This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 832981

Deliverable D8.1

Legal and Ethical State-of-the-Art on CBRNe preparedness and response

Due date of deliverable: 31/12/2019

Actual submission date: 15/03/2021

Gemma Galdon Clavell[1], Miguel Ángel Valbuena León[1], Mariano Martín Zamorano[1], and Irina Marsh[2]

1: ETICAS 2: CBRNE Ltd

Project details

Project acronym	PROACTIVE
Project full title	**PR**eparedness against CBRNe threats through c**O**mmon **A**pproaches between security pra**CTI**tioners and the **V**ulneranb**lE** civil society
Grant Agreement no.	832981
Call ID and Topic	H2020-SU-SEC-2018, Topic SU-FCT01-2018
Project Timeframe	01/05/2019 – 30/04/2022
Duration	36 Months
Coordinator	UIC – Grigore Havarneanu (havarneanu@uic.org)

Document details

Title	Legal and Ethical State-of-the-Art on CBRNe preparedness and response
Work Package	WP8
Date of the document	15/03/2021
Version of the document	05
Responsible Partner	ETICAS
Reviewing Partner	PHE, CBRNE Ltd, and UIC
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	12/12/2019	First Draft
02	17/12/2019	Reviewed by PHE and CBRNE Ltd.
03	19/12/2019	Draft reviewed by UIC
04	20/12/2019	Final version
05	15/03/2021	Update following mid-term periodic review

Consortium – List of partners

Partner no.	Short name	Name	Country
1	UIC	UNION INTERNATIONALE DES CHEMINS DE FER (COORDINATOR)	France
2	CBRNE	CBRNE LTD	UK
3	PPI	POPULATION PROTECTION INSTITUTE (MINISTRY OF THE INTERIOR OF THE CZECH REPUBLIC)	Czech Republic
4	DB	DEUTSCHE BAHN AG	Germany
6	UMU	UMEA UNIVERSITET	Sweden
7	DHPOL	DEUTSCHE HOCHSCHULE DER POLIZEI	Germany
8	RINISOFT	RINISOFT LTD	Bulgaria
9	WMP	WEST MIDLANDS POLICE AND CRIME COMMISSIONER	UK
10	ETICAS	ETICAS RESEARCH AND CONSULTING SL	Spain
11	SESU	STATE EMERGENCY SERVICE OF UKRAINE	Ukraine
12	PHE	DEPARTMENT OF HEALTH	UK
13	SPL	STATE POLICE OF LATVIA	Latvia
14	AGS	AN GARDA SÍOCHÁNA – NATIONAL POLICE FORCE IRELAND	Ireland
15	FFI	FORSVARETS FORSKNINGSINSTITUTT	Norway
16	NPH	KOMENDA GŁÓWNA POLICJI	Poland

List of acronyms

Acronym	Definition
EU	European Union
CBRNe	Chemical, Biological, Radiological, Nuclear, and explosive
LEA	Law Enforcement Agency
GDPR	General Data Protection Regulation
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
T	Task
M	Month
D	Deliverable
WP	Work Package
FAIR	Findable, Accessible, Interoperable and Reusable
IPR	Intellectual Property Rights
PII	Personally Identifiable Information
DPO	Data Protection Officer
PEO	Project Ethics Officer
SAB	Security Advisory Board
CSAB	Civil Society Advisory Board
EEAB	External Ethical Advisory Board
DOI	Digital Object Identifier
UNE	Asociación Española de Normalización (Spanish Association for Standardization).
SOP's	Standard Operating Procedures
EEA	European Economic Area
SSH	Social Sciences and Humanities
CSCs	Crisis Standards of Care

Executive summary

This deliverable is aimed at providing the PROACTIVE consortium with the following:

- An overview of the main human rights that are relevant in the PROACTIVE project;
- An overview of the applicable legal precepts concerning privacy and data protection;
- A review of the legal and policy frameworks through which CBRNe events are regulated in the European Union;
- An ethical framework for PROACTIVE fieldwork and research studies, which draws from a comprehensive review of the literature on ethics in disaster management and elaborates on what has been established in D7.4 *Data Management Plan and Research Ethics*;
- A compilation of summaries of CBRN guidelines documents from Germany (case study).

It is described in the DoA in the following way:

> "*This Deliverable provides a mapping of legal requirements and ethical standards at the EU level. It will offer a comprehensive and holistic understanding of the legal framework as well as ethical principles that will guide the project development, including requirements on protection of personal data. The ethics requirements regarding humans (requirement 1) and the protection of personal data (requirements 6–7) are transferred to WP10 and covered in deliverables D10.1, D10.6 and D10.7, as per post-grant requirements*."

By considering the content included in this deliverable, PROACTIVE partners will be able to carry out their research activities in a legal and ethical manner. The content of this deliverable is meant to inform the content of D8.2 (Legal and acceptability recommendations for PROACTIVE toolkits), along with the ethical requirements included in WP10.

Table of Contents

List of Tables

1. INTRODUCTION

PROACTIVE is an EU funded project within the H2020 framework, addressing topic SU-FCT01-2018-2019-2020: Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism. It began on the 1st of May 2019 and it will finish on the 30th of April 2022.

PROACTIVE aims to increase practitioner effectiveness in managing large and diverse groups of people in a chemical, biological, radiological, nuclear and explosive (CBRNe) environment. The main goal is to enhance preparedness against and response to a CBRNe incident through a better harmonisation of procedures between various categories of practitioners, and a better articulation with the needs of vulnerable citizen groups.

PROACTIVE will result in toolkits for CBRNe Practitioners and for civil society organisations. The toolkit for Practitioners will include a web collaborative platform with database scenarios for communication and exchange of best practices among Law Enforcement Agencies (LEAs) as well as an innovative response tool in the form of a mobile app. The toolkit for the civil society will include a mobile App adapted to various vulnerable citizen categories and pre-incident public information material.

PROACTIVE is divided into ten Work Packages (WPs). This document is the first deliverable within Work Package 8 (Legal, Ethical and Acceptability Requirements) and is based on work carried out in Task 8.1.

Both T8.1 and D8.1 are defined in the Grant Agreement (GA) as follows:

Task 8.1 – Legal and ethical state-of-the-art on CBRNe preparedness and response

Leader: ETICAS. Participants: CBRNE, PHE, FFI

Duration: M1 – M8

The purpose of this task is twofold. On the one hand, a legal assessment of the entire project will be performed. On the other hand, the societal implications of the proposal will also be accounted for. In order to accomplish the first section, the legal framework that will inform the project as a whole will be laid down. These applicable legislations will be analysed during the first 6 months in order to provide the rest of the members of the Consortium with a roadmap that enables them to be acquainted with the legal framework and its logic. This analysis will also include a thorough examination of case studies corresponding to different Member States, the review of similar projects and their normative aspects and the description of LEAs best practices. This analysis permit to:

• Anticipate and minimize potential data protection issues. In order to secure conformity with national regulations, a data controller will be appointed for each participating country, and it will act as an interface with the relevant Data Protection Authority, in case is required.

• Consider and monitor ethical compliance of the proposed mechanisms, anticipating differential impacts on vulnerable citizens.

This legal dimension of our work will be present at all times throughout the unfolding of the project and will be updated in D8.4 if needed. The ethics requirements regarding humans (requirement 1) and the protection of personal data (requirements 6–7) are transferred to WP10 and covered in deliverables D10.1, D10.6 and D10.7, as per post-grant requirements.

D8.1 Legal and ethical state-of-the-art on CBRNe preparedness and response (ETICAS, M8, R, PU)

This Deliverable provides a mapping of legal requirements and ethical standards at the EU level. It will offer a comprehensive and holistic understanding of the legal framework as well as ethical principles that will guide the project development, including requirements on protection of personal data. The ethics requirements regarding humans (requirement 1) and the protection of personal data (requirements 6–7) are transferred to WP10 and covered in deliverables D10.1, D10.6 and D10.7, as per post-grant requirements.

D8.1 is to be handed in M8, with the ethical requirements contained within WP10. As it is said in the description of this deliverable, the aspects covered in WP10 will be covered extensively within the requirements. Nevertheless, all aspects that are relevant from a legal standpoint are, at least briefly, tackled within this deliverable.

It is important to take into account the fact that a number of issues that had already been addressed within D7.4 (Data Management Plan and Research Ethics) are also addressed in this deliverable. These mainly have to do with data protection requirements.

D8.1 includes a section describing the PROACTIVE Ethical framework (section 3), which aims to support the consortium partners in identifying ethics requirements in regards to CBRNe response at the EU level, focusing on emergency assistance for vulnerable groups. The PROACTIVE ethical framework is based on a comprehensive literature review of disaster ethics (including CBRNe incidents) and aims to provide input to the scenario development and evaluation methodology (WP6) and to inform the consortium partners of

the PROACTIVE ethical governance framework, which will guide the research activities and evaluations of procedures and tools (WP8 and WP10).

This document is public, so it will be published by the PROACTIVE consortium in the hope that it will be useful outside of this consortium.

1.1. Objectives

In terms of the objectives established by the deliverable, the objectives of WP8 are the following according to the GA:

> This WP is aimed at developing the legal framework and establishing the ethical principles to be followed by the consortium. With that end in mind, we will define concrete mechanisms to ensure compliance. Therefore, the main objectives of WP8 are:
>
> • **To point out and frame the ethical and legal aspects of PROACTIVE,**
>
> • **To examine the legal, ethical and societal aspects in PROACTIVE from both Privacy by Design and post assessment approaches,**
>
> • To provide stakeholders and partners with the appropriate guidance on the above aspects,
>
> • To carry out an acceptability study for the proposed toolkits in order to assure its sustainability,
>
> • To avoid any negative social impact during the project's execution or in future deployments based on this research.
>
> WP8 runs in parallel with the lapse of the project. The legal, ethical and societal impact assessment is conducted as a cyclical process linked to the overall project strategy, starting at the earliest stages and being revisited at each new project phase. This approach guarantees an early alert on every issue, thus avoiding the risk of having to redesign significant aspects of the proposal for optimisation from the citizen perspective that have already been devised. In order to protect the privacy and integrity rights of the participants in the project, a number of best practices principles will be observed (see Section 5).
>
> The WP8 will also gauge, from a social perspective the emerging socio-technical solutions identified by the project, which should be oriented towards supporting human decision-making. They should also take into account the experiences of citizens, whose problems are the ultimate reason why emergency services exist.
>
> Outputs of this WP will be used in all project WPs. WP2, WP3 and WP6 will give inputs to this WP.

