ASSISTANCE

Adapted situation awareneSS tools and tallored training curricula for increaSing capabiliTie 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 D8.1

Report on the Relevant Legal EU Framework and Assessment of the Ethical Impact

31/10/2019

[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 FRs organizations cooperate together facing large and complex disasters, that in some cases can be amplified due to new threats such as, the climate change in case of natural disasters (e.g. big floods, large wild fires, etc) or the increase of radicalization in case of man-made disasters (e.g. arsonist that burn European forest, big combined terrorist attacks in European cities).

The impact of these kinds of large disasters could have disastrous consequences for the European Member States' regions and social wellbeing in general. On the other hand, each type of FRs organizations (e.g. medical emergency services, firefighters' departments, law enforcement teams, civil protection professionals, etc.) that work mitigating these kinds of events are exposed to unexpected dangers or new threats that can severely affect their personal integrity.

Taking into account these facts, ASSISTANCE proposes a holistic solution that will adapt a well-tested SA application as a core of a wider SA platform, capable of offering different configuration modes for providing the tailored information outcome needed by each FR organization, while they work together mitigating the disaster (e.g. real time video and resources location for firefighters, evacuation routes status for emergency health services and so on).

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

On the other hand, ASSISTANCE also proposes to improve the FRs skills and capabilities through the establishment of a European advanced training network for FRs that will provide tailored training based on new learning approaches (e.g. virtual, mixed and/or augmented reality) adapted to each type of FRs organizations needs 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, contract 832576.

Disclaimer

Executive Summary

This deliverable consists in a report to frame the most relevant legal EU framework and to outline the most adaptable approaches and methods for assessing the ethical impact of ASSISTANCE. The document analyses the European relevant legal and ethical backgrounds for both defining legal and ethical constraints for ASSISTANCE and preparing the pilot operations and understanding the impact of rescue operations on data protection, privacy and human rights.

List of Authors

Organisation	Authors
E-lex	Adriana Perduto, Giovanni Maria Riccio, Maria Laura Salvati
CEL	Antonio Carnevale

Change control datasheet

Version	Changes	Chapters	Pages	Date
0.1	ToC	All	11	17/09/19
0.2	ToC integrated by partners feedbacks	All	11	20/09/19
0.3.1	First draft of deliverable (ethics chapters by CEL)	CEL	16	15/10/19
0.3.2	Internal version for review	e-lex	39	20/10/19
1	Final version to submit to EC	E-lex- CEL		30/10/19

Content

List of Figures

List of Tables

Acronyms

ASSISTANCE	Adapted situation awareneSS tools and taIlored 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
GDPR	Regulation (EU) 2016/679
H2020	Horizon 2020 Programme for Research and Innovation
IPR	Intellectual Property Rights
M#	#th month of the project (M1=May 2017)
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
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle

1. Fundamental Rights Framework

1.1. The Fundamental Rights in the Treaty of the European Union

The original Treaties – i.e. Treaty establishing the European Economic Community also known as the Treaty of Rome - on which is based the European Law did not contain any reference to human rights nor to personal rights.

In fact, the European Communities, at that stage, was essentially aimed at establishing a cooperation with an economic scope of action.

The need of a common framework on fundamental and human rights was not seen as necessary, considering that the member States were all signatories of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) held in 1950.

However the compatibility between the European Law and the national regulations, notably with the constitutional principles on which the member States were based, led the European Court of Justice (CJEU) to the support the principles of direct effect and of primacy of European law, even not stating on the impact of that on the national law.

On the other side, some constitutional Courts – in Germany and Italy – issued decisions in which they reserved to themselves the possibility of reviewing the European law in any case in which it would have been in contrast with the constitutional values of the State.

After these decisions, the CJEU, in the following case-law, affirmed that its decisions were respectful of the fundamental rights, stating that they were based on the fundamental rights held in the general principles of the Community and inspired by the common frame of the constitutional tradition of the member States.

This process was empowered by the Treaty of Maastricht, that contained a specific reference to the ECHR and the common constitutional traditions of Member States as general principles of EU law as well as by the following Treaty of Amsterdam.

1.2. The Charter of Fundamental Rights of the European Union

The need of a European bill of rights was clearly expressed by the Council in 1999, when the Council suggested the creation of a "body composed of representatives of the Heads of State and Government and of the President of the Commission as well as of members

of the European Parliament and national parliaments" should be formed to draft a fundamental rights charter".

The Charter of Fundamental Rights of the European Union was approved and proclaimed by the European Parliament, the Council of Ministers and the European Commission on 7 December 2000.

The Charter has not included in the existing Treaties and came into force with the Lisbon Treaty in 2009.

The Charter is divided into 7 titles:

- first title (Dignity);
- second title (Freedoms)
- third title (Equality)
- fourth title (Solidarity)
- fifth title (Citizen's Rights)
- sixth title (Justice)
- seventh title (General Provisions)

Some of the provisions held in the Charter were already in the European law and many of them are an outcome of the case-law of the Court of Justice. Some other provisions are new, such as those disability and sex-discrimination as well as those on data protection and access to administrative documents.

1.3. The right to privacy

Article 8 of the Charter of Fundamental Rights of the European Union states that everyone has the right to the protection of personal data concerning him or her. The second paragraph holds that the 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’.

The last paragraph of article 8 grants the control on data protection issues to independent authorities.

2. Relevant Legal EU Framework

2.1. The General Data Protection Regulation

The General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council, hereinafter: GDPR) has been issued on 27th April 2016 and is in force in all EU members from 25th May 2018.

The text is composed by 99 articles plus 173 recitals. It is a complex text which aims, on one side, at updating the European legislation on data protection with a legislative act which is more adequate to the modified technological and sociological scenario and, on the other hand, to adopt a text which will be enforceable, without differences, in all the member States. In fact, being the GDPR a regulation, it does not require an implementation by the member States into their national legal framework.

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".* This purpose of harmonisation has not been achieved by the previous EU directives and notably by the Directive 46/97/EC, although it is regarded as a central issue by the same European Institutions. The option of adopting a Regulation instead of a Directive aims at ensuring a common framework, limiting the regulatory interventions by member States and national data protection authorities.

However, a limited State legislative power remain, as some sectors do not fall into the scope of the GDPR, such as: freedom of expression and research; labor law; access to official documents.

The GDPR has followed a complex path before its formal and final approval. It has been proposed on January 2012, then on March 2014 the European Parliament has issued and amended version, as well the Council of Europe, on June 2015.

The approach of the GDPR, if compared with the previous legislative acts of the European institutions, contains a significant innovation, as it combines the strictly regulatory aspects with organizational and technological aspects.

2.2. Personal data. Anonymized and pseudoanonymized data

Regulation no. 2016/679 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 aspect 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, physio- logical or behavioral 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 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. Whereas n. 26 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".

Furthermore, according to Whereas n. 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 using 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 as personal data, once anonymized, may be freely processed, without any prior authorization by the data subject.

