant requirements in the GDPR worth noting

Security

Article 32.1:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...].

As a result, the GDPR's security approach is based on risks and current best practices. As part of the project field exercises, such an assessment will be tailored to the TEAMAWARE particular procedures and performance. In other words, the TEAMAWARE project's security measures, as well as its ethical and societal effect assessment, which analyzes legal compliance, will meet the standards of Article 32.1.

Also D15.3 "POPD- Requirements No3" provided a description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as a deliverable. This includes an opinion on whether a data protection impact assessment should be carried out under art. 35 of the General Data Protection Regulation 2016/679 or Directive 2016/680"), which are also concerned with security within TEAMAWARE. Furthermore, throughout the research, all TEAMAWARE consortium partners are committed to guaranteeing the highest security data protection requirements..

Data breaches

Article 33.1:

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Personal data breaches are defined in the GDPR as follows

Article 4 (12):

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

The GDPR does not specify any precise requirements for complying with it. Instead, it allows for a great deal of flexibility in the implementation process, allowing the rule to continue to be effective even after technical change has occurred. However, there is some legal confusion as a result of this. The GDPR, in particular, requires the data controller to assess the likelihood that a specific data breach would result in harm to natural persons' rights and freedoms. A list of negative repercussions that a personal data breach can have on individuals can be found in Recital 85 GDPR.:

Recital 85:

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Regarding controller obligations in the event of a personal data breach the GDPR establishes:

Article 33

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
    a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
    c. describe the likely consequences of the personal data breach;
    d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
    a. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
    b. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
    c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Encryption, anonymization, access control, and password protection are among the data security mechanisms in place to ensure proper data protection. TeamAware does not pose any specific security threats, as stated throughout this deliverable and in those that are more directly concerned with data protection and security.

In continuation, the GDPR mandates that the controller keep a record of any personal data breaches, including information on their consequences and the actions taken to mitigate them. If there are any personal data breaches, TeamAware will keep track of them. Furthermore, in circumstances where a personal data breach is likely to result in a high risk to natural persons' rights and freedoms, the data controller is required to notify both the supervisory authority and the data subjects affected.

Article 33.5:

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34.1:

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

It can be safely said that the TeamAware consortium will implement all required safeguards to prevent data breaches (data security) and to comply with GDPR standards in the case of a breach. If a data breach occurs, the affected consortium member must first notify SIMAVI (the coordinator), assess the likelihood of the data breach posing a potentially high risk to data subjects' rights and freedoms using the criteria

outlined in this document, and then notify the data supervisory authority and/or the affected data subject according to the terms outlined in the regulation.

DPIA (Data Protection Impact Assessment)

It has previously been established in D15.3 that at this point of the project, we do not foresee the need for a DPIA. However, this is a topic that will be addressed once it has been appropriately discussed with partners.

3.3 Rights of the data subjects

The GDPR recognizes data subjects' subjective rights, which is one of the most significant parts of the regulation. Among them:

- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restriction of processing;
- Right to be notified regarding the rectification or erasure of personal data or the restriction of processing;
- Right to data portability;
- Right to object to the processing.

These rights are outlined in Chapter III of the legislation and give data subjects more control over how their data is processed. TeamAware will ensure that these rights are implemented for study participants, consortium members, AB members, and app/toolkit users.

The primary means through which these rights will be implemented inside TeamAware is by alerting those who are affected of their existence. When personal data is gathered, data subjects must be informed of their rights. That will be the case for TeamAware, which will include pertinent information about these rights in the consent forms and information sheets created for the project's field exercises and research activities. A privacy policy will also be included in the app's privacy policy, which will include information about the data subject's data protection rights.

It is critical that consortium members receive training on how to respond to data subjects' requests and that a methodology be established for DPOs to follow. In order to address this, the following shall be considered by controllers concerning data subjects' rights.

1. The Data Controllers are each responsible for the data subjects from whom it gathers personal data, including the following responsibilities:
    a. to inform the data subject of the processing of personal data and the rights of the data subject;
    b. to ensure that the necessary authority exists for the processing of the registered data, including the obtaining of consent;
    c. that data are erased when they are no longer necessary.