The two first objectives (in bold) are the ones addressed in this deliverable. They are accomplished by this deliverable in combination with D7.4 and the ethical/legal requirements included in WP10.

1.2. Description and structure

This deliverable is divided into the following sections:

- **Section 2 (Legal and policy frameworks)**: This section encompasses the legal frameworks on human rights and data protection, as well as the policy and legal frameworks at the European level concerning CBRNe. At this stage of the project, the legal frameworks are meant to enable the project to carry out its research activities legally. Onene of the main objectives is to ensure that the participants' data protection rights are guaranteed at all times. For its part, the CBRNe legal and policy frameworks described here within are done so with an aim to facilitate the understanding of the importance that the PROACTIVE project has within the wider field of CBRNe in Europe.

- **Section 3 (PROACTIVE Ethical framework):** Drawing from what has been established in D7.4 and a comprehensive review of the literature on ethics in disaster management, this section provides an ethical framework to be observed during the fieldwork activities and the project as a whole.

- **Section 4 (National CBRNe guidelines. The case of Germany):** A set of guidelines coming from Germany, a country where one of the field exercises will be conducted, is examined.

- **Section 5 (Conclusion):** This section wraps up the deliverable and sets out a way forward as far as how to deal with the ethical and legal aspects of the PROACTIVE project.

- **Section 6 (References).**

It has already been established that the main purpose of this deliverable is to provide the legal and ethical framework that is relevant for the PROACTIVE project. The main frameworks that are analysed in order to create PROACTIVE's legal and ethical framework are the following:

1. Human rights;

2. Privacy and data protection;

3. CBRNe.

The relevance of human rights within PROACTIVE is determined by the fact that one of the fundamental principles of ethical research is that the participant's human rights have to be ensured at all times. Furthermore, PROACTIVE intends to involve vulnerable individuals in field exercises in order to assess their particular needs and, thus, improve the response

capacity of end-users. As a result of that, the role of human rights becomes even more salient within the project.

The human rights to privacy, protection of personal data, non-discrimination and integrity have been identified as the most relevant ones for this project. These four human rights are examined in section 2.1 (Human rights). Three different pieces of legislation have been consulted in order to construct this framework:

- Charter of Fundamental Rights of the European Union
- European Convention on Human Rights
- Universal Declaration of Human Rights

2. LEGAL AND POLICY FRAMEWORKS

The role of this section is to provide a general outlook of the principles that should inspire both the research activities carried out within the project and the toolkits that will result from it.

The second framework that is analysed within this deliverable is privacy and data protection. The basic framework within the European Union in terms of privacy and data protection is the General Data Protection Regulation (GDPR), which is the main piece of legislation analysed in section 2.2.

Personal data will be gathered and processed within the project in order to carry out the research. It will also be processed by the application developed as part of the project's toolkits, which will be aimed at facilitating communications between the victims of CBRNe attacks and first responders, among other things. In addition to that, some of that data will be sensitive, which is required for the research to achieve a number of its goals, such as finding out more about the specific needs of different categories of vulnerable individuals in CBRNe events. This calls for the consortium to establish and implement adequate data protection policies and measures. Section 2.2 aims at establishing the main legal precepts that have to be complied with, which will then be translated into specific recommendations in D8.2, and which have been partially addressed in D7.4.

Lastly, this deliverable includes a comprehensive review of the EU's policy framework in which CBRNe events are framed. This framework is predominantly composed of "soft law" rather than binding legal instruments. This body of soft law is mainly composed of agreements, action plans, and strategies. Therefore, the review of the CBRNe policy framework will provide the consortium with an overview of the context in which CBRNe incidents are perceived and acted upon. This enables the consortium to better understand where PROACTIVE stands within the broader field of CBRNe intervention.

2.1. Human rights

2.1.1. Right to integrity

The right to integrity, defined in the following manner, is relevant when considering that the field exercises carried out within PROACTIVE will expose research participants to conditions that might have a detrimental effect on their physical and mental integrity due to the nature of live-action field exercises:

Charter of Fundamental Rights of the European Union

Article 3:
1. Everyone has the right to respect for his or her **physical and mental integrity**.

2. In the fields of medicine and biology, the following must be respected in particular:

(a) the free and informed consent of the person concerned, according to the procedures laid down by law;

(b)the prohibition of eugenic practices, in particular those aiming at the selection of persons;

(c) the prohibition on making the human body and its parts as such a source of financial gain;

(d) the prohibition of the reproductive cloning of human beings.

Therefore, one of WP8's future deliverables, D8.3, will include measures aimed at preserving the participants' mental and physical integrity during the field exercises carried out within PROACTIVE.

The importance of human rights within PROACTIVE is especially salient due to the presence of individuals belonging to vulnerable groups. These individuals need extra attention and care to have their human rights respected precisely because of their vulnerabilities. Along these lines, D7.4 (Data Management Plan and Research Ethics) and D8.3 (Materials and briefing for PROACTIVE exercises) are aimed at putting in place measures intended to guarantee that their participation in PROACTIVE's research activities takes place in a way that is not detrimental to the protection of their human rights. This includes specific precautions in terms of environment and safety which will be reflected in the mentioned deliverables and monitored by ETICAS during the development of fieldwork activities.

2.1.2. Right to privacy

To fully understand what the right to privacy entails, and how the research activities carried out within PROACTIVE might affect it, the following definitions in various international instruments are of relevance:

Charter of Fundamental Rights of the European Union.

Article 7:
Everyone has the right to respect for his or her private and family life, home and communications.

European Convention on Human Rights.

Article 8:
1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Universal Declaration of Human Rights.

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

The right to privacy is **not an absolute right**, but a conditional one; someone's privacy might be breached for legitimate purposes, in a proportional manner. The European Convention on Human Rights hints towards this in its second paragraph. Therefore, PROACTIVE must deal with the research participants' personal data in a proportional manner and according to the legal standards on data protection.

The right to the protection of personal data, if not to be extensively developed in this section, is worth mentioning too:

Charter of Fundamental Rights of the European Union

Article 8:
1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person **concerned or some other legitimate basis laid down by law. Everyone has the right of access** to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

This article emphasises the principle of **purpose limitation and two of the data protection rights that people enjoy in the European Union**, namely the right to access and rectification. The right to data protection is detailed in the General Data Protection Regulation, which constitutes the main regulatory framework on the topic in the European Union.

Furthermore, **non-discrimination** has been identified by the consortium as a fundamental value in PROACTIVE within the context of the processing of research participants' personal data belonging to vulnerable categories of the population. The right to non-discrimination has been defined in the following ways by different international legal documents:

Charter of Fundamental Rights of the European Union.

Article 21. Non-discrimination:
1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.

European Convention on Human Rights.

Article 14. Prohibition of discrimination:
The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Article 1. General prohibition of discrimination (Protocol No. 12):
1. The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

2. No one shall be discriminated against by any public authority on any ground such as those mentioned in paragraph.

Universal Declaration of Human Rights.

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

PROACTIVE has carefully considered all the potential implications that the processing of sensitive information may have for individuals belonging to the above-mentioned collectives. As a matter of fact, one of the core aims of the project is to provide practitioners with valuable insight on how to deal with vulnerable people in the event of a CBRNe crisis. Potential discriminatory treatment during the research will be avoided through the recommendations established in D8.3.

An important aspect that must be taken into consideration within PROACTIVE is how the project will ensure the human rights of the vulnerable people partaking in the project. This is due to the fact that the PROACTIVE project will involve up to 15% of vulnerable individuals in the field exercises in order to allow a better understanding of their needs during a CBRN crisis and validate the PROACTIVE toolkits. Their feedback will be taken into consideration at all times in the project and will be gathered during workshops, interviews and through the interventions of the CSAB.

The vulnerable groups that are expected to be included in the field exercises are disabled people, minors, members of religious minorities and the elderly. However, prior to that, it is necessary to discuss how these vulnerable groups are legally defined in order to have some solid criteria when grouping people into categories. Other vulnerable groups that might participate in the exercises are pregnant people, people with chronic illnesses and others as it is established in the DoA. If they end up participating, their vulnerabilities will be properly taken into account as well.

Minors/Children

Article 1 of the Convention on the Rights of the Child defines a child in the following way:

Article 1

For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

Therefore, children/minors will be those that are under the age at which legal capacity is acquired. According to the European Union Agency for Fundamental Rights, the age of majority is 18 years in all EU Member States except for Scotland, where children are considered to have full legal capacity from the age of 16 years.

People with disabilities

The Convention on the Rights of Persons with Disabilities, an international human rights treaty that was accepted by the EU in 2010, provides a definition in its first article.

> **Article 1**
>
> The purpose of the present Convention is to promote, protect and ensure the full and equal enjoyment of all human rights and fundamental freedoms by all persons with disabilities, and to promote respect for their inherent dignity. Persons with disabilities include those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others.

At the European level, the Charter of Fundamental Rights of the European Union affirms the right of disabled people not to be discriminated against on the basis of their disability as it is discussed previously.

