ASSISTANCE

Adapted situation awareneSS tools and tailored training curricula for increaSing capabiliTies and enhANcing the proteCtion of first respondErs

European Commission

Project co-funded by the European Union within the Horizon 2020 Programme

Project Ref. N°	ASSISTANCE H2020 - 832576
Start Date / Duration	May 1, 2019 (36 months)
Dissemination Level[1]	PU (Public)
Author / Organisation	E-LEX

Deliverable D8.5

Report on data protection, privacy & ethical impact

31.08.2021

[1] PU: Public; PP: Restricted to other programme participants (including the EC services); RE: Restricted to a group specified by the Consortium (including the EC services); CO: Confidential, only for members of the Consortium (including the EC services).

ASSISTANCE

Nowadays different first responder (FR) organizations cooperate together to face large and complex disasters that in some cases can be amplified due to new threats such as climate change in case of natural disasters (e.g. larger and more frequent floods and wild fires, etc) or the increase of radicalization in case of man-made disasters (e.g. arsonists that burn European forests, terrorist attacks coordinated across multiple European cities).

The impact of large disasters like these could have disastrous consequences for the European Member States and affect social well-being on a global level. Each type of FR organization (e.g. medical emergency services, fire and rescue services, law enforcement teams, civil protection professionals, etc.) that mitigate these kinds of events are exposed to unexpected dangers and new threats that can severely affect their personal safety.

ASSISTANCE proposes a holistic solution that will adapt a well-tested situation awareness (SA) application as the core of a wider SA platform. The new ASSISTANCE platform is capable of offering different configuration modes for providing the tailored information needed by each FR organization while they work together to mitigate the disaster (e.g. real time video and resources location for firefighters, evacuation route status for emergency health services and so on).

With this solution ASSISTANCE will enhance the SA of the responding organisations during their mitigation activities through the integration of new paradigms, tools and technologies (e.g. drones/robots equipped with a range of sensors, robust communications capabilities, etc.) with the main objective of increasing both their protection and their efficiency.

ASSISTANCE will also improve the skills and capabilities of the FRs through the establishment of a European advanced training network that will provide tailored training based on new learning approaches (e.g. virtual, mixed and/or augmented reality) adapted to each type of FR organizational need and the possibility of sharing virtual training environments, exchanging experiences and actuation procedures.

ASSISTANCE is funded by the Horizon 2020 Programme of the European Commission, in the topic of Critical Infrastructure Protection, grant agreement 832576.

Disclaimer

List of Authors

Organisation	Authors
E-LEX	Giovanni Maria Riccio / Adriana Peduto / Fabiola Iraci Gambazza

Change control datasheet

Version	Changes	Chapters	Pages	Date
0.1	First draft (ToC)	E-Lex	5	30.07.2021
0.1.1	Version 0.1.1	UPVLC	24	18.08.2021
0.2	Updates after internal review	UC	24	26.08.2021
1	Final version completed	E-Lex	28	27.08.2021

Content

1. 8**2.** 8**3.**

9*3.1. The General Data protection legislation applicable to the Project* *12*

3.2. Processing of personal data in rescue operations *13*

4. 14*4.1. The structure of questionnaire* *15*

4.2. Section I of the Questionnaire *15*

4.3. Section II of the questionnaire *16*

4.3.1. Processing of data and the methodology 16

4.3.2. Category of data 18

4.3.3. Technical measures 20

4.4. Section III of the questionnaire *21*

4.4.1. The performance of the pilots 21

4.4.2. Preliminary results and final output 21

5. 21*5.1. Recommendation in the pilot scenarios* *22*

5.2. Mapping of ethical risks *24*

List of Tables

Table 1 - Ethics risk map 23

Acronyms

ASSISTANCE	Adapted situation awareneSS tools and tallored training curricula for increaSing capabiliTie and enhANcing the proteCtion of first respondErs
PC	Project Coordinator
D#.#	Deliverable number #.# (D1.1 deliverable 1 of work package 1)
DoA	Description of Action of the project
EC	European Commission
EU	European Union
GA	Grant Agreement
H2020	Horizon 2020 Programme for Research and Innovation
IPR	Intellectual Property Rights
LED	Directive (EU) 2016/680 (Law Enforcement Directive)
WP	Work Package
IPR	Intellectual Property Rights
PSC	Project Steering Committee
PIC	Project Implementation Committee
PSB	Project Security Board
AB	Advisory Board
TL	Task Leader
WPL	Work Package Leader