2. The Data Controller who obtains specific data from sources other than the data subject is responsible for informing the data subject accordingly.
3. Each Data Controller is responsible for ensuring the rights of the data subjects in accordance with the below provisions of the GDPR:
    a. duty of disclosure when collecting personal data from the data subject;
    b. duty of disclosure if personal data are not collected from the data subject;
    c. right of access by the data subject;
    d. right to rectification;
    e. right to erasure (the right to be forgotten);
    f. right to restriction of processing;
    g. notification obligation regarding rectification or erasure of personal data or restriction of Processing;
    h. right to data portability (but not for public authorities);
    i. right to object to processing.
4. If one of the Data Controllers receives a request or inquiry from a data subject regarding matters covered by another Data Controller's responsibilities, see above, the request is forwarded to such Data Controller without undue delay.
5. The parties are responsible for assisting each other to the extent this is relevant and necessary in order for both parties to comply with their obligations to the data subjects.

Concerning individual data protection rights, the GDPR specifically states:

Article 15 (Right of access)

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
    a. the purposes of the processing;
    b. the categories of personal data concerned;
    c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
    d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
    e. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
    f. the right to lodge a complaint with a supervisory authority;
    g. where the personal data are not collected from the data subject, any available information as to their source;
    h. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 16 (Right to rectification)

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Article 17 (Right to erasure)

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
    a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
    b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
    c. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
    d. the personal data have been unlawfully processed;
    e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
    f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
    a. for exercising the right of freedom of expression and information;
    b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e. for the establishment, exercise or defence of legal claims.

Article 18 (Right to restriction of processing)

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
   a. 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;
   b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
   c. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
   d. the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
2. Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Article 19 (Notification obligation regarding rectification or erasure of personal data or restriction of processing)

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

Article 20 (Right to data portability)

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
   a. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
   b. the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Article 21 (Right to object)

1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. 4.At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

3.4 Transfer to third countries or international organisations

TeamAware presents two sets of issues regarding personal data transfers to third countries or international organisations, namely:

Five of the partner organisations (HAVELSAN, SRDC, SU, BBB, AAHD) are based in a country outside of the European Union (Turkey) and one partner is based in the UK.

In both cases, personal data transfers will be made to countries outside the European Union. The GDPR obliges controllers and processors to put in place safeguards when personal data is to be transferred outside of the European Union and the EEA (European Economic Area).

Article 44

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

And Article 45.1 states that data transfers can take place under normal circumstances if an adequacy judgment has been granted for the country to which the data will be transferred.

Article 45.1

A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

Article 45.2

When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

- the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Because the consortium includes nations that are not members of the European Union, it will maintain alternate methods for transferring personal data that are compliant with the GDPR on hand in case they are required. The following are some alternatives:

- Transfers subject to appropriate safeguards (Article 46 GDPR);
- Binding corporate rules (Article 47 GDPR);
- Derogations for specific situations (Article 49 GDPR).

The main legal precepts are the following:

Article 46:

1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided

appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
    a. a legally binding and enforceable instrument between public authorities or bodies;
    b. binding corporate rules in accordance with Article 47;
    c. standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
    d. standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
    e. an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
    f. an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
3. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
    a. contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
    b. provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.
4. The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.
5. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:
    a. are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
    b. expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
    c. fulfil the requirements laid down in paragraph 2.
2. The binding corporate rules referred to in paragraph 1 shall specify at least:
    a. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
    b. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
    c. their legally binding nature, both internally and externally;

d. the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
e. the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;
f. the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;
g. how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;
h. the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;
i. the complaint procedures;
j. the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;
k. the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
l. the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);
m. the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
n. the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).