Members of religious minorities

It is difficult to find a legal definition of what constitutes a religious minority, probably given the difficulty that establishing such definition entails. The Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities establishes the following:

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

Given the lack of a proper definition of what constitutes a religious minority in international law, we can say that for the purposes of PROACTIVE people belonging to religious minorities are those that profess a religion different to that of the majority of the population of the country in question. As established in the Declaration, people belonging to religious minorities have the right to profess their religion and participate in society without being discriminated against. Therefore, PROACTIVE will need to ensure that that is the case and attempt to include these considerations when developing the toolkits and outcomes of the project in order for CBRNe response to be in alignment with human rights.

The elderly

Regarding the elderly, the Charter of Fundamental Rights of the European Union establishes the following:

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

Although there is no legal definition of "the elderly", Eurostat considers elderly people as those who are above 65 years old. The PROACTIVE project will take that same approach.

The intersection between PROACTIVE and human rights is a very relevant one since one of the main aims of the project is to develop response protocols that take into account the needs of vulnerable people in the event of CBRNe events. Not only do the research activities must be carried out in a way that guarantees that these are respected, but also the outcomes of the project (including the various toolkits developed as part of it) must ensure that the rights of vulnerable people are guaranteed.

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

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

Therefore, D8.3 will include measures aimed at preserving the participants' mental and physical integrity during the field exercises carried out within PROACTIVE.

When it comes to vulnerable groups, PROACTIVE addresses the issue of ensuring their human rights in two manners. First, the actual PROACTIVE toolkits are oriented towards improving the efficiency of first response activities during CBRNe attacks concerning these groups. Second, D7.4 (Research Ethic Protocols) and D8.3 are aimed at putting in place measures intended to guarantee that their participation in PROACTIVE's research activities takes place in a way that is aligned with human rights.

2.2. Data protection

In this section, relevant data protection regulations will be described and analysed in order to frame their implications for PROACTIVE's design and deployment. The examination is focused on the GDPR since this text reflects the newest standard for data protection and includes the main requirements of PROACTIVE to lawfully process personal data.

2.2.1. The General Data Protection Regulation (EU GDPR)

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

Article 2

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

2. This Regulation does not apply to the processing of personal data:

a. in the course of an activity which falls outside the scope of Union law;

b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

c. by a natural person in the course of a purely personal or household activity;

d. by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

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

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

Article 3

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

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

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

The PROACTIVE consortium is composed of organisations that are mostly based in countries belonging to the European Union or the European Economic Area (EEA) that will process personal data belonging to data subjects also based within those areas for research purposes. The only exception to that is SESU (State Emergency Service of Ukraine), a partner that is based in Ukraine, a country that is not currently a member of the European Union. Nevertheless, even this partner must abide by the GDPR given that the personal data it may process as part of PROACTIVE belongs to data subjects whose data is being monitored for research purposes within the Union (Article 3.2). In addition, the joint controller's agreement obliges this partner to at least meet the minimum requirements established in it, which will ensure a minimum standard of compliance.

In spite of the fact that some members of the consortium are Law Enforcement Agencies (LEA's), they will not be processing personal data for 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, which means that Directive (EU) 2016/680 of the European Parliament and of the Council (known as the Police Directive) does not apply within PROACTIVE.

In light of the above, the GDPR and its national developments in the different member states constitute the main applicable legislation in terms of personal data.

Personal data

As briefly mentioned above, the protection of personal data is considered a fundamental right in the European Union, and its main legal framework consists of the GDPR. Given that PROACTIVE does process personal data, a framing of this right is required. First of all, personal data is defined in article 4 as such:

Article 4 (1):

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

The subjects of the data protection rights granted by the GDPR are defined as data subjects, who are natural persons to whom data can be linked. Correctly identifying what data are personal data for data subjects is of the utmost importance for the legal analysis of PROACTIVE's outcomes and research process. **Personal data can be any information that either identifies or allows for the identification of natural persons**. The GDPR gives a number of examples but does not provide a comprehensive list. This is due to the fact that even data that seems to not be problematic from a data protection standpoint has proven to allow for the identification of individuals (Narayanan and Shmatikov, 2008).

The PROACTIVE consortium will be processing mainly data coming from:

- Representatives and contact points from members of the AB's.
- Research participants involved in the field exercises carried out within the project, some of them belonging to vulnerable categories of the population.

D7.4 includes a data summary in which an overview of the data processed within the project is provided. The data summary includes both personal data and non-personal data. It identifies a number of data points concerning the types of data processed within PROACTIVE, such as the following:

- WP/T within which data will be collected.
- Partner mainly responsible for the collection of the data.

In order to minimise the risks of handling the above data, for instance concerning their misuse, there are a number of ways in which data can be protected. One of these is to pseudonymise data, which is a process the GDPR defines as:

Article 4(5):

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

This is a general definition that the Working Party Article 29 (WP29) has provided an opinion on (Article 29 Data Protection Working Party, 2012), to detail further. Pseudonymisation guarantees a lower level of knowledge about an individual to re-identify this person in a database. Depending on the criticality of the database, this technical method of protecting data might be sufficient. It must be emphasised, however, that pseudonymised data remains personal data, and still falls within the scope of the GDPR.

Anonymised data, on the other hand, is not considered personal data by the GDPR. It is defined as:

> **Recital 26:**
>
> [...] The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Anonymisation consists of **altering the dataset containing personal data in a manner that makes it theoretically impossible to re-identify individuals**. There are various ways to alter a dataset, which can consist of grouping individuals according to certain common attributes, deleting certain fields, replacing fields with false data that are similar, making the data less precise, etc. These are also further ways which were discussed by the WP29 (2014). Anonymisation has to be distinguished from pseudonymisation, with the main different pertaining to the impossibility of re-identify individuals.

The anonymisation points and the methods of anonymisation used in each case are described in D10.5, where the technical and organisational measures that are implemented to safeguard the rights and freedoms of the data subjects/research participants are discussed. This process is particularly relevant since it involves changes in the legal status of data (Recital 26 GDPR), but also because it is one of the most important security measures for sensitive data to be conducted as part of PROACTIVE and its data life cycle. Moreover, with the exception of prior approval given via the use of informed consent, in order to disclose personal information to third parties requires it to be anonymised beforehand.

The consortium has decided not to adopt a unified approach to anonymisation and pseudonymisation. Instead, each member of the consortium that has been tasked with implementing such measures and will share information will be reflected in D10.5.

2.2.1.1. Special categories of data

As mentioned above, some of the activities to be carried out in PROACTIVE require the processing of sensitive personal data, namely data belonging to special categories as reflected in D7.4. The categories of personal data that are considered to be sensitive are described in Article 9.1 GDPR:

> **Article 9.1**
>
> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

The personal data belonging to some of these categories (ethnic origin, religious beliefs, and data concerning health) must be processed in accordance with what is established in D7.4 and this deliverable and for the purposes established in D10.4.

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

Article 9.2:

2. Paragraph 1 shall not apply if one of the following applies:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e. processing relates to personal data which are manifestly made public by the data subject;
f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant

to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

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

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

Taking the above into consideration, the **processing of sensitive personal data is not prohibited but subjected to further safeguards.** The sensitive data used for research purposes will be processed on the basis of informed consent in all cases in PROACTIVE. Sensitive data may also be processed by the App to be developed by RINISOFT if that is absolutely critical for the functionality of the service also on the basis of consent (T4.3). Furthermore, as established in Article 9.2 g) GDPR, this type of processing shall be "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". In brief, **the management of special categories of data by the PROACTIVE project must be based on one of the requirements stated above and their controllers/processors (see next section) must establish special security measures for their treatment,** which may include anonymisation, encryption, strong user authentication, and backup solutions or data erasure.

A summary of the types of sensitive data that are going to be collected within PROACTIVE can be found in D7.4. Information is provided in the form of a table that gives the following information regarding the different types of sensitive personal data collected within the project:

- Type of sensitive personal data;
- Partner responsible for data collection;
- Partners or entities with which data are shared;
- Purpose for data processing;
- Basis for processing;
- WP/T concerned.

The questionnaires that were circulated during the process of elaboration of D7.4 were intended to raise awareness on the importance of adopting appropriate security measures when processing sensitive personal data. Especially relevant is the purpose for which these data are collected, mainly in terms of complying with the principle of data minimisation, which obliges controllers to only collect the amount of personal data that is strictly necessary for achieving their purposes. Along these lines, D10.4 establishes the purpose behind the collection and processing of all the types of data collected within the project to ensure that no extra personal data is being collected and processed, which is especially important when dealing with personal data belonging to special categories.

Regarding further mitigating measures, they will be addressed in the updated version of D7.4 that will be turned in due M18. A member of the External Ethical Advisory Board (EEAB) highlighted the importance of adopting further preventive measures when dealing with these types of data, which prompted the consortium to start addressing this particular issue. In particular, CBRNE Ltd., UmU, DHPol, and PHE are the partners more concerned by this as they will mostly gather and process the data.

2.2.1.2. Roles

It is crucial to be clear on the roles and corresponding responsibilities of the different actors in the GDPR and in the PROACTIVE project.

The data controller is the key role in data processes involving personal data, as it is the entity that bears most of the responsibility for what happens to personal data. What a controller is defined in Article 4(7):

Article 4(7):

'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

The responsibilities of the controller, on the other hand, are defined in article 24:

Article 24:

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 24 does not provide an exhaustive list of all the obligations of the controller. The following are also relevant:

- Transparent information, communication, and modalities for the exercise of the rights of the data subject (Article 12 GDPR);
- Data protection by design and by default (Article 25 GDPR);
- Obligation to only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject (Article 28 GDPR);
- Records of processing activities (Article 30 GDPR);
- Security of processing (Article 32 GDPR);
- Notification of a personal data breach to the supervisory authority (Article 33 GDPR);
- Communication of a personal data breach to the data subject (Article 34 GDPR);
- Data protection impact assessment (Article 35 GDPR);
- Prior consultation (Article 36);
- Designation of the data protection officer (Article 37 GDPR);
- Transfers subject to appropriate safeguards (Article 46).