Working Group Article 29, in Opinion 05/2014 of 10 April 2014 on anonymisation techniques, states that "anonymisation is a technique that applies to personal data in order to obtain an irreversible de-identification". Then the pseudonymisation is the case in which the processing of personal data is made in such a way that personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures intended to guarantee that such personal data is not attributed to an identified or identifiable individual.

2.3. Data roles

Article 4 GDPR defines the controller as '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'.

The processor is 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'. Pursuant to article 28 GDP, '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'.

The data processor cannot appoint a sub-processor without prior specific or general written authorisation of the controller.

Two or more controllers may be considered as joint-controllers where they jointly determine the purposes and means of processing. This last case is quite rare, as the determination of purposes and means is limited to specific data processing activities. In other words, where two subjects collect and manage personal data for a single activity, but they use the data also for other purposes, which are autonomously determined by the subjects themselves, they will be considered joint-controllers only in the first case

and not in the latter. According to the Opinion 1/2010 of the WP Article 29, this is the case where a plurality of subjects pursues distinct purposes of processing, but they decide to create a common infrastructure to pursue said purposes, sharing the choices regarding the means to be used.

According to the same article 4, recipient 'means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not'.

2.4. Data Protection Officer

The GDPR has introduced the figure of the data protection officer - DPO. This role was already mentioned in some member States' legislation, such as in France and Germany.

The DPO is a complex role, as it is expected to supervise all the matters which are related to data processing. In particular, pursuant to article 37 GDPR the appointment of the DPO is compulsory in 3 cases:

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

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;

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.

The boundaries of the notion of "large scale" is not predetermined by the GDPR. Initially, the proposed Regulation referred - like German law - to a minimum number of employees (250). The Whereas 91 qualifies large-scale treatments such as those which aim to treat a significant amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and potentially present a high risk. Although missing, in numerical terms, a precise indication, the parameters to consider, in order to assess whether the concept in question exists are the following:

a. the number of subjects involved in the processing, in absolute terms or expressed as a percentage of the reference population;

b. the volume of data and / or the different types of data being processed;

c. the duration, or persistence, of the treatment activity;

d. the geographical scope of the treatment activity.

This notion includes, for example, banks and insurance companies in the context of ordinary activities involving customers; subjects that use geolocation services (for example, for customers of commercial chains or for monitoring traffic or access to historic centers); processing of data (metadata, content, location) by telephone or telecommunications service providers. They do not fall under the notion of "large scale" and, therefore, do not determine the obligation to appoint a DPO, the treatments carried out by individual professionals for the data of their clients or patients (for example: accountants, lawyers, doctors, etc.).

Also in this case, the GDPR does not provide a delimitation of the concept of "regular and systematic monitoring". First of all, it must be noted that monitoring must be both regular and systematic, since the assumptions are to be understood as cumulative and not alternative. As for the notion of regular, this is the monitoring that is carried out with one of the following conduct:

a. continuously or at defined intervals for a defined period of time; b) recurrent or repeated at constant intervals;

b. consistently or at periodic intervals (see WP29, pag. 11).

Instead, monitoring is systematic when:

a. it happens by system or by default;

b. it is predetermined, organized or methodical;

c. it takes place as part of an overall data collection project;

d. it is carried out as part of a strategy.

Among the examples listed by the WP29 of "regular and systematic" monitoring can be mentioned: loyalty programs; behavioural advertising; monitoring of data relating to the state of psychophysical well-being, physical fitness and health through wearable devices; connected devices such as smart meters, smart cars, home automation devices.

The DPO must be designated "according to the professional qualities, in particular of the specialized knowledge of the legislation and practices regarding data protection" (art. 37, par. 5 GDPR). There are no registers or other professional bodies for this figure, nor specific training courses or certifications: therefore, the documented experience in the sector is sufficient to cover this position.

Article 38 GDPR requires that the data controller and the data processor must involve the DPO in all matters concerning the protection of personal data.

In particular, the DPO must be informed and consulted regarding the impact assessments on data protection, from the initial stages. WP29, by way of example, stated that the DPO should participate in senior and mid-level management meetings,

with regular deadlines; that his presence is necessary every decision that have an impact on data protection, providing him with all the information necessary to render a suitable consultation; that the opinion of the DPO receives the attention of the owner, the manager and the management of the structure of the latter (WP29, 18).

The DPO therefore acts primarily as a consultant to the data controller or data processor: they are not required to comply with the opinions of DPO, but any dissent must be documented. The DPO must not, in any case, subrogate to the obligations which are due by the data controller or by the data controller. For example, in the event of a data breach, the disclosure obligations are in any case on the data controller, although the DPO must be promptly consulted.

2.5. Material and territorial scope of the GDPR

The material scope of the GDPR is limited to the processing involving individuals and so the data related to entities are generally out of the scope of the Regulation. Furthermore, the application involves automated processes, even partially, for non-personal purposes, as state by the European Court of Justice in Ryneš - Case C-212/13.

The GDPR has significantly extended the territorial scope of application. The GDPR covers the cases in which:

a) the controller is established in the territory of the European Union

b) regardless of whether the processing is carried out within the borders of the European Union it applies to non-EU subjects:

a) if they offer goods or services, regardless of the payment of the same, to a subject who is based in the European Union;

b) if they monitor the behaviour of subjects and such monitoring takes place in the European Union.

2.6. Principles of data processing

The architecture of the GDPR is essentially based on 5 principles.

The principles are the following:

a) lawfulness, fairness and transparency: transparency is one of the key points in relation to big data. Users are often not fully informed and in the position of properly understanding the privacy policy of the services (e.g. App) which collect their data. The data subject must be, among other things, in a position to easy access the information related to his data, to the data protection officer and to the methods and purposes of the processing. It must also be able to exercise the rights granted to him by the GDPR.

b) Purpose limitation: the person who collects the data needs to inform the data subject of the purposes for which the data are collected. Subsequently, personal data may be processed only for those purposes and not be used for different purposes.

c) Data minimization: The data must be relevant and limited to the purposes for which they were collected. Therefore, personal information cannot be collected if they are not closely related to the purposes of collection or, rather, only personal data which are necessary for these purposes can be collected. Thus, the amount of personal data processed must be limited to the minimal amount possible.

d) Accuracy and updating: the data must be constantly updated and rectified in case of request of the person concerned. In relation to big data, among these rights, the right of cancellation or erasure is specifically important.

e) Storage limitation: data can only be kept for the time necessary for processing and later destroyed. Personal data can also be stored for longer time 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.

f) Integrity and confidentiality: the data controller must ensure adequate security of personal data by appropriate technical and organizational measures, including protection against unauthorized or unlawful processing and against the loss, destruction or accidental damage.

2.7. Consent

The general principle is that personal data can be processed if the data subject has provided his consent to the processing of his or her personal data for one or more specific purposes. However, the GDPR lists several cases in which personal data may be processed based on other circumstances and prerequisites, such as where 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.

Pursuant to article 6 GDPR, 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.

The consent may be expressed in any form, but the data controller be able to demonstrate that the data subject has consented to processing of his or her personal data.

The consent must be freely provided and the information provided to the data subject in the privacy policy should be easily understandable by the data subject itself and written in a clear and non-technical language.