1. Executive Summary

This deliverable consists of a report to frame the most relevant EU legal framework and to outline some recommendations in the assessment of the impact of the rescue operations in relation to the ASSISTANCE technology on privacy and data protection. The document, starting from the analysis already proposed in the D.8.1, provides an overview on the relevant legal framework, including the General Data Protection Regulation (EU) no. 679/2016 (hereinafter: GDPR), aimed at supporting the methodology to be followed in the assessment of privacy and data protection issues involved in the rescue operations. Furthermore, this report holds recommendations for software and technology developers, in order to comply with the data protection regulations and principles, i.e. by following the privacy by design and privacy by default approaches, as well as complying with technical and organisational measures to store and protect personal data pursuant to the GDPR and the other data protection regulations.

2. Methodology

The main aim of the Deliverable 8.5. is to represent the results of the assessment of the impact of rescue operations in relation to the ASSISTANCE technology on privacy, data protection and human rights.

The pilot demonstrations of the project, simulating rescue operations, shall take place in Turkey, Spain and The Netherlands, during natural disasters or terrorist attacks, and evaluate the ASSISTANCE technologies to be used to efficiently intervene in the course of the accidents, including, for instance, drones, sensors, robots and related UAV Platforms.

The pilot scenarios in the ASSISTANCE project will involve human beings, simulating possible and real rescue operations. However, due to the pandemic caused by COVID-19, the participation of human beings has not been possible yet. Due to this issue, at the present stage, it is not possible to assess the real impact of rescue operations on privacy and data protection issues.

For the time being, in a theoretical perspective and in order to guarantee a first evaluation on the risks and impacts, the methodology followed by E-LEX will be based on:

i) an update on the general overview on the relevant legal framework, including Regulation EU 679/2016. In particular, a focus on the legal basis of personal data processing during the rescue operations;

ii) the drafting of a questionnaire that will be submitted to the partners after the pilots;

iii) the analysis of the hypothetical answers and related issues to the questions and the project of a preliminary hypothetical assessment;

iv) in the conclusion, some recommendations for software and technology developers, enabling the data protection, privacy and the adoption of PbD (Privacy by Default) and Privacy by Design approaches, as well as technical and organisational measures to protect personal data and store, respecting the rules and providing internal measures for the retention of the data according to the provisions of the GDPR.

However, the assessment based on real data will be reported in the D8.7, when the pandemic situation should allow the development of pilots.

3. Rescue operations and potential scenarios in ASSISTANCE and data protection issues

Introduction

Provided that ASSISTANCE will involve human beings in dealing with rescue operations during natural disasters, accidents and terroristic attacks, and that the project outcome will collect personal data, some issues related to ethics and data protection aspects must be taken into account.

Particularly, in the context of the rescue operations, the Project has implemented the following pilot scenarios:

- **scenario 1**: earthquake in urban environment pilot scenario. In this scenario, the first activity consists in taking photos and videos with cameras mounted on drones and UGVs. Furthermore, the technologies adopted may collect and register human voices, which are included in the personal data as biometric data. The sensors integrated on the unmanned platforms are: GPS; Cameras on UxV;
- **scenario 2:** chemical plant explosion pilot scenario. In this scenario, due to the fact that it is an industrial accident, the first activity consists in taking photos and videos with cameras mounted on drones and UGVs and samples of possible presence of toxic gases. The sensors identified to be integrated in the pilots are: GPS; Gas sensors; Video cameras mounted on UxV; Infrared (IR) cameras mounted on UxV; Wind speed sensor mounted on UGV. Furthermore, the technologies adopted may collect and register human voices, which are included in the personal data as biometric data.;