Concerning the obligation to keep records of processing activities, it does not always apply. Article 5 GDPR establishes the situations in which the obligation of keeping records will apply in the following manner:

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

Therefore, **at least the partners that will process personal data belonging to special categories** (among them CBRNE Ltd., Umea University, PHE, and DHPol) **will need to keep records of the processing activities that involve data belonging to special categories**.

The consequences of not complying with the regulations for controllers are established in Articles from 82 to 84. Data subjects who have their data protection rights harmed as a result of a lack of compliance of the controller have the right to be compensated. Furthermore, violations of the regulation can result in administrative fines and penalties.

The controller is not necessarily the only entity processing personal data. Other entities can also process personal data on behalf of the controller. These are called processors and are defined as such:

Article 4(8):

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

The processor does not decide on the purposes or the means to process data themselves, as it is established in Article 28.2, which also asks the processor to not engage other processors without having an authorisation from the controller:

Article 28.2:

The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

In order for the terms by which the relationship between the controller and the processor must abide to be as clear as possible, the GDPR has established that the purposes and means of the processing have to be established in a document or other legal act that is binding on the processor.

Article 28.3:

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

The terms of such agreement must not be breached by the processor unless Union or Member state law asks them to do so.

Article 29:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

As well, controllers must keep records of the processing activities it has carried out on behalf of the controller. Such records need to include a certain number of categories, including information on the data controllers on behalf of which a given processor is processing data, the categories of data being processed, the policy on data transfer and information on technical and organisational security measures.

Article 30.2:

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

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

The above articles establish the main obligations of data processors. In general, data processors are responsible for supporting the controller in order to comply with the GDPR, not processing data for different purposes or by different means than those established by the controller, keeping records of their processing activities and, in general, abiding by the terms agreed with the controller.

In certain cases involving the processing of a certain amount of personal data, or when the processing is a special kind of entity, the appointment of a Data Protection Officer (DPO) by said entity is required, as per article 37.1 of the GDPR:

Article 37.1:

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

a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c. 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 tasks the DPO must ensure are detailed in article 39:

Article 39:

1. The data protection officer shall have at least the following tasks:
a. to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
b. to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c. to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
d. to cooperate with the supervisory authority;
e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.
2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

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

To ensure compliance with national regulations, a data controller will be appointed for each participating partner, acting as an interface with the relevant Data Protection Authority when required. The partners in charge of exercises (PSAB; CSAB; partners of eNOTICE project; French, German and Polish authorities; French, German and Polish Policy Makers – please see WP6) in which volunteers' participation is envisaged, will obtain the approval for the personal data management from their respective National Data Protection Authorities prior to the activities described in the WP.

However, as the EEAB pointed out during the reviewing process of D7.4, controllers are not an appointed position. Therefore, the consortium decided to appoint a DPO for all the participating organisations at the first progress meeting. The DPO's have been appointed by each participating organisation through a DPO statement. The list of appointed DPOs, their respective DPO statements, and their contact details are included in D10.3. The DPOs are tasked with ensuring compliance with the GDPR within their organisations and helping data subjects when they exercise their data protection rights.

2.2.1.3. Legal basis of processing

Processing personal data can only be lawful if it is carried out on the basis of one of the following grounds:

Article 6:

Processing shall be lawful only if and to the extent that at least one of the following applies:

a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c. processing is necessary for compliance with a legal obligation to which the controller is subject;
d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

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

Consent is a key element in the GDPR. Indeed, in many cases, the processing of personal data is not allowed unless consent is provided; **consent thus represents the main key to processing of personal data.** People's consent has been taken advantage of during the past, which is why the GDPR strengthened the concept to make sure consent is informed and explicit.

Consent is therefore defined as follows:

Article 4(11):

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

The conditions for consent to be valid are the following:

Article 7:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Within PROACTIVE, the processing of personal data will be justified exclusively on the grounds of informed consent, which will be given by research participants according to the processed and via the instruments established in D10.6. Also, the contact details of members of the AB's are processed on the basis of consent, expressed through the signing of Non-disclosure agreements.

Given that all personal data processed within PROACTIVE will be justified on the basis of informed consent, ensuring that it will be given in a manner that is GDPR compliant and in alignment with the principles of the GDPR. As it has been said above, D10.6 establishes the informed consent procedures adopted within PROACTIVE. Informed consent sheets and forms will be of vital importance in this regard as they will have to be designed in such a way that consent is effectively given in a free and informed manner. For them to be able to do so, they will need to contain all that is included in Article 13 GDPR.

Article 13

1.Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

a. the identity and the contact details of the controller and, where applicable, of the controller's representative;
b. the contact details of the data protection officer, where applicable;
c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
e. the recipients or categories of recipients of the personal data, if any;
f. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2.In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
c. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d. the right to lodge a complaint with a supervisory authority;
e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
f. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3.Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data

> subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.
>
> 4.Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

In the least, the aspects in bold need to be included within the information sheet and in the consent/assent form as they are relevant for the project activities.

Another question that must be taken into consideration in regards to informed consent within PROACTIVE is the vulnerable nature of a sizeable part of the project participants as it is said in the GA:

> these are members of the public but specifically including citizens with needs that differ from the average population such as persons with disabilities, the ill (e.g. with chronic or acute health conditions), elderly, or members of an ethnic minority or of a vulnerable group. Vulnerable groups may include children, pregnant women, persons with disabilities, chronic medical disorders or addiction, older persons with functional limitations and health restrictions, institutionalised individuals as well as their carers and companions. Vulnerable citizens also include persons with limited proficiency of the respective national languages or with restrictions regarding use of transportation.

Such vulnerable participants will be recruited according to the criteria and procedures described in D10.1 and they will constitute up to 15% of the sample. PROACTIVE intends to work deliberately with vulnerable groups of the population in order to improve the capacities of end-users and the population in terms of dealing with their needs and specificities in the event of a CBRNe attack. Therefore, consent must be adapted to address the needs of such vulnerable groups. Informed assent will have to be collected in the case of those vulnerable individuals who are not able to provide explicit consent. The vulnerable categories of the population that will be represented during the research activities will be established in D10.1. Among them the following groups will be represented:

- Minors;
- Disabled people;
- Elderly people;
- Pregnant women;
- People with limited proficiency in the respective national language;
- People with limited mobility.

The ethical and legal aspects having to do with the involvement of individuals belonging to these categories of individuals in the exercises are dealt with in D8.3, which is due on M17. Nevertheless, this deliverable is concerned with the issue of the legal age at which consent can be given in a free and informed manner. The host countries of the field exercises have different criteria. The following table summarises the information the consortium has regarding this that comes from the Fundamental Rights Agency (FRA), a document titled "Informed Consent for Paediatric Clinical Trials in Europe" (Working Group on Ethics, 2019), and feedback from our partners and collaborators based in the countries where the field exercises are meant to take place:

Table 1 Minimum ages to consent in countries where field exercises take place

Country	General	Recommended assent ranges	Parents
Italy	18	6-10 years 11-14 years 15-17 years with own signature No official mandatory age(s) for assent.	Consent from both parents
Germany	18	7-11 years 12-16 years 17 years own consent Parental consent required	Consent from both parents
Belgium	18	4-11 years (some sites do not use under 12 years) 12-14 years 14-17 years	One parent at recruitment, but both parents at some point for signatures

The consortium will seek to enrol minors in an ethical and legally compliant manner, which generally means asking for parental/guardian approval, as well as for assent from the minors. More details about these mechanisms will be provided in D8.3 (Ethics Briefing Pack for Project Fieldwork), which is due on M17. In any case, minors will be recruited through a procedure in which not only them but also their parents will give consent. The recruitment will likely be carried out in conjunction with educational institutions and other grassroots organisations, which adds further safeguards and guarantees that minors will be cared for and that their best interest will be taken into account at all times.

2.2.1.4. Principles

Processing personal data in a fair manner which is respectful of the fundamental rights of the data subjects represents the incentives behind the data protection legislation that has proliferated in the past decades. The first ethical principles to follow were set out in 1980 by the Organisation for Economic Co-operation and Development, and have served as a baseline for subsequent pieces of legislation.

The GDPR has also drawn from these principles, and includes the following:

Article 5.1 (a):

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

Lawful processing is that which is carried out on some of the basis for processing established in Article 6.1 GDPR. As for the principles of fairness and transparency, they require that the data subject be informed of the existence of the processing operation and its purposes (see Article 60). Therefore, they have to do with informed consent.

Article 5.1 (b):
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('**purpose limitation'**);

The principle of purpose limitation implies that data must be collected in order to fulfil certain goals. This is also related to informed consent since data subjects must be informed of the purposes for which their data are going to be processed in order for consent to be considered truly informed and lawful (see Articles 13 and 14 GDPR).

Article 5.1 (c):

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation'**);

The principle of data minimisation establishes that the data collected from data subjects must be kept to a minimum. In other words, no more data should be collected than what is strictly necessary in order to achieve the purpose of the processing.

Article 5.1 (d):
accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **('accuracy'**);

Data must be accurate and reflect reality, which needs to be judged in relation to the purposes of the processing. The main way in which this principle is enforced in the GDPR is the rights of the data subject, who can ask the controller to erase or rectify the data that it has regarding the data subject (Articles 16 and 17 GDPR).

Article 5.1 (e):
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('**storage limitation'**);

The principle of storage limitation establishes that personal data should not be kept for any longer than is reasonable for achieving the purposes for which they were collected in the first place. The period can be longer if the data are being processed for one of the purposes in Article 89 GDPR (public interest, scientific or historical research purposes, and statistical purposes), which could be the case for PROACTIVE as raw data sets may be collected and shared with other researchers for research purposes. However, that does not exempt the controller from putting in place technical and organisational measures aimed at safeguarding the rights and freedoms of the data subject, which will be discussed in D10.5. That is especially true for the sensitive data collected during the project that will be subject to further security measures, which will be included in the new version of D7.4 due in M18.