2.8. Privacy by design and privacy by default

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

These concepts were not included in the EU Data Protection Directive (Directive n. 96/45/CE), and the Directive only held the obligation for data processors to implement technical and organizational measures in order to fully protect personal data against unlawful conducts. Similarly, member States' regulations did not hold any specific rules on these issues, even if some Data Protection Authorities (e.g. UK's ICO) has already issued specific guidelines for implementing such measure by default or by design.

According to Whereas n. 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 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 regarding 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".

Privacy by default was not included in the European or national regulations and, as said, it can be considered as a corollary of the accountability principle.

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".

2.9. Privacy Impact Assessment

As mentioned, the GDPR has assumed an accountability approach according to which data controllers are expected to make a preliminary check on the potential risks connected with the processing of personal data. The privacy impact assessment has replaced the obligation of notifying processing of personal data to the national data protection authority.

In this context, a basic role is given to the privacy impact assessment (PIA), which is one of the most important news introduced by the GDPR in the data protection scenario.

In any situation where a data processing may involve personal information, data controllers are expected to conduct a privacy risk assessment, together with the DPO, in order to ensure that such processing is compliant with the requirements of the GDPR. The PIA is due if the processing is "*likely to result in a high risk*" (such as, for instance, users profiling, processing of sensitive and judicial data).

In case of residual high risks, the data controller will have to contact the competent data protection authority for a prior consultation. In this case, the DPA will decide whether the data processing may expose data subject to relevant risks or not and authorize (or not) the processing.

The GDPR does not provide a complete list of the cases in which a processing is likely to result in a high risk, and the data controller is the one, together with the DPO, who has to evaluate these potential risks. The risks may be minimized by taking some technical and legal measures, such as: pseudonymization/anonymization of personal data; adoption of certifications; adhesion to codes of conduct; implementing privacy by design and privacy by default procedures.

2.10. Data Breach

A data breach is any event that accidentally or illegally involves the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or otherwise processed.

Whereas no. 86 GDPR states that 'The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication'.

Some examples of data breach are: cyber-attacks and unauthorized access to the IT systems of the data controller; theft or loss of laptops, smartphones, tablets belonging to the data controller containing personal data; theft or loss of paper documents containing personal data; theft or loss of unencrypted portable storage devices, such as USB sticks and external hard drives, containing personal data; loss or irreparable modification of files containing personal data in digital format (for example, due to incorrect deletion or modification by the digital systems or files belonging to the data controller that cannot be restored through the use of a backup).

It seems important to underline that not any of the above-mentioned cases holds the necessity of a notification but exclusively those that, as mentioned above, could lead to a high risk to the rights and freedoms of individuals.

The data breach must be notified to the Data Protection Authority within 72 hours. In case of communication to the data subjects concerned, a clear and understandable language must be used. It is also necessary to communicate the contact details of the DPO or of another contact point at which to obtain more information, as well as describe the likely consequences and the measures taken.

3. The ePrivacy Regulation

3.1. The purposes of the Regulation

On January 10th 2017 the European Commission issued a Proposal for a Regulation on Privacy and Electronic Communications (hereinafter "the Regulation"), set to replace the ePrivacy Directive. The aim of the Commission is to reinforce trust and security in the Digital Single Market by updating the legal framework: this Regulation would have a significant and far-reaching implications for internet-based services and technologies.

Article 5 of the Regulation explicitly states that "*electronic communications shall be confidential, any interference by natural or legal person without the consent of the end users concerned shall be prohibited*".

Like the GDPR, the Proposal is a «*regulation*». The EU Commission, again, chose this instrument instead of a directive, since the Regulation applies in all EU countries without the need for any implementation. It also means that the text of the Regulation is the same for all the member States, which do not have the power to modify it in the course of the transposition, and this aims at harmonizing the data protection rules in all the EU countries, providing a legal instrument which is the same for all the entities which operate within the EU territory.

3.2. Material and territorial scope

The ePrivacy Directive only applies to traditional telecoms operators, while the ePrivacy Regulation would cover new providers of electronic communications services (such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, or Viber). The Regulation applies to the processing of electronic communications data processed in connection with the provision and the use of electronic communications services but also to information related to the terminal equipment of end user[2].

Similarly to the GDPR, with this regulation the EU Commission would extend the territorial scope of application to all providers of electronic communications services, including over-the-top service providers (OTTs) based outside EU. According to the Regulation, OTTs are the internet-based services enabling inter-personal communications (e.g., instant messaging, VOIP services, web-based email, IoT devices, machine-to-machine communications), which are currently not covered by the ePrivacy Directive 58/2002. Then, the Regulation expands the reach of European law to non-EU companies providing electronic communications services to, or processing data of, European individuals.

3.3. Basic principles of ePrivacy Regulation

As for the material scope, the ePrivacy Regulation is based on the following rules.

[2] Art. 2 of Proposal for a Regulation on Privacy and Electronic Communications

Restrictions on the Use of Electronic Communications Data. The Regulation significantly limits the processing of electronic communications data to:

i. the content of the communications (e.g., text, voice, sound, images, videos), and

ii. the metadata (e.g., location, date, time, duration, type of the communication), please note that the term 'metadata' replaces the current definition of 'traffic data' under the current e-Privacy Directive.

Normally electronic communications data can only be processed as necessary to guarantee the transmission of the communication or to ensure the security of the communications. In addition, the Proposal allows the processing of metadata and the content of electronic communications in limited situations:

Content of communications can be processed: for the sole purpose of providing a specific service to an end-user, if the end-user consent to the processing and if that processing is necessary to provide the service; or if all parties to the communication consent to the processing of the content for a specific purpose, given that this purpose could not be achieved by processing anonymous data and that the company complies the GDPR prior consultation requirement.

Metadata can be processed: if the end-user concerned consents to the processing of metadata for specific purpose and provided that the purpose could not be achieved by processing anonymous data; if necessary to meet mandatory quality of service requirements; or if required for billing, calculating interconnection payments, detecting or stopping fraudulent or abusive use, or subscription to electronic communications services.

Cookie Law. The Proposal keeps the requirement to obtain prior informed consent for using cookies and similar technologies. The prior consent is not required if the use of such technologies is necessary for:

i. the sole purpose of carrying out the communication; or

ii. to provide an information society service requested by the individuals.

It is worth noting that the Regulation simplifies the process by recognizing that the consent can be obtained via browser settings and by creating an exemption from the consent requirement for first party analytics.

Users' Terminal Equipment. The ePrivacy Regulation holds conditions for the collection of data emitted by users' terminal equipments (MAC address, IMEI, IMSI). Such data collection is only permitted to establish a connection; if users receive a clear and prominent notice that complies with the GDPR privacy notice requirements and explains the measures individuals can take to minimize or stop the data collection; and if appropriate security measures are in place. The goal is to cover the tracking of users'

devices for services such as people-counting in defined areas or providing personalized offers to individuals as they enter a store.