- **scenario 3:** terrorist attack pilot scenario. In this scenario, which recreates a terrorist attack in a crowded environment, the first activity consists of taking photos and videos with cameras mounted on drones and UGVs, and also collecting samples of the possible presence of chemical agents. The sensors identified to be integrated on the unmanned platforms in the pilots are: GPS; Gas sensor; Video cameras mounted on UxV; Infrared (IR) camera mounted on UGV; Wind speed sensor mounted on UGV. Furthermore, the technologies adopted may collect and register human voices, which are included in personal data as biometric data.

Thus the Project, considering the pilot scenarios, will involve the processing of personal data. For that reason, an assessment on the impact of rescue operations in relation to data protection and human rights is crucial.

Furthermore, in order to ensure the full protection of the rights and interests of the individuals involved in the pilots and the lawfulness and correctness of the processing of the personal data, appropriate technical and organisational measures have to be implemented.

In that way, the project research process and outcomes should be compliant with the ethics principles as well as with the data protection European relevant legal framework.

Apart from the pilots, the purpose is providing a full assessment of the data protection issues related to the development of the ASSISTANCE technologies. In particular, the analysis will be focused on the measures to be taken to minimize the risks connected with the processing of personal data. In the light of the accountability principle held by the GDPR, the assessment will evaluate the security of the organizational and technical measures adopted by ASSISTANCE. Furthermore, the approach based on privacy by design and privacy by default will be underlined to minimise data protection risks from the very beginning of the design of the technologies used.

Accordingly, ASSISTANCE is complying with the fundamental principles of data protection legislation:

a) Lawfulness, fairness and transparency;
a) Purpose limitation;
b) Data minimization;
c) Storage limitation;
d) Adoption of security measures;
e) Adoption of data protection internal procedures;
f) Designing and adoption of technologies following the principles of privacy by design and privacy by default.

3.1. The General Data protection legislation applicable to the Project

As already mentioned in the D8.1, it is not questionable the application of the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council, hereinafter: "GDPR"), to ASSISTANCE.

It is important to remember that the GDPR has, among its purposes, that of "*ensuring a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data in the Union*". The GDPR is applicable to natural persons (individuals), but anonymised data, i.e. the data which do not allow to identify a data subject, do not fall within the material scope of the GDPR. As for the territorial scope, it covers the cases where the controller is established within the EU territory, but also the case in which the controller is established outside the EU territory, but he offers goods or services to data subjects in the Union, or he monitors their behaviour as far as their behaviour takes place within the Union. In other words, the GDPR is applicable also to companies even if they are not based in Europe, once they provide services or goods to European citizens.

However, GDPR and the remaining data protection legislative provisions are applicable to ASSISTANCE, primarily because the data collected during the pilots fall within the territorial scope, as above mentioned, but also because pilots are programmed to collect real personal data and not fake data, nor these data are anonymised once collected.

As for the technologies, they will be mainly based in the European territory, and thus within the territorial scope of the GDPR. Furthermore, ASSISTANCE is projected in order to use data of individuals (i.e. personal data), through new generation sensors (e.g. advanced cameras, CBRN sensors, UAV/drones, etc.) and then the material scope covers again the outcomes of the project.

Moreover, it is important to remark on the roles that will be played by the different actors of ASSISTANCE.

The **data controller** (or simply the "**controller**") is the subject (natural person or legal entity), public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In other words, the data controller is the one who is directly responsible for the processing, for its purposes, for the security measures, and so on. As for the Assistance project, the single partners will be considered as autonomous data controllers for the data collected and processed during the pilots that they manage, as long as these data are not transferred to the Consortium. The Consortium on its turn will be considered as data controller for the data collected and processed within the outcomes of the project, unless the technologies developed by ASSISTANCE will be transferred to third parties.