In the case of PROACTIVE, the agreed data retention period that was included in the DMP was five years after the end of the project. However, DHPol has established that the policy in their organisation is to keep personal data for 10 years, which, following the above-described requirements will have to be properly reflected in the consent forms. DHPol has established that all the sensitive personal data needed for the exercise including medical conditions, dietary restrictions and others will be deleted as soon as the second field exercise has passed. They will only keep one e-mail address from each participant for the duration of the project in case they need feedback or any upcoming questions need to be addressed later on. In addition to that, all remaining sensitive data will be deleted after the project. DHPol will also store all raw data anonymised in files. These are kept in a locked armoured steel cabinet, to which only one person responsible in the DHPol has access authorisation. The files will also be marked with a note that they will be destroyed after 10 years.

Moreover, partners are advised to delete data as soon as they do not need it so risks for the research participants' data protection rights can be kept to a minimum. The principle of storage limitation obliges controllers to justify their data retention period on the grounds of utility.

Article 5.1 (f):

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

D10.5 is entirely dedicated to the technical and organisational measures adopted by PROACTIVE in order to safeguard the rights and freedoms of data subjects and research participants.

Article 5.2:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('**accountability**').

In order for the other principles established in the GDPR to have teeth, the principle of accountability asks for those responsible to be held accountable if they are not compliant. The sanctions and fees established in the GDPR (see Articles 83 and 84 GDPR) have been devised in order to provide incentives for good behaviour. The PROACTIVE consortium has decided to constitute itself as a joint controller through a joint controller's agreement in which the responsibilities of the different partners are established.

As far as the processors, partners are advised to only involve processors that offer sufficient guarantees regarding data protection. As the GDPR establishes, the relationship between a given consortium member and processors needs to be regulated by means of a contract.

All of these principles should be applied by the processing entity when processing personal data.

PHE has established its intention to share raw personal data for a limited time. For this, they have an established relationship with Way With Words (transcription company), which constitutes a data-sharing agreement indicating the requirement for the company to (among other things); keep the data in a secure and encrypted format, not distribute the data beyond their organisation, or transfer or process the data outside of the EEA. As per this agreement, all data is to be kept confidential by Way with Words.

The GDPR asks the data controller to consider data protection by design and by default when developing a technology or service which requires the use of personal data:

> **Article 25:**
>
> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

It could be said that this very deliverable and the whole of WP8 are aimed at complying with the principles of data protection by design and by default since they attempt to raise awareness of the potential issues that the project can create. This Deliverable is also aimed at addressing them at an early stage in order to improve the level of legal compliance and ethical awareness in observance of the principle of "data protection by design and by default". In this regard, beyond the analysis of legal compliance with the data protection requirements, concrete recommendations will be made in D8.3 to ensure that the fieldwork carried out within PROACTIVE is aligned with this and the other principles established in the GDPR. This includes the security measures aimed at avoiding function creep, the limitation in the collection of personal data, and the thorough and understandable explanation of the aims and processes behind the collection of personal data belonging to both end-users and research participants.

2.2.1.5. Other relevant requirements in the GDPR

Security

Ensuring the security of personal data from misuse or abuse is an essential aspect of data protection legislation. The GDPR states concerning security:

> **Article 32.1:**
>
> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...].

Therefore, the GDPR's approach to security is based on risks and the current state of the art. Such an assessment must be adapted to the PROACTIVE specific processes and

performance, as it will be done during the project field exercises. In other words, the security measures adopted by the PROACTIVE project (D10.2) and its ethical and societal impact assessment analysing legal compliance (D8.4) will address the requirements of Article 32.1.

Also D10.5 (described in the GA as "A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants must be submitted as a deliverable") and D10.7 (described in the GA as "The beneficiary must evaluate the ethics risks related to the data processing activities of the project". This also includes an opinion if a data protection impact assessment should be conducted under art. 35 General Data Protection Regulation 2016/679 or Directive 2016/680") are also concerned with security within PROACTIVE. Moreover, all partners in the PROACTIVE consortium are committed to ensuring the highest security data protection standards throughout the research.

Breaches

The GDPR establishes the obligation for controllers to notify the competent supervisory authority in the event of a data breach in Article 33.1:

Article 33.1:

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

Personal data breaches are defined in the following way in the GDPR:

Article 4 (12):

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

Once again, the GDPR does not establish a very specific requirement for achieving compliance. Instead, it gives a considerable degree of autonomy in the implementation process, which makes the regulation able to still be useful after technological change has taken place. However, that also creates a certain degree of legal uncertainty. In particular, the GDPR expects the data controller to assess how likely it is for a particular data breach to result in a risk to the rights and freedoms of natural persons. Recital 85 GDPR includes a list of examples of negative effects that a personal data breach can have on individuals:

Recital 85:

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

Article 33 and 34 of the GDPR establish the following regarding the obligations of the controller in the event of a personal data breach:

Article 33

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

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3.The notification referred to in paragraph 1 shall at least:

a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b. communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c. describe the likely consequences of the personal data breach;
d. describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4.Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

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

Article 34

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

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3.The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4.If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Beyond this ambiguity, PROACTIVE does not involve particular security risks as it is established throughout this deliverable and in those more directly concerned with data protection and security. Data security measures are in place to ensure adequate data protection, such as encryption, anonymisation, access control, and password protection. These measures are detailed in D10.2 and D10.5.

The PROACTIVE consortium will use the criteria laid down in the “Guide on personal data breach management and notification” elaborated by the Spanish Agency of Data Protection (AEPD) in order to identify what data breaches are likely to result in high risks for the rights and freedoms of natural persons. These criteria are the following:

The category or critical level with regards to the security of the affected systems;

- Nature, sensitivity, and categories of personal data affected;
- Legible/illegible data;
- Volume of personal data;
- Ease of identifying individuals;
- Severity of the consequences for individuals;
- Individuals with special characteristics;
- Number of individuals affected;
- Data controllers with special characteristics (the entity itself);
- Profile of the users affected;
- Number and classification of the systems affected;

The impact that the breach could have on the organisation, from the points of view of information protection, provision of services, legal compliance, and/or public image.

Legal and regulatory requirements: Notification of the breach to the supervisory authority and any other notification requirement, communication to law enforcement bodies in the event of a crime.

In line with the above, the GDPR establishes that the controller also needs to keep a record of any personal data breaches that include information on its effects and the actions taken to mitigate its effects according to what is said in Article 33.5. Records of personal data breaches will be kept in PROACTIVE if they take place.

Article 33.5:

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

Additionally, the data controller is not only obliged to notify the supervisory authority but also to notify the data subjects affected by it in those cases where a **personal data** breach is likely to result in a high risk to the rights and freedoms of natural persons as it is stated in Article 34.1:

Article 34.1:

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

Once more, the GDPR leaves significant room for manoeuvre in the implementation, this time regarding the interpretation of what is considered undue delay.

Nevertheless, Article 34.5 provides a set of criteria with which they need for communicating the data breach to data subjects can be assessed in a more objective way.

Article 34.3:

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

All in all, the PROACTIVE consortium will put in place all the necessary measures to avoid data breaches from happening (data security) and follow the requirements established by the GDPR in the event of one. If a data breach takes place, the affected member of the consortium must first notify UIC (the coordinator), assess the likelihood of the data breach to result in a potentially high risk to the rights and freedoms of data subjects of the data breach according to the criteria laid down in this document and, finally, notify the data supervisory authority and/or the affected data subject in the terms established by the regulation.

DPIA (Data Protection Impact Assessment)

The carrying out of a Data Protection Impact Assessment might be required when developing new technologies or using special categories of data. The GDPR lays down criteria so as to establish under what conditions a DPIA is needed in Article 35.

Article 35.1:

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

This set of criteria is aimed at facilitating the decision about whether a DPIA needs to be carried out or not. The two main elements to be taken into account are how novel the technologies being developed are and the level of risk that the project presents to the data subjects' rights and freedoms. Nevertheless, these elements are still very broad, which is why Article 35.3 specifies a list of cases in which a DPIA has to be carried out.

Article 35.3:

A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b. processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
c. a systematic monitoring of a publicly accessible area on a large scale.

D10.7 includes an opinion on the need for conducting a DPIA which takes into account each of the circumstances described in the article above. It also factors in the guidelines issued by the ICO (Information Commissioner's Office) on this topic. D10.7 goes over the activities that necessitate the processing of personal data, examined in light of the GDPR and the ICO's guidelines. The conclusions reached are summarised in the following excerpt:

All in all, it is concluded that a DPIA is not mandatory within the context of PROACTIVE. However, that does not mean that the risks for privacy that the system presents won't be identified and addressed by the consortium as part of WP8. In fact, an "Ethical and Societal Assessment of PROACTIVE outputs" will be conducted (D8.4). It will address privacy and data protection issues posed by the project. Moreover, D7.4 (Data Management Plan and Research Ethics) addresses data management and data governance from an ethical perspective.

Therefore, the consortium has ruled out the need for conducting a DPIA since PROACTIVE will not threaten the data subjects' data protection rights to an extent that would justify it according to the criteria set out in the GDPR.

Rights of the data subjects

One of the most important aspects that can be found within the GDPR is the subjective rights that it recognises for data subjects. Among them, the following can be found:

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

Right to object the processing. These rights are included in chapter III of the regulation and empower data subjects in terms of the processing of their data. PROACTIVE will make sure that these rights are made effective for research participants, members of the consortium and AB members and users of the app/toolkits.

The main way by which these rights will be made effective within PROACTIVE will be by informing the concerned individuals about their existence. As it is established within section 2.2.1.3 of this deliverable, data subjects must be informed about their rights when data are collected from them. That will be the case for PROACTIVE, which will include relevant information regarding these rights in the consent forms and information sheets produced for the field exercises and research activities carried out during the project. In addition to that, the app's privacy policy will count with a privacy policy in which information about the data subject's data protection rights will be included.