Direct e-Marketing Rules. The e-marketing provisions will be applicable to all communications means (e.g. automated phone calls, instant messaging application, social media messaging, SMS, MMS, Bluetooth, e-mails). Direct e-marketing to individuals requires prior informed consent (opt-in), unless communications are sent to existing customers regarding the company's own similar products or services and the customers receive means to opt-out at the time of data collection and in each marketing communication.

4. European and national legal framework on drones and other devices

4.1. The attempts towards a European regulation

Since 2015 both the European Parliament and the Council of the European Union, considering their role as the main decision-making bodies of the European Union, are actively working on the adoption of the first ever EU-wide rules for civil drones.

On 2018, the European Parliament and the Council issued the Regulation (EU) 2018/1139 on common rules in the field of civil aviation, creating a European Union Aviation Safety Agency (EASA) to occupy a coordinating role in cybersecurity in aviation. In the same year EASA was empowered to propose to the European Commission the technical expertise to regulate drones of all sizes and to harmonize standards for the European commercial market and urban air mobility, the so-called new Basic Regulation.

Before that, the use of drones and data protection rights were already a concern of the European Parliament Article 29 Data Protection Working Party (WP29). The WP29, on 2015, released the Opinion n. 01/2015 regarding privacy and data protection issues related to the use of unmanned aircrafts. Through such opinion, some principles as transparency, proportionality and minimization on the collection of personal data were stablished as the foundation for processing personal data using drones.

In 2019, more precisely on the months of March and May, the European Commission published the Regulation (EU) 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems and the Regulation (EU) 2019/947 on the rules and procedures for the operation of unmanned aircraft, respectively. These first EU-wide regulations for civil drones were kept as simple as possible, with a strong focus on the particular risk of the specific operation (for example, flying the same drone over a city center or over the sea entails completely different risks). The regulations,

which will enter into force on 2020, aim to the harmonization of operations and regulations in Europe and to create a common EU market for drones.

Since the use of unmanned aircraft systems pose a series of challenges and concrete risks on safety, security and the fundamental rights, the new rules include technical and operational requirements for unmanned aircrafts. The rules define the capabilities a drone must have to be own safely, but they also cover each operation type, as well as minimum remote pilot training requirements.

The new rules are meant to allow everyone to buy and operate a drone ensuring safety, security, privacy and environmental protection.

4.2. Basics on the Spanish legal framework

In 2017, Spain approved the Royal Decree n. 1036 which regulates the registration and circulation of unmanned aircrafts. According to the new rules, operators shall ensure that drones are visible and identifiable as possible. The Royal Decree introduced new scenarios regarding drones' use: for aircrafts weighting more than 2 kilograms and dedicated to professional use, flights over cities, night flights or flights with less visual control are now authorized, but also having license and a liability insurance is mandatory.

Recreational flights, however, shall not exceed 120 meters of height from the ground and for night flights only aircrafts weighting less than 2 kilograms are authorized. They may flight maximum over 50 metres height from the ground.

The Spanish Data Protection Authority clarifies that, accordingly with articles 8, 9 and 10 of the Royal Decree, the drones shall have characteristics associated with the data controller and the operator shall be visible and identifiable as the controller of the drone.

In the data protection prospective, the Spanish Authority issued a guide aiming to clarify privacy aspects when using a drone. In cases when is inevitable to the operator record personal data during the flight, the Authority advises to minimize as much as possible the presence and/or collection of personal data in the operating zone. To comply with such recommendations, operators should perform flights at times where there are not large concentrations of people or when access to the flight zone is restricted, consider the possibility of not capturing the full flight but only necessary moments as well to promote and apply privacy features from design such as, for example, adjust the resolution of the image to the minimum necessary, reduce the granularity of geolocation or apply techniques for the anonymization of images.

4.3. Basics on the Italian legal framework

In Italy the European regulation did not came fully into force. At the time being, the use of drones is regulated by the "Air Pilot Regulation with Remote Pilotage" of ENAC - National Civil Aviation Authority.

The first version of the Remote Pilotage Aircraft Regulation is dated December 16, 2013 and has undergone several amendments to adapt it to the international and European legislation.

The ENAC, pending the adoption of a regulation implementing the European legislation, with a provision dated 25 September 2019, has decided to partially suspend the application of the Remote Piloting Aircraft Regulation.

It can certainly be anticipated that the registration on the D-Flight website www.d-flight.it and the application of an electronic identification device will become mandatory. For critical operations, future Specific operations, the pilot and the vehicle must have the relevant authorizations, certifications and be registered on the D-Flight site.

As regards the protection of personal data, the Italian regulation, in accordance with European legislation, states as follows:

Remotely Piloted Aircraft System with aircraft with operating take-off mass of less than 25 kg

Art. 8 General provisions for operating RPAS

The RPAS shall be identified by a plate installed on the RPA showing the identification of the system and the operator. An identical plate is also on the remote ground pilot station. 2. As of the 1st of July 2016, in addition to plates required by the Art 8.1, any RPAS shall be equipped with an Electronic Identification Device, which allows the transmission of real time data, its owner/operator and basic flight parameters, as well as the recording of these data. Electronic Identification Device performances and characteristics are defined by ENAC.

Remotely Piloted Aircraft System with aircraft operating with take-off mass of more than or equal to 25 kg

Art. 14 Registration and identification

1. RPA with operating take-off mass more than or equal to 25 kg, flying inside the Italian airspace, shall be registered by ENAC in the RPAS register, by assigning dedicated registration marks; identical registration marks to be shown on the remote ground pilot stations. The identification plates shall be installed on the RPA and the remote ground pilot station. 2. The application for registration shall be made by the RPAS owner in a form and manner established by ENAC.

Art. 34 Data protection and privacy

1. When operations carried out by a RPAS could lead to the processing of personal data.
2. As amended (Italian Data Protection Code), with regard to the use of forms of identification of a person only, pursuant to Article 3 of the related Code, as well as in accordance with the regulations in charge of protection of personal data.

4.4. Basics on the German legal framework

In Germany, the Federal Aviation Office is the responsible office for the issuance of permits and authorizations for unmanned aircrafts operations. The German law was modified in 2017 and added a certain number of restrictions in comparison with the former regulation.

The 2017 Act to regulate drones' use stablished that for drones weighting more than 250 grams an identification label – water, fire and crash resistant - with the operator's name and address is required. Drones up to 5 kilograms may be operated without a permit as long as it complies with other safety rules, still a license is required. One of the peculiarities of the German Act is the prohibition of drones' flights over nature reserves due to the German Laws for nature conservation.

The new drone regulation eliminated mostly of the previous separation between leisure and commercial pilots and having a liability insurance is a mandatory requirement for all types of operators.

Regarding data protection aspects, the German Act states that aircrafts weighting more than 250 grams or capable to collect, store or transmit optical data, acoustic data or radio signals are prohibited to fly over residential properties. For flights with the usual camera drones, the consent of the person whose rights might be affected must be obtained.

4.5. Basics on the France legal framework

The regulation of the drones has been recently modified by the Decree n°2019-348 of 19th April 2019 on the notification of the information concerning the use of aircrafts traveling without anyone on board.