Article 49.1

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
    a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
    b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
    c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
    d. the transfer is necessary for important reasons of public interest;
    e. the transfer is necessary for the establishment, exercise or defence of legal claims;
    f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
    g. the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

Given the above and in consideration of the specific circumstances in TeamAware, the following table establishes the different options that the consortium has in order to transfer personal data to third countries in a way that is compliant with the GDPR:

Table 4 Options for data transfer to third countries

Option	Approval of supervisory authority	Further requirements
Standard data protection clauses	No (Article 46.2)	
Contractual clauses	Yes (Article 46.3)	
Binding corporate rules	Yes (Article 47.1 and 47.2)	• All the information established in Article 47.2 GDPR must be included within the binding corporate rules.

		• A member of the consortium based in the EU would have to accept liability for data breaches caused by the one based outside of the Union.
Explicit consent/assent	No (Article 49.1.a)	• Research participants must be informed of the risks involved given the absence of adequacy decision and adequate safeguards.
Special cases (legitimate interest)	No (Article 49.1)	• The data controller must inform the supervisory authority. • Aside from the information that needs to be given to data subjects according to Articles 13 and 14, the controller will also need to inform the data subject about the transfer and the compelling interest pursued.

In addition, the controller must inform the subject of the transfer and the compelling interest pursued. The TeamAware collaboration will take a method that is appropriate for the project's requirements while also providing proper data protection. In any event, it appears that data transfers to third parties are not planned at this time.

4 INSARAG Guidelines for First Responders

Most of the First Responder teams operate under the INSARAG Guidelines. TeamAware will include the INSARAG guidelines principles into the consortium and ethical principles and guidelines in the development of the exercises.

INSARAG is a global network of more than 90 countries and organizations under the United Nations umbrella. INSARAG deals with urban search and rescue (USAR) related issues, aiming to establish minimum international standards for USAR teams and methodology for international coordination in earthquake response based on the INSARAG Guidelines. According to Volume I INSARAG Guidelines (V1) Policy in the chapter 2.4 "Values, operational, norms and humanitarian principles" INSARAG is mandated by the INSARAG Steering Group (ISG) to:

- Operate in accordance with the Humanitarian Principles, which form the core of humanitarian action.
- Render emergency preparedness and response activities more effective and thereby save more lives, reduce suffering and minimise adverse consequences.
- Improve efficiency in cooperation among international USAR Teams working in collapsed structures at a disaster site, including by managing the IEC/R process.
- Promote the strengthening of national USAR capacities and activities designed to improve search-and-rescue preparedness in disaster-prone countries, thereby prioritising developing countries, including by assisting Member States in setting up national USAR Team classification processes.
- Develop internationally accepted procedures and systems for sustained cooperation between national USAR Teams operating on the international level.
- Develop USAR procedures, guidelines and best practices, and strengthen cooperation between interested organisations during the emergency relief phase.

Principles INSARAG operates in accordance with the Humanitarian Principles, which form the core of humanitarian action being the following principles:

Adherence to common standards and methodology: Members of INSARAG commit to adhere to the INSARAG Guidelines and methodology as globally accepted and independently verifiable minimum operational standards and procedures, based upon expert knowledge and evidence-based experience. The INSARAG network continues to develop these standards and procedures though shared and continued learning.

Inclusiveness: INSARAG brings together governments, governmental organisations, NGOs and disaster preparedness and response professionals. INSARAG particularly encourages disaster-prone countries to join the network, as well as any country or organisation with USAR response capacity.

INSARAG emphasises the importance for gender awareness and considerations while working in disaster-affected areas.

Professionalism: INSARAG promotes responsible, ethical and professional standards amongst USAR Teams and stakeholders.

Respect for diversity: INSARAG acknowledges and respects USAR Teams' varied operational procedures in achieving common objectives, while disseminating principles and minimum standards agreed upon by the INSARAG network.

Cultural sensitivity: INSARAG promotes awareness and respect by international USAR Teams of cultural differences so that international USAR Teams can cooperate more effectively with national and international actors.