It is important for the members of the consortium to be trained on how to respond to data subjects' requests and to put in place a protocol for the DPOs to follow. Regarding the consortium protocol concerning data subjects' rights, the joint controllers' agreement signed by the members of the consortium establishes the following.

2.1. UIC has been designated as contact point for data subjects, always provided that data subjects can exercise their rights under the GDPR vis-à-vis each individual data controller. 2.2. The Data Controllers are each responsible for the data subjects from whom it gathers

personal data, including the following responsibilities:

● to inform the data subject of the processing of personal data and the rights of the data subject;

● to ensure that the necessary authority exists for the processing of the registered data, including the obtaining of consent;

● that data are erased when they are no longer necessary.

2.3. The Data Controller who obtains specific data from sources other than the data subject is responsible for informing the data subject accordingly.

4.1. Each Data Controller is responsible for ensuring the rights of the data subjects in accordance with the below provisions of the GDPR:

• duty of disclosure when collecting personal data from the data subject;

• duty of disclosure if personal data are not collected from the data subject;

• right of access by the data subject;

• right to rectification;

• right to erasure (the right to be forgotten);

• right to restriction of processing;

• notification obligation regarding rectification or erasure of personal data or restriction of Processing;

• right to data portability (but not for public authorities);

• right to object to processing.

4.2. If one of the Data Controllers receives a request or inquiry from a data subject regarding matters covered by another Data Controller's responsibilities, see above, the request is forwarded to such Data Controller without undue delay.

4.3. The parties are responsible for assisting each other to the extent this is relevant and necessary in order for both parties to comply with their obligations to the data subjects.

The articles concerning the individual data protection rights included above are listed below.

Article 15 (Right of access)

1.The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

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

2.Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

3.The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4.The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Article 16 (Right to rectification)

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

Article 17 (Right to erasure)

1.The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
c. the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
d. the personal data have been unlawfully processed;
e. the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f. the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2.Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3.Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

a. for exercising the right of freedom of expression and information;
b. for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c. for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
e. for the establishment, exercise or defence of legal claims.

Article 18 (Right to restriction of processing)

1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

a. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c. the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d. the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2.Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

3.A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

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

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

Article 20 (Right to data portability)

1.The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

a. the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
b. the processing is carried out by automated means.

2.In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3.The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Article 21 (Right to object)

1.The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

2.Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

3.Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4.At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

5.In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

6.Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Transfer to third countries or international organisations

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

- One of the partner organisations (SESU) is based in a country outside of the European Union (Ukraine);
- A number of other partners are based in the UK, which is due to leave the European Union within the lifespan of the project.

In both cases, personal data transfers will be made to countries outside the European Union.

Article 44

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

Therefore, the GDPR obliges controllers and processors to put in place safeguards when personal data is to be transferred outside of the European Union and the EEA (European Economic Area).

According to Article 45.1, data transfers can take place under normal conditions if an adequacy decision concerning the country to which data are going to be transferred has been issued.

Article 45.1

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

However, an adequacy decision concerning Ukraine has not been issued. As for the UK, the process can only start once Brexit happens. The criteria that have to be taken into account by the Commission when making a decision suggests that an adequacy decision for the UK will probably be issued.

Article 45.2

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

a. the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

b. the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

c. the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Nevertheless, it takes on average 28 months for the European Commission to issue an adequacy decision, which makes it very likely that the UK will remain a third country with no special status regarding data transfers, at least for a number of months and certainly during the lifespan of the project.

This would force the consortium to find an alternative way to carry out personal data transfers in alignment with the GDPR. The alternatives would be the following:

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

The main legal precepts are the following:

Article 46:

1.In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

2.The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:

a. a legally binding and enforceable instrument between public authorities or bodies;
b. binding corporate rules in accordance with Article 47;
c. standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
d. standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

e. an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
f. an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

3.Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:

a. contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
b. provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

4.The supervisory authority shall apply the consistency mechanism referred to in Article 63 in the cases referred to in paragraph 3 of this Article.

5.Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed, if necessary, by that supervisory authority. Decisions adopted by the Commission on the basis of Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed, if necessary, by a Commission Decision adopted in accordance with paragraph 2 of this Article.

Article 47

1.The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

a. are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
b. expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
c. fulfil the requirements laid down in paragraph 2.

2.The binding corporate rules referred to in paragraph 1 shall specify at least:

a. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
b. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
c. their legally binding nature, both internally and externally;

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

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

Article 49.1

In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

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

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

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

Table 2 Options for data transfer to third countries

Option	Approval of supervisory authority	Further requirements
Standard data protection clauses	No (Article 46.2)	
Contractual clauses	Yes (Article 46.3)	
Binding corporate rules	Yes (Article 47.1 and 47.2)	• All the information established in Article 47.2 GDPR must be included within the binding corporate rules. • A member of the consortium based in the EU would have to accept liability for data breaches caused by the one based outside of the Union.
Explicit consent/assent	No (Article 49.1.a)	• Research participants must be informed of the risks involved given the absence of adequacy decision and adequate safeguards.
Special cases (legitimate interest)	No (Article 49.1)	• The data controller must inform the supervisory authority. • Aside from the information that needs to be given to data subjects according to Articles 13 and 14, the controller will also need to inform the data subject about the transfer and the compelling interest pursued.

The PROACTIVE consortium will adopt an approach that suits the circumstances of the project and that provides an adequate level of data protection as well. In any case, it seems at this stage that data transfers to third parties are not foreseen.

The mobile application developed within PROACTIVE

The PROACTIVE App to be developed as part of WP4 by RINISOFT will be designed to process personal data for a series of purposes. RINISOFT was consulted about how they planned to manage the processing of personal data within the App in order to reflect such information in this deliverable. It is still quite early days in the development process, which has not started yet. However, RINISOFT provided the consortium with the following information:

All personal or personally identifiable information (PII) that is gathered and stored will be treated in accordance with GDPR regulations. Only information that is critical to the functionality of the service will be gathered and stored. Every service user will be explicitly told, in advance, what PII will be gathered and what, specifically, it will be used for. All PII will be stored on encrypted volumes and only made available to those who have a specific and authorised reason to view or modify the data. Access to PII will be subject to logging and automated audit. Each user may request an export of all PII stored relating to themselves, which will be provided to them in digital format in a timely manner. Each user may request for their PII to be deleted and removed in its entirety from our active systems, this will be undertaken in accordance with our privacy policy.

It can be inferred from this that the App developers have taken into consideration privacy and data protection from the beginning. There will be ongoing communication between RINISOFT and ETICAS to ensure that the technological outcomes of the project are aligned with the GDPR. Last, compliance with the GDPR will be guaranteed in the following two ways. First, the Privacy by Design recommendations to be provided in D3.3 (M24). Second, the Privacy Impact Assessment in D3.4 (M40) which is meant to review the efficacy of the measures put in place to ensure privacy.

2.3. CBRNe response and disaster relief international mechanisms, standards and regulations

2.3.1. Historical background

The history of the European crisis management framework is quite recent. The first precedent of the Civil Protection Mechanism took place in the 70's. Its creation was due to two different catastrophes that happened in European territory:

- Production of a dioxin cloud as the result of an accident in Givaudan's chemical plant belonging to the ICMESA firm, located near Seveso, Northern Italy;
- The sinking of the oil tanker Amoco Cádiz, which provoked 4,000 tons of fuel oil being spilled into the seafront of Britain and France.

These incidents contributed to creating an atmosphere that was favourable to the coordination of the disaster management agendas of member states. This happened during a ministerial meeting in Rome in 1985. However, the first milestone that started the process of development of the current legal and institutional framework should be placed in 1987, when the Council passed the Resolution of the Council and the representatives of the Governments of the Member States, meeting within the Council of 25 June 1987 on the introduction of Community Cooperation on Civil Protection. It signalled a new era regarding CBRNe events, given that member states became more aware of the need for further cooperation at the EU level. Even though civil protection and disaster response remain a national prerogative, the EU could facilitate cooperation and the sharing of information and resources between states.

After this document, the following resolutions were produced:

- Resolution of the Council and the representatives of the Governments of the Member States, meeting within the Council of 13 February 1989 on the new developments in Community cooperation on civil protection;
- Resolution of the Council and the representatives of the Governments of the Member States, meeting within the Council of 23 November 1990 on Community cooperation on civil protection;
- Resolution of the Council and of the representatives of the Governments of the Member States, meeting within the Council of 8 July 1991 on improving mutual aid between Member States in the event of natural or technological disaster.
- The main result of these developments was the above-mentioned creation of a Civil Protection Mechanism which was a sort of precedent to the "Solidarity Clause".

Having said that, disaster management remained a national competence until 1997, when the Council of the European Union approved a major civil protection action programme through the Council Decision 98/22/EC of 19 December 1997 establishing a Community action programme in the field of civil protection. This Action program directed the Commission to step up its efforts aimed at the pooling of member state expertise, thus fostering mutual assistance, and proposing training programs.

The terrorist attacks that targeted the United States of America on the 11th September 2001 constituted a major milestone in the way to the construction of an EU common management and response to major crisis situations, such as those related to CBRNe incidents. In the face of these new threats, the European Union took conscience of the need for a common framework on disaster management with the potential to allow member states to pool resources and improve their response.

In that context, the European Commission issued a communication (COM (2001) 707 final: "Communication from the Commission to the Council and the European Parliament — Civil protection — State of preventive alert against possible emergencies"). Also, the Council Decision of October 23, 2001, establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions was passed. This document set up the Community Mechanism for Civil Protection, whose main goal was to enable cooperation within civil protection interventions. During the years 2002 and 2003, the EU adopted several resolutions linked to civil protection, disaster management, and related matters.