In general, the use of drones is regulated by articles from L6214-1 to L6214-3 of the Transportation Code, which are dedicated to the rules on the circulation of drones.

As for the data protection aspects, the Direction Générale de l'Aviation Civile has issued, in 2016, the guidelines which have been agreed with the CNIL, the French data protection authority. These rules mix security and data protection interests, and notably hold that

the pilot must never lose sight of his drone, nor fly it at night or higher than 150 meters; that the drone must not fly over the urban area or where crowded people may be located; and also that the drone does not have to approach aerodromes and sensitive sites.

In case of drone equipped with cameras, microphones and other sensors must respect the general privacy rules. Especially, it is forbidden to record images allowing to directly or indirectly recognize or identify people (such as through faces, number plates, etc.) without their prior consent.

5. Relevant Ethics Framework and Assessment Methods

This is a premise to elucidate the modus operandi in next paragraphs of the present ethics' section.

In a first paragraph (3.1), there will be described the most significant EU framework acting as value-based backgrounds of the ethical analysis as well as evaluation that will be led during the entire WP8. In this sense, this deliverable constitutes a sort of ground to overview the most pertinent ethics codes in EU. This overview has not solely a state-of-art function, rather it wants to explore and provides evidence to those settings of values that meet the research needs of ASSISTANCE.

In a second paragraph (3.2), the argumentation will move from the EU frameworks to the different theoretical kinds of approach for evaluating and assessing ethics concerns in a project like ASSISTANCE. The most prominent methods of ethics impact assessment will be described, providing for each ones some brief remarks on its virtues/deficits account, so that, in the further researches of the project, the teams and the consortium will be aware on the kind of approach to be used.

5.1. Relevant Ethics Framework

5.1.1. Ethics and ASSISTANCE research

ASSISTANCE consortium is fully committed to adhere to the highest ethical and fundamental rights standards, as recognized at the European Union and International condes and legislations, including, among others:

- *Charter of Fundamental Rights of the EU* (2007/C 303/01[3]), repealing older version 2000/C 364/01.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12007P/TXT&from=en

- *General Data Protection Regulation (GDPR)* (Regulation (EU) 2016/679[4]), repealing Directive 95/46/EC.
- *Regulation on Privacy and Electronic Communications* (ePrivacy Regulation), repealing Directive 2002/58/EC.
- *Convention No. 108 of the Council of Europe for the Protection of Individuals* with regard to Automatic Processing of Personal Data adopted on 28 January 1997., as well as the modernised "Convention 108 +" (April 2019)[5].
- *Directive 96/9/EC* of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases[6].
- *Directive (EU) 2019/790* of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
- Rome Declaration on *Responsible Research and Innovation* in Europe, 21 November 2014[7].
- *European Charter for Researchers*, 2000[8].
- *European Code of Conduct for Research Integrity*, ALLEA 2017[9].
- *Ethics in Social Science and Humanities*, European Commission, DG Research and Innovation, 2018[10].

Most of these ethical principles' sources have been already mentioned in the first part ("legal framework") of this document.

As a result, ASSISTANCE teams have already submitted a series of 11 deliverables within **WP10** dedicated to describing the principles and the measures to set up and implement the ethics requirements of the project (**D10.1-D10.11**, delivery dates: Month 4 and 6). As a result, we remand to these documents for more details.

5.1.2. Ethics and ASSISTANCE technologies

From a technological point of view, as stated in GA, ASSISTANCE "proposes a holistic solution that will adapt a well-tested SA application as a core of a wider SA platform, capable of offering different configuration modes for providing the tailored information outcome needed by each FR organization, while they work together mitigating the disaster (e.g. real time video and resources location for firefighters, evacuation routes status for emergency health services and so on)." (p. 9)

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1565626226399&uri=CELEX:32016R0679
[5] https://www.coe.int/en/web/data-protection/convention108/modernised
[6] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01996L0009-20190606
[7] https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf
[8] https://euraxess.ec.europa.eu/jobs/charter/european-charter
[9] https://allea.org/code-of-conduct/
[10] https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf

"With this solution ASSISTANCE will enhance the FRs SA during their mitigation activities through the integration of new paradigms, tools and technologies (e.g. drones/robots equipped with different sensors, robust communications capabilities, etc.) with the main objective of increasing both their protection and their efficiency. On the other hand, ASSISTANCE also proposes to improve the FRs skills and capabilities through the establishment of a European advanced training network for FRs that will provide tailored training based on new learning approaches (e.g. virtual, mixed and/or augmented reality) adapted to each type of FRs organizations needs and the possibility of sharing virtual training environments, exchanging experiences and actuation procedures." (p. 9)