Needs-driven: Mobilisation and deployment of international USAR Teams is only supported when the affected country's capacities are overwhelmed by the impact of a collapsed-structure emergency and national authorities agree to accept international assistance. Moreover, the type of international assistance rendered is based on the needs of the affected country and not driven by the availability of resources.

Predictability: INSARAG promotes predictability in search and rescue response operations, both in terms of response capacities available when they are needed, as well as in terms of coordination platforms put in place to ensure a most efficient use of available assets in relation to the identified humanitarian needs.

5 Research Considerations

In the field of research, pilot development and field work, the following aspects will be taken into consideration.

Ensure that all participants have read and signed informed consents. In the case of vulnerable populations, comply with legal requirements and ensure that informed consent forms are written in understandable language.

The principles of the GDPR will be taken into consideration as it was described throughout deliverable. It is underlined that the privacy of religious or ethnic minorities will be preserved in line with their own cultural sensitivities.

Furthermore, for the completion of questionnaires for research purposes, which could be filled in online by pilot participants, or the completion of forms, secure platforms will be used to preserve data security and privacy, such as EU Survey.

Since the GA mentioned CBRNE risks, environmental principles will be considered in order to ensure that the environment of the pilot sites will be preserved.

6 Conclusions

TeamAware will at all times take into consideration the rights and legislation described throughout this deliverable at the different stages of the development process. Likewise, it will also ensure the rights of the vulnerable population that may participate in the development of the pilots planned in the AG and in the different research phases developed within the project.

The present deliverable provides sufficient legal and ethical basis to help guide consortium partners build knowledge and the TeamAware systems, not only under GDPR compliance, but also, and equally important, following the ethical principals laid out here to strengthen the systems' architecture. This ultimately provides a more rounded and well thought technology where the user and the subjects whose data is being collected have their safety and privacy put first and foremost, which results in a much more complete and safer tool.

It is also important to note that this deliverable and WP15 deliverables are setting the foundation on how to deal with humans and personal data during research activities and findings. Deliverables submitted up to date cover a range of ethical and legal research considerations when it comes to research subjects and participants covering areas such as consent, data minimization, information sheets, data breaches, security, subjects' rights, etc.

References

Operational Guidelines and Field Manual on Human Rights Protection in Situations of Natural Disaster, March 2008, available at: https://www.refworld.org/docid/49a2b8f72.html

Commission Staff Working Paper Risk Assessment and Mapping Guidelines for Disaster Management. (2009).

Charter of Fundamental Rights of the European Union. (2012).

Commission Staff Working Document EU Host Nation Support Guidelines. (2012).

Communication from the Commission - An Open and Secure Europe: making it happen. (2014).

Communication from the Commission to the Council and the European Parliament — Civil protection — State of preventive alert against possible emergencies. (2001).

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. (2010).

Directive (EU) 2016/680 — protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data. (2016).

Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. (2005).

European Convention on Human Rights. (1950).

ICO. (n.d.). Conducting privacy impact assessments code of practice. Retrieved from https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

INSARAG Guidelines (2020). Volume 1. Policy. Retrieved from https://www.insarag.org/wp-content/uploads/2021/06/INSARAG20Guidelines20Vol20I.pdf

Joint Proposal for a Council Decision on the arrangements for the implementation by the Union of the Solidarity clause. (2012).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. (2016, April 27th).

Resolution of 19 June 2008 on stepping up the Union's disaster response capacity. (2008).

Resolution of 21 September 2010 on the Commission communication: A Community approach on the prevention of natural and man-made disasters. (2010).

Resolution of the Council and of the representatives of the Governments of the Member States, meeting within the Council of 8 July 1991 on improving mutual aid between Member States in the event of natural or technological disaster. (1991).

Stockholm Programme. (2010).

TeamAware (2021). Consortium Agreement

The European Counter Terrorism Strategy. (2005).

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007. (2007).

Universal Declaration of Human Rights. (1948).

Working Group on Ethics. (2019, October 23). Informed Consent for Paediatric Clinical Trials in Europe 2015.

Working Party Article 29. (2014, May). Opinion 05/2014 on Anonymization Techniques.