Beyond the regulatory framework that was developed during the beginning of this decade, an important policy document was published in 2006, the Barnier Report, which was authorised by Michel Barnier and was the result of a study commissioned by José Manuel

Barroso and Wolfgang Schüssel. In this document, 12 measures were considered relevant as far as the enforcement of the EU's capacity to respond to a crisis is concerned:

- A European-wide civil protection force Europe Aid;
- Support for the force in seven ultra-peripheral regions of the European Union;
- Creation of a Civil Security Council and strengthening of the General Affairs and External Relations Council;
- One-stop-shop for humanitarian response;
- Integrated European approach to anticipate crises;
- Six EU regional delegations to specialise in crisis management;
- Clear information system for European citizens;
- Sharing of consular resources;
- Creation of flying consular teams;
- Setting up European consulates in four pilot zones;
- Drawing up a European consular code;
- Laboratories to specialise in the fight against bioterrorism and the naming of victims.

After this, the Treaty of Lisbon (2007) introduced radical changes in the nature and governance of the Union, which had implications for disaster management and CBRNe response. One of the most important ones is that the European Union got competences to carry out actions to support, coordinate or supplement the actions of the Member States in different areas, being civil protection one of them.

Nevertheless, the most important element introduced by the Treaty was usually called "Solidarity Clause". This clause was meant to complement the "Mutual Defense Clause" with the aim of more efficiently facing new kinds of threats that manifested themselves after the terrorist attacks of New York or Madrid. It can be found in article 222 of the Consolidated Version of the Treaty on the Functioning of the European Union which entered into force since 1 December 2009.

> 1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) — prevent the terrorist threat in the territory of the Member States; — protect democratic institutions and the civilian population from any terrorist attack; — assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.

2. Should a Member State be the object of a terrorist attack or the victim of a natural or manmade disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council.

3. The arrangements for the implementation by the Union of the solidarity clause shall be defined by a decision adopted by the Council acting on a joint proposal by the Commission and the High Representative of the Union for Foreign Affairs and Security Policy. The Council shall act in accordance with Article 31(1) of the Treaty on European Union where this decision has defence implications. The European Parliament shall be informed. For the purposes of this paragraph and without prejudice to Article 240, the Council shall be assisted by the Political and Security Committee with the support of the structures developed in the context of the common security and defence policy and by the Committee referred to in Article 71; the two committees shall, if necessary, submit joint opinions.

4. The European Council shall regularly assess the threats facing the Union in order to enable the Union and its Member States to take effective action.

The solidarity clause imposes significant obligations upon member states and attempts to foster cooperation during catastrophic events, such as CBRNe attacks. Therefore, this clause is called to be a keystone of the EU's CBRNe response strategy in spite of the challenges that its interpretation poses.

Regarding interpretation, in 2010 the EU institutions made a real effort to effectively address the problems derived from it. For this purpose, a Joint Proposal from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the Council of the European Union (Joint Proposal for a Council Decision on the arrangements for the implementation by the Union of the Solidarity clause), following the mandate included in paragraph 3 of Article 222. This article requires the Commission and the High Representative to submit to the Council a proposal on the Union's arrangements for implementing the Clause, which was effectively submitted. However, the reluctance of member states to implement binding arrangements has limited the real application of the solidarity clause.

2.3.2. Policy/Legal framework

This section aims at describing some of the most significant documents on CBRNe related matters at the European level during the last two decades. A number of them are still in

force, while others have already been repealed or updated, but are useful so as to understand the legal background PROACTIVE needs to deal with. Others are working papers, studies or policy frameworks that are useful in order to understand how CBRNe has been approached by the European policymaker and legislator.

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

This recent regulation has provided a definition of terrorism for the first time, which is relevant regarding the prosecution of terrorist offences that occur within the territory of the European Union. The Directive has also defined what a terrorist group is.

Article 2 (3)

'terrorist group' means a structured group of more than two persons, established for a period of time and acting in concert to commit terrorist offences; 'structured group' means a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.

Article 3

1.Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2:

a. attacks upon a person's life which may cause death;
b. attacks upon the physical integrity of a person;
c. kidnapping or hostage-taking;
d. causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
e. seizure of aircraft, ships or other means of public or goods transport;
f. manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons;
g. release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;
h. interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
i. illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council (19) in cases where Article 9(3) or point

(b) or (c) of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies;

j. threatening to commit any of the acts listed in points (a) to (i).

2.The aims referred to in paragraph 1 are:

a. seriously intimidating a population;
b. unduly compelling a government or an international organisation to perform or abstain from performing any act;
c. seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.

European CBRNe action plan (2009) and the Progress Report on the Implementation of the EU CBRN Action Plan (2012)

According to the European Commission, the CBRNe action plan "was adopted in December 2009 by the EU Council and aimed to strengthen CBRN security throughout the EU" (European CBRNE action plan , 2009). As far as the action plan's goal, it "was to reduce the threat of and damage from CBRN incidents of accidental, natural and intentional origin, including terrorist acts." (Ibid.). It was based on an all-hazard approach and its overall goal was to reduce the threat of, and damage from CBRN incidents of accidental, natural and intentional origin, including terrorist acts. The Action Plan supported the implementation of the EU Counter-Terrorism Strategy and was in alignment with the Internal Security Strategy.

The implementation of the action plan was expected to take place between 2010 and 2015. It resulted in the issuing of the progress report on the implementation of the EU CBRN Action plan (Progress Report on the Implementation of the EU CBRN Action Plan , 2012). The document reviews the actions that have been taken in the different areas concerned by the action plan. The aim of this report, issued in May 2012, was to review the progress made in the implementation of the plan. Therefore, its aim was not to assess the plan itself.

A general assessment is made in the introduction:

Progress has been made in all the areas, C, B, R, N, and H, with many examples of successful activities in all these domains, however, it can be noted that the implementation of the actions has been relatively uneven, the Member States and EU bodies have made progress in the same actions to a varying extent, and many of the activities carried out so far are of preparatory nature vis-à-vis the full objectives and deliverables of the Actions. Therefore, work should be taken forward in continuing to implement the majority of the C, B, RN and H actions, nevertheless, focusing on some of the more generic and comprehensive ones in order to streamline efforts and ensure more tangible results.

The uneven nature of the progress made in the different areas is also pinpointed in the document.

"Further work and a structured approach is needed to carry out activities in the framework of this Action Plan in the field of detection, including development of detection technology, in C, B and RN fields"

"Continued and further streamlined research into the CBRN areas is also crucial for overall progress in achieving security from CBRN threats".

"In order to ensure a structured approach and progress in all the fields, but in particular in areas where specific studies and research has been taken forward, it is important to keep track on and disseminate the results of such work, be it carried out by EU bodies or Member States"

As far as the policy objectives that will be relevant in the long run (after the lifetime of the action plan), the report establishes the following:

In the longer run (beyond the life cycle of the Action Plan) it would be important to get away from a pure "shopping list" of individual actions and develop a more strategic and overarching approach to CBRN policies.

All these remarks are particularly interesting from the PROACTIVE project's perspective, as they reinforce the importance of research on detection technologies and the dissemination of the results of this research. The PROACTIVE project aims at providing tools for addressing many of the logistical and governance gaps identified by the report in the first response around CBRN events. The report also underlined the importance of developing a more strategic and overarching approach to CBRN and explosives (E) policies, which ties in with PROACTIVE's objectives which include improving standardisation and improving how the police responds to the needs of vulnerable people.

European Security Strategy (2003)

The 2003 European Security Strategy - A Secure Europe in a Better World (European Security Strategy , 2003), was adopted by the European Council held in Brussels on 12 December 2003. Both terrorism and the proliferation of weapons of mass destruction (WMD) are established as the first and second main challenges to EU security in this document. As a matter of fact, a combination of both threats is considered to be the worst scenario.

The most frightening scenario is one in which terrorist groups acquire weapons of mass destruction. In this event, a small group would be able to inflict damage on a scale previously possible only for States and armies.

The European Counter Terrorism Strategy (2005)

The EU Counter-Terrorism Strategy (The European Counter Terrorism Strategy , 2005) was adopted in 2005 to fight terrorism globally and make Europe safer. The Strategy is built around four pillars:

- PREVENT people from turning to terrorism and stop future generations of terrorists from emerging through addressing the causes of radicalisation and terrorist recruitment.
- PROTECT citizens and critical infrastructure by reducing vulnerabilities against attacks is the second priority;
- PURSUE and investigate terrorists, impede planning, travel, and communications, cut off access to funding and materials and bring terrorists to justice;
- RESPOND by preparing, managing and minimising the consequences of a terrorist attack is the fourth objective of the EU counter-terrorism strategy.

PROACTIVE aims at enhancing the response capabilities of end-users and first responders through the creation of a toolkits focused on improving how first responders deal with individuals belonging to vulnerable groups. Therefore, it is mainly concerned with the fourth dimension of the strategy.

In the following excerpt, the importance of the response to CBRNe events is highlighted:

> We cannot reduce the risk of terrorist attacks to zero. We have to be able to deal with attacks when they occur, recognising that attacks can have effects across EU borders. The response to an incident will often be similar whether that event is natural, technological or man-made, hence the response systems in place to manage the consequences of natural disasters may also be used to alleviate the effect on citizens in the aftermath of a terrorist attack. Our response to any such events should make full use of the existing structures, including the Civil Protection Mechanism, which the EU has developed to respond to other major European and international crises, and be co-ordinated with the action of other Major European and international crises, and be co-ordinated with the action of other international organisations involved.

PROACTIVE aims at improving response protocols in the event of CBRNe events, especially regarding the needs of vulnerable groups such as disabled people, minors, people with limited proficiency in the national language of the country in which the CBRNe event took place and the other groups detailed in D10.1. In this excerpt, it is also underlined that response protocols are likely to be the same no matter the cause of the CBRNe event in question. That goes to show PROACTIVE's findings can be used across a range of situations in which first responders have to deal with individuals affected by a CBRNe event, especially those that belong to vulnerable groups.