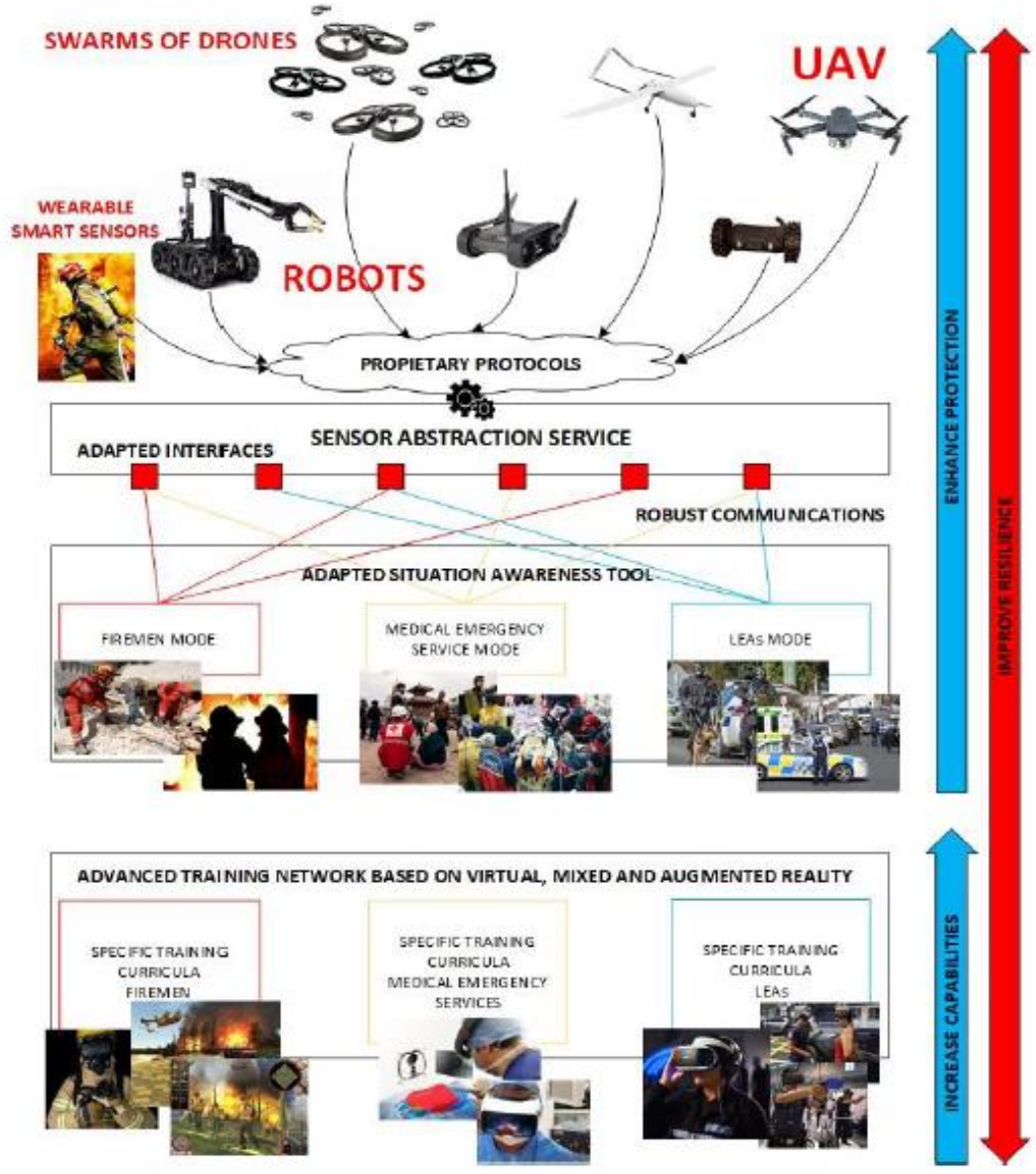


Figure 1 - ASSISTANCE System schema (from ASSISTANCE GA)

Against this backdrop, ASSISTANCE teams will primary applied the ethics and legal constrains and recommendations contained in the following regulatory documents:

- Directive on security of network and information systems (NIS Directive) (Directive (EU) 2016/1148[11]) concerning measures for a high common level of security of network and information systems across the Union.
- Cybersecurity Act (Regulation (EU) 2019/881[12]) of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification, repealing Regulation (EU) No 526/2013.

Going further into the merit of the developed technological system of the project, a special mention for ethics framework needs the uses **UAV** (Unmanned Aerial Vehicle, in the project drones) and **UGV** (Unmanned Ground Vehicle, in the project disaster robots). In the following, some brief elucidations will be provided about the approach of ethics of technology we will adopt to manage the R&D activities in the project with unmanned vehicles, broadly understood, that is aerial + ground, drones and robots.

UAV and UGV

In line with the approach of the European Commission, the project wants to contribute to the development of an ecosystem of UAV and UGV surely supporting the emergence of these promising commercial and technological sectors but with a plain compliance with the most advanced legal and ethics constraints and codes at international level, thus addressing related societal concerns such as safety, security, privacy and environmental protection. The documentary references that lie in the background of our ethical framework (some already mentioned in the legal chapters of this document):

- Opinion of the European Group on Ethics in science and new technologies (EGE) on the ethics of security and surveillance technologies (n°28) which addresses the use of drones for surveillance missions (2014)[13];
- Riga declaration on REMOTELY PILOTED AIRCRAFT (drones) (2015)[14];
- Opinion of the article 29 data protection working party on privacy and data protection issues relating to the utilisation of drones (2015)[15];

More generally speaking, in relation to UAV and UGV, ASSISTANCE ethics approach will follow:

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC
[12] https://eur-lex.europa.eu/eli/reg/2019/881/oj
[13] http://ec.europa.eu/DocsRoom/documents/11493
[14] https://ec.europa.eu/transport/sites/transport/files/modes/air/news/doc/2015-03-06-drones/2015-03-06-riga-declaration-drones.pdf
[15] http://ec.europa.eu/DocsRoom/documents/11481

The on-going procedure of EASA for establishing new rules to ensure that drone operators – whether recreational or professional – will have a clear understanding of what is allowed or not[16];

A set of basic principles and democratic prerequisites, based on the fundamental values laid down in the EU Treaties and in the EU Charter of Fundamental Rights, in line with the Statement on "Artificial Intelligence, Robotics and 'Autonomous' Systems" claimed by the EGE in March 2018[17].

5.2. Relevant Methods for Assessing Ethics Impacts

During the twentieth century, technology development has increasingly become a mean for unlimited and invasive progress. To this regard, many thinkers have criticized the 'instrumental' view of technology based on the idea that technology is per se neutral and can be used for either good or bad purposes[18]. In fact, technologies are not at all *neutral* and can have unforeseen societal and ethical effects: on one hand, smarter technological devices are gradually designing the moral structure of human relationship (the way we talk, feel, build relationship, etc.)[19], on the other hand, technology is steadily more equipped with artificial intelligence and could be shortly transformed into a real political actor.[20]

Therefore, a specialist ethics – the *ethics of technology* – have emerged with the initial scope of guiding the responsibility of those stakeholders directly involved in the design, production and marketing of technological products. As a result, many approaches have been conceived in order to assess the ethical and societal impacts[21] of technological innovations and provide strategies to offset the risks[22] and uncertainties[23] engaging not

[16] https://www.easa.europa.eu/easa-and-you/civil-drones-rpas

[17] http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf

[18] Among others, see: Heidegger M. (1993), The Question Concerning Technology [1949], in Basic Writings, Second Edition, Harper Collins, New York; Marcuse H. (1964), One-Dimensional Man: Studies in Ideology of Advanced Industrial Society, Routledge, London

[19] Verbeek, P.P. (2008). Design ethics and the morality of technological artefacts. In Vermaas et al. (eds.), Philosophy and Design, 95.

[20] Winner L. (1980), Do Artifacts Have Politics?, Daedalus, 109(1), 121-136

[21] Brey P. (2017), Ethics of Emerging Technologies, in: Methods for the Ethics of Technology, S.O. Hansson (ed.), Rowman and Littlefield International, London

[22] For or a 'cultural approach', see: Verbeek P.-P. (2011), Moralizing Technology. Understanding and Designing the Morality of Things, University of Chicago Press, Chicago; for a 'risk approach' see: Haimes Y. (2015), Risk Modeling, Assessment, and Management, 4th ed., Wiley and Blackwell, Hoboken, New Jersey; for a 'techno-political approach, see: Winner L. (1980), Do Artifacts Have Politics?, Daedalus, 109(1), 121-136; social constructivist approach: Latour, B. (1992). Where are the missing masses? In Bijker and Law, 225-258.

[23] Sollie P. (2007). Ethics, Technology Development an Uncertainty: An Outline for Any Future Ethics of Technology. Journal of Information, Communication and Ethics in Society, 5(4), 293-306.

only experts, but the participation of those people that might shape the usability and acceptability of emerging technologies.[24]

In the following an evaluation of main existing assessment frameworks, with their strengths and weaknesses.

5.2.1. Ethical Technology Assessment (ETA)

Ethical Technology Assessment (ETA) describes how ethicists should be involved in current technology development throughout the entire lifecycle of development projects.[25] The aim is that ethicists should act as dynamic sparring partners for technology developers and decision-makers in confronting ethical issues that arise at different stages.