3.2. Processing of personal data in rescue operations

The assessment is also aimed at analysing and mapping the typologies of personal data that will be collected in the single phases of the project, as well as the rules on which this processing may be considered lawful.

The general principle is that personal data can be processed if the data subject has provided his or her consent to the processing of his or her personal data for one or more specific purposes.

However, the GDPR lists six lawful basis - i.e. "legal basis" - for the processing of personal data. Each basis is most appropriate depending on the purpose and the relation with the data subject.

The legal basis for processing are set out in the Article 6 of the GDPR, as follows:

- **consent:** the data subject has given consent to the processing of his or her personal data for one or more specific purposes [article 6, lett. a)];
- **contract:** 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 [article 6, lett. b)];
- **legal obligation:** processing is necessary for compliance with a legal obligation to which the controller is subject [article 6, lett. c)];
- **vital interests:** processing is necessary in order to protect the vital interests of the data subject or of another natural person [article 6, lett. d)];
- **public task:** 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 [article 6, lett. e)];
- **legitimate interests:** 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 [article 6, lett. f)].

Specifically concerning the vital interests, Recital 46 of the GDPR states "*the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters*".

In its Opinion 06/2014, the Article 29 Data Protection Working Party had already examined this case, as the legal ground was limited to cases in which the processing of personal data is necessary to protect the vital interests of the data subject.

The application of such legal basis should be limited to life or death situations, or, at least, to cases where there is a risk of injury or other damage to the health of the data subject.

Additionally, concerning the special categories of data, Article 9, lett. c) GDPR provides that "*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*".

Considering the rescue operations, information on human beings is going to be processed under the legal basis of vital interest, thus the life and/or the physical integrity of human beings are threatened.

Moreover, concerning the legal basis, alongside the GDPR, the Reform encompassed a Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data establishing rules for the protection of individuals with regard to the processing of personal data by competent authorities for purposes of law enforcement (so-called Law Enforcement Directive, hereinafter also "LED").

Precisely, the LED applies to the processing of personal data 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.

The scope is 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.

Under the Directive, the personal data shall be processed lawfully only for the purposes listed above. On the contrary, if the purposes are different from the one specified in the Directive, the GDPR will apply instead.

The aspects to be taken into account are related to the technologies that will be used (notably the recourse to video cameras and GPS technologies) and which have an impact on the individuals and on their personal data. However, in the light of the above considerations, the processing of these personal data should be considered legitimated by the mentioned legal basis, in particular for those individuals depicted by the video cameras for security reasons as well as to the FRs that will be monitored through GPS sensors.

On the other hand, the Directive refers to the GDPR with reference to the security measures and the principle of privacy by design and by default.

As for the pilots developed within the ASSISTANCE project, as already mentioned in D8.1, D10.1 and D10.2, the legal basis for the collecting of the data will be based on the consent of the data subjects involved in the pilots themselves. In this case, before collecting the data, the data subjects will be provided with a privacy policy, in which it will be notably explained the typologies of data collected, the purposes of the processing, the data retention period, the rights provided by the GDPR.

The assessment will take into account the retention of the collected data, by drafting procedures in order to delete these data when they are no longer necessary. In this sense, different scenarios can be drawn based on the purposes of data collection and notably whether the data have been collected to manage the pilots (in which case the data should be deleted after the end of the pilots) or whether the data have been collected for security reasons, in which case a longer period of retention should be allowed.

4. Assessment on the rescue operations

4.1. The structure of questionnaire

In order to assess the impact of rescue operations in relation to the ASSISTANCE Project, the methodology adopted consists in the submission of a questionnaire to the Partner dealing with the pilot scenarios that reproduce a critical event (hereinafter, the "**Questionnaire**"). The principal purpose of the questionnaire is to confirm the methodology of the assessment conducted by E-LEX by acquiring all the information related to the implementation of pilot scenarios and transposing the results to a real rescue operation.