Strengths: Avoid 'crystal ball ambitions' of future developments.
Weaknesses: No predicting consequences

5.2.2. Ethical Impact Assessment (EIA)

Ethical Impact Assessment (EIA) is an approach for assessing the role that specific contexts play in limiting our current understanding of technologies. With such an understanding, decision makers should better be able to think beyond the immediately obvious applications of technologies in development and subject to an EPIA and imagine "how it is used or might be used in the future, not only by itself but as a component in a larger technological framework".[26]

Strengths: Contextualized research on ethical assessment.
Weaknesses: Significant gap between research assessment and application of EIA on the field.

5.2.3. Technology Assessment (TA)

Technology Assessment (TA) is a broad field of scientific and professional activities united by the ambition to help decision-makers harvest the benefits of technological development while avoiding harmful consequences. TA has typically strived for a value-neutral role in between science and society. Despite that there is no universal protocol,

[24] Cotton M. (2014), *Ethics and Technology Assessment: A Participatory Approach*, Springer, Berlin.
[25] Palm, E. and Hansson, S. O. (2006). The case for ethical technology assessment (ETA).Technological forecasting and social change, 73(5), 543-558.
[26] David Wright (2011), *A framework for the ethical impact assessment of information technology*

TA can be described as a broad range of analytical perspectives that try to apply cost-benefit analysis and risk assessment to new technology.[27]

Strengths: Cover a broad spectrum of impacts. Neutral judgment on technology.
Weaknesses: Not considering the role of normative and political powers.

5.2.4. Impact Assessment (IA)

Impact Assessment (IA) is a structured a process for considering the implications of technology, for people and their environment, of proposed actions while there is still an opportunity to modify (or even, if appropriate, abandon) the proposals. It is applied at all levels of decision-making, from policies to specific projects. IA includes as important subsets environmental impact assessment (EIA) and Social Impact Assessment (SIA). Nevertheless, the idea of "impact" is typically defined in consequentialist terms based on rational decision-making model. For this reason, this approach is appreciated and adopted by different international and European conventions as well as international environmental law.

Strengths: Clear analysis of benefits limits directly applicable to reality.
Weaknesses: No addressing societal Challenges. Not adequate for unexpected and long-term consequences.

6. (A)SSISTANCE (LE)gal and E(TH)ics Int(E)grated (I)mpact (A)ssessment (*ALETHEIA*)

6.1. ALETHEIA: Outline

Aletheia (Ancient Greek: *ἀλήθεια*) means "truth" or "disclosure" in philosophy. It is a Greek word variously translated as "unclosedness", "unconcealedness", "disclosure" or "truth". According to Henry George Liddell and Robert Scott's *Greek-English Lexicon*, the literal meaning of the word *ἀ–λήθεια* is "the state of not being hidden; the state of being evident.[28]" It also means factuality or reality

The well-known German philosopher Martin Heidegger has revised in the 20th century the meaning of *aletheia*. In his masterpiece *Being and Time* (German: *Sein und Zeit*,

[27] Decker, M. (eds.) (2001) *Interdisciplinary in Technology Assessment Implementation and its Chances and limits*. Springer, Berlin
[28] Henry George Liddell. Robert Scott. A Greek-English Lexicon. revised and augmented throughout by. Sir Henry Stuart Jones. with the assistance of. Roderick McKenzie. Oxford. Clarendon Press. 1940.

1927)[29], Heidegger demonstrated that the propositional truth is only the lowest level of truth, taken to be as a mere logical correspondence or agreement between a proposition and a being. There is also a more extend and imperceptible level of truth that refers not to the appearance of the beings, but rather the *Being* of these appearance. It refers to the event, or to the fact or the dynamics of openness itself which makes possible reality's own openness to beings and the openness of beings themselves.

We infer from these philosophical meanings the conceptual background of the impact assessment method that will be applied in the ASSISTANCE to assess the ethics landscape and the legal compliance of the project development. In the same way as Heidegger's philosophical formulation, **ASSISTANCE ALETHEIA *aims to bring to light the evidence of the facts (risks and opportunities) that determine the apparent complexity of a reality, so that the assessing judgment can be a comprehensive act as refined as possible***.

In fact, making an impact assessment of something always involves an assumption of value. No evaluation is a completely neutral act. The non-neutrality of an evaluation manifests itself both with respect to its *genesis* and to its *application*. Genesis: The types of moral and legal principles as well as the ethical visions of the world from which assessments arise are culturally oriented. Application: every evaluation, when introduced into the world of the facts, contributes not only to interpret the world but also to build it, to give the world meaning and structure.

But the non-neutrality of an evaluation must not lead to arguing in favor of an ethical and legal relativism. We need to make assessments to govern the complex processes of reality, especially when these processes take place by devices and systems that we humans have built.

And then?

In order to respond to these preliminary assumptions, ALETHEIA will be applied in this project as method to make integration of different components and accounts of impact assessment. The trend to "integrated" models of impact assessment is an increasingly sustained approach in the scientific debate, at least for three reasons[30]: (1) since "everything is inherently interconnected", "a complete understanding of all the impacts can only be achieved by a comprehensive and integrated assessment"[31]; (2) efficiency

[29] M. Heidegger (1927). Being and Time. New York: Harper and Row, 1962

[30] An example of challenging attempt to try to define an ethics and privacy impact assessment method able to integrate different models is being tested in the EU PERSONA project, see: http://persona-project.eu/.

[31] Vanclay, F. (2004). The triple bottom line and impact assessment: How do TBL, EIA, SIA, SEA and EMS relate to each other? Journal of Environmental Assessment Policy and Management, 6(3), 265–288.

"in terms of monetary and time resources", and inclusion of the aspects not legally required in the types of assessments that are required by law (i.e. "greater visibility of voluntary impact assessments by piggy-backing on those that are legally mandated")[32].

The accounts (with specific functions) that form ALETHEIA are:

6.1.1. Data Protection Impact Assessment (DPIA)

This model of impact assessment serves us both in the proper sense and in a translated way. In a strict sense, the protection of personal data is one of the most important legal and ethical aspects for monitoring and evaluating a project like ASSISTANCE. Accordingly, ALETHEIA will analyze the different phases of the project and constantly monitor its impacts in order to understand if a DPIA is necessary and, if necessary, it will be provided.

The methodology to conduct a DPIA has its starting point in the WP248 rev.01 – Annex 1, that suggests some generic frameworks, in the specific context of "Personal Data Protection". An integrated approach will be taken, in keeping with the criteria of the WP29-Guidelines and, when compatible, with the international standards on risk management (such as [ISO 31000]).

6.1.2. DPIA for processing legal and ethical issues at large

The DPIA offers an additional tool. Its processing phases are well constructed[33] and can be adopted even beyond the data protection field. Therefore., we will adopt the DPIA structure as metric to evaluate ALL the ethical and legal aspects of the project.