Specifically, the questionnaire is structured as follows:

- **Section I** - the role of the partner in the project and the rescue operations activities;
- **Section II** - a general part on data protection;
- **Section III** - the results of the rescue operations. This section is divided in two parts:
    - Part A "the performance of the pilots";
    - Part B "preliminary results and final output".

4.2. Section I of the Questionnaire

Section I is entitled “The role of the partner in the project and the rescue operations activities” and aims at acquiring information regarding the role played by each partner in the Project.

In particular, the Partners must provide information about the rescue operations they are involved in and the specific technologies used to carry them out.

These preliminary elements will be useful to understand the organization of rescue operations, especially the technologies used and their scope within the project.

In fact, depending on the technologies’ functionality, the impact on human beings involved can be evaluated.

For example, the use of sensors for localization are capable of collecting information related to the exact location of the subject (geolocation data) or other sensors concerning the detection of temperature are capable of learning aspects related to the health of an individual.

4.3. Section II of the questionnaire

Section II is entitled “General part on data protection” detects the information related to the application of the GDPR in the context of the rescue operations conducted by the Partner.

Section II is crucial for learning about processing operations, categories of data, and the flow of data throughout a rescue operation.

Specifically, the Partners are required to describe these processes, and how the flow of data (including personal data) is projected and developed. Furthermore, the Partners should explain which measures, also in terms of security, are planned to be adopted during the data processing, including the phase of the data flow.

4.3.1. Processing of data and the methodology

The processing of personal data must comply with some specific principles. Namely, personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘**lawfulness, fairness and transparency**’);

- 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**');
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**');
- 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'**);
- 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**');
- 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 controller shall be responsible for and be able to demonstrate compliance with **'accountability'**.

It has to be reminded of the definition of processing held by Article 4, n. 2 GDPR: "*'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

Precisely, in the Questionnaire, the Partner shall inform about which processing is put in place during the pilots, among the following ones:

- collection;
- recording;
- organisation;
- structuring;

- storage;
- adaptation;
- alteration;
- retrieval;
- use;
- disclosure by transmission;
- dissemination;
- alignment or combination;
- restriction;
- erasure;
- destruction.

The Partners shall also specify the methodologies and the supporting assets, used to process personal data.

4.3.2. Category of data

The GDPR defines (article 4, par. 1) the personal data as *"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, an online identifier or to one or will more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*.

Article 4 of the GDPR includes definitions of specific personal data, which are mostly related to sensitive and peculiar aspects of the personality of physical subjects, and notably:

- **genetic data:** personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question [article 4, n. (13)];
- **biometric data**: personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data [article 4, n. (14)];
- **data concerning health:** personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status [article 4, n. (15)].

Furthermore, processing of personal data being able to reveal 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 are, in general, prohibited and may be processed exclusively in some specific cases. These categories of personal data that are subject to additional protections, as they are considered as the hardcore of the protection that must be ensured to citizens by privacy regulations.

Anonymous information is not covered by the EU Regulation. Recital 26 of the GDPR states that "*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*".

The GDPR makes a distinction between the anonymisation and the pseudonymisation. The latter refers to the reversible de-identification of personal data, for example in cases where it is allowed to re-identify hashed identifiers.

Furthermore, according to Recital 26 of the GDPR, "*the principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. 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*".

It is a crucial point for the use of big data as personal data, once anonymised (or pseudonymised), may be freely processed, without any prior authorization by the data subject.

Even if the GDPR does not define anonymous data, it includes a definition of pseudonymisation as 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.

During the rescue operations, the use of drones and robots may collect personal data, in the forms of video and photographs, as well as geolocation data. For this purpose, the questionnaire is aimed at mapping the typologies of data, in order to provide partners with the measures to be adopted for the compliance with data protection regulations.

4.3.3. Technical measures

The GDPR, in the light of the accountability principle, has introduced the concepts of privacy by design and privacy by default.

According to Recital 78 of the GDPR "*In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*".

Pursuant to Article 25, paragraph 2 of the GDPR "*the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*".

As provided by Article 5, par. 1, lett. f) - also reported above - the personal data shall be 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').

In line with this principle, the Article 32 provides that the appropriate technical and organisational measures shall be implemented to ensure a level of security appropriate to the risk, including *inter alia*, as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

A relevant aspect regarding conducting operations is to illustrate the security measures implemented including encryption; anonymisation; partitioning data; logical access control; surveillance; data breach procedure; traceability; paper document security; minimising the amount of personal data; operating security; backups; physical access control; hardware security; protecting against non-human sources of risks.

4.4. Section III of the questionnaire

Section III is meant to illustrate the results from the simulated rescue operations, starting from the preliminary results detected in the Laboratory environment, Outdoor controlled environment and Realist environment.

The Section consists of two different subsections:

- **Part A - the performance of the pilots**
- **Part B - Preliminary results and final output**

4.4.1. The performance of the pilots

To have a specific view of the Partner's activity within the Project, as a preliminary step, the Partner must provide a description of the pilot and his involvement and, in general, his activity.

In this section, the Partner shall inform also of the critical aspects detected during: the Laboratory environment; the Outdoor controlled environment; the Realist environment.

The Partner is asked to illustrate the critical aspects in order to determine any countermeasures to be put in place.

4.4.2. Preliminary results and final output

In Section B entitled "Preliminary results and final output", the Questionnaire is structured in such a way as to reveal information relating to the results of the operations. The scope is to verify whether in - concretely - the rescue operations were carried out successfully. In particular, the Partner shall evaluate the preliminary results of the rescue operations, with reference to the collection and processing of personal data.

The Partner shall describe all the process conducted and evaluate the risks deriving from them and analyse during the pilots.

5. Conclusions

This paragraph gives an overview on the preliminary conclusions of the assessment, deferring the results after the pilots and the submission of the Questionnaire in the D8.7.

This deliverable will then provide some recommendations for software and technology developers, enabling the data protection, privacy and e adoption of PbD (Privacy by Default) and Privacy by Design approaches, as well as technical and organisational measures to protect personal data as defined by the GDPR.

The aim is to minimize the impact on the rights of data subjects.

5.1. Recommendation in the pilot scenarios

The pilots developed within the ASSISTANCE project involve the use and combination of state-of-the-art technologies provided by the Partners. From the analysis of these technologies, it is possible to trace the type of information that can be collected during such activities.

Most of the data collected during the pilots do not fall within the objective scope of data protection legislation, as they are information not related to natural persons (e.g., morphology of the territory concerned, scientific and/or chemical data, and other general information).

On the other hand, given that devices such as video cameras, IR cameras, microphones and temperature sensors are used, common and biometric data on the individuals involved can also be collected.

As already mentioned, the processing of such data will not take place through the provision of consent by the data subjects. The legal basis of processing, in fact, should be the protection of vital interests and the purposes of public order and public security.

Since the pilot scenarios consist of simulations of potential hazard or threat, there is no real danger to the safety, life or security of the participants, and they are therefore asked to consent to the processing of their personal data.

Nevertheless, and irrespective of the legal basis / purpose of the processing, the relevant provisions ensure that data subjects have the right to be properly informed about any processing of their personal data. This right corresponds to the obligation of the data controller to provide data subjects with any useful information about the processing.

For such reasons, in the context of the pilot scenarios, all the participants in project activities implying the processing of personal data will be given an information pack about the project with an Information Sheet. The participants must be informed about:

- The voluntary nature of their participation;
- The degree of risk and burden involved in participation;
- Who or what will benefit from participation;
- The procedures that will be implemented during all the pilot scenarios.