6.1.3. Contextual model of ethics impact assessment

As mentioned above, making an impact assessment is never neutral. This assumption becomes unquestionably more significant and important when we must make an evaluation of the ethical impact. In this case the assumption of value is even double: (1) as an act of evaluating as such and (2) referring to what is evaluated. Against this backdrop, ALETHEIA is based on an open approach. The ethics background on which the impacts will be able to affect is contextual and constructive. It depends on the criteria by which it is defined and according to the principles and purpose it intends to promote. To this end, any judgment or evaluation or assessment on possible impact of ASSISTANCE developments will be made according to the ethics coordinates within

https://doi.org/10.1142/9789814289696_0006.

[32] Tajima, R., & Fischer, T. B. (2013). Should different impact assessment instruments be integrated? Evidence from English spatial planning. Environmental Impact Assessment Review, 41, 29–37. https://doi.org/10.1016/j.eiar.2013.02.001.

[33] On this, see: Kloza, D., van Dijk, N., Casiraghi, S., Vazquez Maymir, S., Roda, S., Tanas, A., & Konstantinou, I. (2019). Data protection impact assessments in the European Union: designing an appraisal method towards a more robust protection of individuals (forthcoming). D.Pia.Lab Policy Brief, VUB, 2, 4.

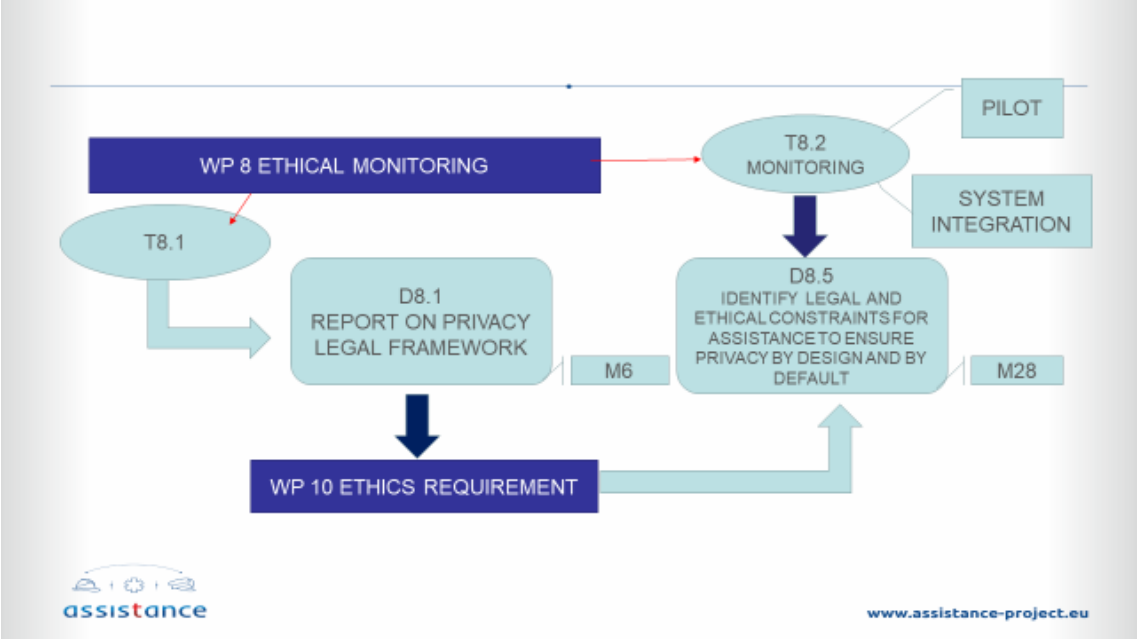
which the specific impact takes place, as effective risk or opportunity. These coordinates are deduced by the most advanced contemporary types of ethics.

- An **ethics of the scope** (consequentialism = right or wrong depend on the consequences of the action)
- An **ethics of the rule** (deontology = based on whether the action itself is right or wrong under a series of rules, regardless the consequences)
- An **ethics of virtue** (ethics depends neither from duties nor from consequences, rather from the moral character of the action, that is the capacity to create happiness, flourishing, well-being, awareness in people)

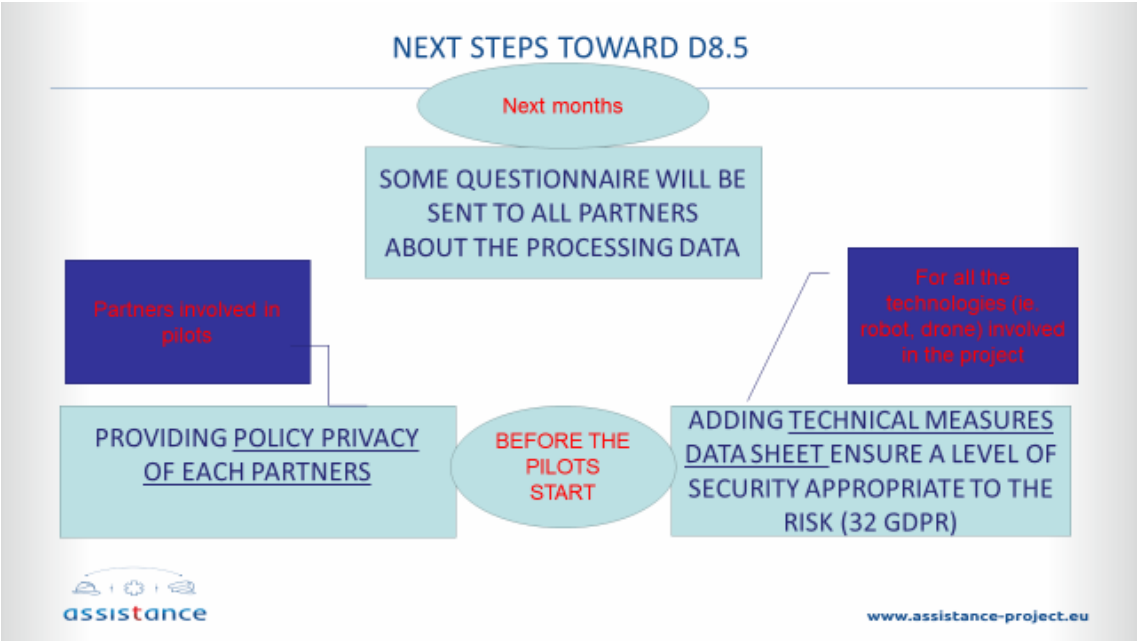
6.2. ALETHEIA: Processing

6.3. ALETHEIA: Processing

Starting from the above-mentioned legal and ethical framework, the following figures would illustrate the next step monitoring process.



The next activities that are deemed necessary to carry out a proper monitoring of the project are shown in the figure below.


NEXT STEPS TOWARD D8.5
Next months
SOME QUESTIONNAIRE WILL BE SENT TO ALL PARTNERS ABOUT THE PROCESSING DATA
Partners involved in pilots
For all the technologies (ie. robot, drone) involved in the project
PROVIDING POLICY PRIVACY OF EACH PARTNERS
BEFORE THE PILOTS START
ADDING TECHNICAL MEASURES DATA SHEET ENSURE A LEVEL OF SECURITY APPROPRIATE TO THE RISK (32 GDPR)
assistance
www.assistance-project.eu