Participants must be informed about the collection of the data and their protection during the project, as well as their destruction or re-use at the end of the research. This aspect will be complied by providing participants with a privacy policy, explaining these aspects. Participants will also know that they can ask questions and receive understandable answers before deciding and withdraw themselves and their data from the project at any time without any negative consequence.

As also specified in the Deliverable D10.02, the ASSISTANCE project will perform all activities involving human participants, upon release of information sheets and consent forms. The Information sheets contain detailed information to the potential participants such as the purpose of the project, the duration of the research activities, the possible risks, the data protection, confidentiality and privacy policies.

The Consent Form will provide evidence of participant's agreement to be involved in the project, including: a statement of agreement in participation; the participant identification, the anonymisation code.

As for software and technology developers a list of measures to be adopted will be provided based on the information collected through the questionnaires, also to minimize the data protection risks since the designing of the technologies will be used.

Lastly, in-depth considerations concern the retention periods of personal data collected through pilot activities. Both the GDPR and the LED establish a general principle of limitation of storage, whereby personal data is kept only as long as necessary to achieve the purpose of processing. This is without prejudice to retention for longer periods – and with the appropriate safeguards – only for archiving purposes in the public interest, or for scientific, historical or statistical purposes.

Since the legislation does not provide for specific retention periods, it leaves it to the data controller to establish them, informing data subjects at least of the criteria used to determine these periods.

Moreover, as this is a subject that is also currently examined by the bodies responsible for interpreting the relevant legislation (e.g., the European Data Protection Board, the European Data Protection Supervisor, the judicial authorities or the independent supervisory authorities of the individual Member States), we recommend that the issue be closely monitored, also to offer any suggestion regarding the interpretation and practical implementation of the applicable rules.

5.2. Mapping of ethical risks

The risks that will be considered with the questionnaire are aimed at highlighting a scenario describing an event/research action/result of the project and its consequences, estimated in terms of severity of impact on data subjects and likelihood of its occurrence.

As already pointed out in the D10.11, the metrics of the evaluation of the risks will be the following ones and, at the present stage, the risk may be confirmed as already reported and may be still evaluated as follows:

Table 1 - Ethics risk map

GDPR	**Ethics risk**	**Probability of risk:** ***High*** ***Medium*** ***Low***
Right to be informed		
Article 12	No transparency of Information	***Low***
Article 13 (1) and (2) and Article 14 (1) and (2)	No content of Information	***Low***

Article 13 (1) and Article 14 (3)	Insufficient time of providing Information	***Low***
Article 12 (1), (5) and (7)	Poor means of providing Information	***Low***
Article 13 (2) (d) and Article 14 (2) (e), Articles 77, 78 and 79	No satisfaction of right to lodge a complaint	***Low***
Right of access		
Article 15 (1)	No satisfaction of right of access to one's own data	***Low***
Right to rectification		
Article 16	No rectification of inaccurate personal data	***Low***
Right to erasure		
Article 17 (1)	No erasure of personal data	***Low***
Right to restriction of processing		
Article 18 (1)	No satisfaction of right to restrict use of personal data	***Low***
Article 19	No notification	***Low***
Right to object		

Article 21 (1)	No satisfaction of right to object due to the data subject's particular situation	***Low***
Article 21 (2)	No satisfaction of right to object to use of data for marketing purposes	***Low***
Article 21 (5)	No satisfaction of right to object by automated means	***Low***
Rights related to automated decision-making and profiling		
Article 22	No satisfaction of right related to automated decision-making and profiling	***Low***
Article 21	No satisfaction of right to object automated decision-making	***Low***
Article 13 (2) (f)	No satisfaction of right to a meaningful Explanation	***Low***
Compliant organizational and technical measure		
All	Failure in implementing the measures foreseen in D10.7 of ASSISTANCE	***Medium***
All	Unauthorized access, exfiltration or destruction of personal data	***Low***