The Stockholm Programme (2010)

The Stockholm Programme (Stockholm Programme, 2010), issued the 4th of May, 2010, establishes the European Union's (EU) priorities in the area of justice, freedom, and security during the period 2010-14. The strategic guidelines for legislative and operational planning

are defined in alignment with The Lisbon Treaty. 'A Europe that Protects' is one of the main priorities established in the document. It calls for the development of an internal security strategy.

> A Europe that protects: An internal security strategy should be developed in order to further improve security in the Union and thus protect the lives and safety of citizens of the Union and to tackle organised crime, terrorism and other threats. The strategy should be aimed at strengthening cooperation in law enforcement, border management, civil protection, disaster management as well as judicial cooperation in criminal matters in order to make Europe more secure. Moreover, the Union needs to base its work on solidarity between Member States and make full use of Article 222 TFEU (Treaty of the Functioning of the European Union).

The need to turn Europe into a political entity that takes care of the security of its citizens is further detailed in the document in certain sections. One of them includes direct references to CBRNe events.

> The CBRN (chemical, biological, radiological and nuclear) risk, and in particular the threat of terrorist groups using CBRN materials, has led to action at national and EU levels. The overall goal of the policy on CBRN security is to present a prioritised, relevant and effective European strategy to enhance the protection of EU citizens from incidents involving CBRN materials. In order to achieve this goal, the implementation of the EU CBRN Action Plan based on an all-hazards approach, including actions to prevent, detect, prepare and respond to larger incidents with high risk CBRN materials, is vital.

Once again, the PROACTIVE project is primarily concerned with response to CBRNe events, although preparedness is another focus of the project through information campaigns geared towards citizens. In this context, protecting citizens and especially those in vulnerable situations is deemed to be a vital objective of the Union.

The EU Internal security strategy (2010)

The EU Internal Security Strategy (titled "Towards a European Security Model") was adopted in 2010 by the Member States (European Union Internal Security Strategy, 2015). It details the challenges, principles, and guidelines that seek to deal with a number of emerging threats and to increase Europe's level of security. The strategy called on the Commission to suggest specific actions aimed at enabling its implementation.

These actions were established in the "Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" (COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, 2010). It builds on what Member states and institutions had already established. It sets out a way in which the different stakeholders (Member States, the European Parliament, the Commission, the Council and agencies and

others, including civil society and local authorities) can collaborate during the period 2010 - 2014 to be more competent when fighting and preventing serious and organised crime, terrorism and cybercrime, in strengthening the management of the EU external borders and in building resilience to natural and man-made disasters.

This communication identified the most urgent challenges to EU security from 2011 to 2014. It suggests five overarching objectives and specific actions for this period which, in combination with ongoing actions and initiatives, will help make the EU more secure. These objectives are serious and organised crime, terrorism, cybercrime, border security and (man-made or natural) disasters.

Objective 5, “Increase Europe's resilience to crises and disasters," used a cross-sectoral approach (The EU is exposed to an array of potential crises and disasters, such as those associated with climate change and those caused by terrorist and cyberattacks on critical infrastructure, hostile or accidental releases of disease agents and pathogens, sudden flu outbreaks and failures in infrastructure) that calls for improvements to long-standing crisis and disaster management practices in terms of efficiency and coherence. Although all actions proposed by this strategy under this objective are indirectly related to CBRN incidents management, none of them contains specific measures to deal with them. The importance of increasing the protection for individuals, especially the vulnerable ones, is underlined in the document.

EU action in the field of civil protection must be guided by the objectives of reducing vulnerability to disasters through the development of a strategic approach to disaster prevention and anticipation and by further improvements in preparedness and response while recognising national responsibility. Guidelines for hazard and risk-mapping methods, assessments and analyses should be developed as well as an overview of the natural and man-made risks that the EU may face in the future. This EU-wide risk analysis should be the basis for cooperation initiatives between risk-sharing Member States and the EU in the field of civil protection and capacity planning. New risks and threats are to be identified, such as energy shortage, ICT breakdowns and pandemics. The resilience of citizens as well as the public and private sectors to the effects of disasters are to be included in prevention policies.

In June 2014, the European Commission published a report assessing the progress made under the Internal Security Strategy and identifying its future priorities for a renewed Internal Security Strategy. In the next section, it will be seen how the European Union issued a new internal security strategy intended to inform the policy of the European Union from 2015 to 2020.

The renewed European Union Internal Security Strategy (2015)

A document including conclusions on the Renewed European Union Internal Security Strategy (2015-2020) was drafted by the European Council in 2015 (The renewed European Union Internal Security Strategy , 2015). It attempts to replace the strategy described in the previous section. Like the previous strategy, it aims at enhancing the level of protection of

European citizens concerning an ongoing surge of threats, particularly those posed by terrorism and serious and organised crime.

The crucial importance of ensuring full compliance with fundamental rights, including those related to privacy, personal data protection, confidentiality of communication and the principles of necessity, proportionality, and legality for all measures and initiatives taken to protect the internal security of the European Union is emphasised in the strategy.

UNDERLINING the need to respect and promote the rights, freedoms and principles, as set out in the Charter of Fundamental Rights of the European Union, within the European Union and in all work carried out in creating and upholding an area of freedom, security and justice,

Although the focus of the document is on preventive strategies to fight against the threat that terrorism constitutes for the European Union, the need for mitigating the effects of man-made disasters on the population, especially those among us who are the most vulnerable, is also taken into consideration.

UNDERLINES the necessity to strengthen the protection of critical infrastructures and STRESSES the need to ensure resilience, operational preparedness and political coordination to react, deal with and mitigate crises and natural/man-made disasters,

Conclusions on preparedness and response in the event of a CBRN attack (2010)

During the 3043rd Justice and Home Affairs Council meeting held in Brussels, 8 and 9 November 2010, the Council invited the Member States (Conclusions on preparedness and response in the event of a CBRN attack , 2010):

- To ensure that the CBRN risk is properly incorporated into their emergency response planning, in particular by taking its possible terrorist origins into account;
- To integrate the different elements of the response when drawing up such plans (especially police, intelligence, rescue, health, communication);
- To take the requirements of possible criminal investigations and forensics adequately into account in those plans;
- To ensure the implementation of the CBRN emergency response planning through appropriate simulation exercises;
- To exchange information and best practices with other Member States concerning their CBRN emergency intervention and response planning;
- To examine any problems raised by the Member States during the preparation and implementation of CBRN planning which require action at European level;

- To raise awareness on CBRN risks and appropriate action among the population in the event of an attack.

PROACTIVE aims at creating protocols of action and toolkits that are meant to mitigate the potential damage of a CBRNe event, which is in alignment with the principles established in the conclusions on preparedness and response in the event of a CBRNe attack.

Council conclusions on the new CBRNE Agenda (2012)

The Council's conclusions on the new CBRNE agenda were adopted on the 29th of November 2012. These conclusions followed the Commission's Progress Report on the Implementation of the EU Chemical, Biological, Radiological and Nuclear (CBRN) Action Plan of May 2012, underlining the importance of maintaining a strategic approach to reduce the threat of, and damage from, CBRN incidents of accidental, natural and intentional origin, including terrorist acts, and took account of the report of the EU CBRNE Conference in Malmö in October 2012, which, in its recommendations, called for consideration to be given to a comprehensive approach to CBRNe incidents including crimes and terrorism, and for the establishment of a structured approach to prevention, detection and response, focusing on enhanced interagency collaboration especially between law enforcement, military, civil protection, and other competent authorities, as well as for ongoing development of close interaction on CBRNe between the public sector and private actors.

As the main outcome of this document, the Council encourages the Commission, in the creation of a new CBRNE Agenda, to use the EU Chemical, Biological, Radiological and Nuclear Action Plan, and the Action Plan on Enhancing the Security of Explosives, as a foundation for creating a revised policy which should (among other recommendations):

> *- use synergies between the above mentioned Action Plans, encouraging the development of prevention and detection measures, awareness raising, and research on the security of CBRN materials and explosives, as well as the exchange, as appropriate, of information and knowledge regarding the management and handling of incidents with CBRN materials and explosives, while also keeping in mind relevant differences during future work.*

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

In the Communication 'An Open and Secure Europe' COM(2014) 154 adopted on the 11th of March, 2014, the European Commission checks the progress made since the Stockholm programme in 2009. It also establishes its vision on the future agenda concerning Home Affairs.

The European Council's five-year Stockholm programme finished in December 2014. This Communication arranges the Commission's guidelines concerning the political direction to be taken by the EU's efforts towards a more open and safe Europe by 2020.

This text establishes five political priorities for the area of Security, being “A Europe that Protects” the last one listed. It lays down the objectives set out in the 2010 Internal Security Strategy and checks if they are still valid.

Regarding how the text relates to the PROACTIVE project, the document does not go too deep. In fact, the only mention of CBRNe can be found in section 5.2 “Prevention of terrorism and addressing radicalisation and recruitment” (Communication from the Commission - An Open and Secure Europe: making it happen , 2014):

> The EU has already agreed on legislation to make it more difficult to access precursors to produce explosives. Now we must make sure it is being implemented in an effective way. There is also a need to enhance and further prioritise work on Chemicals, Biological, Radiological, Nuclear materials and Explosives.

Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on a new EU approach to the detection and mitigation of CBRN-E risks (2014)

This communication was adopted on the 5th of May, 2014. In the introduction to the document, a description of the context is presented. It depicts the current situation in the EU with respect to the work that is being carried out in this field (Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on a new EU approach to the detection and mitigation of CBRN-E risks , 2014):

> The EU, its Member States and other key partners have undertaken numerous activities to improve the ability to prevent chemical, biological, radiological, nuclear (CBRN) and explosives incidents and protect citizens, institutions and infrastructure against such incidents.
>
> More needs to be done however. Following the progress reports under the EU CBRN Action Plan and under the Action Plan on Enhancing the Security of Explosives in 2012, extensive consultation took place with Member States and other stakeholders on how best to address these issues. A new CBRN-E Agenda was set out to focus on key priorities to be addressed at EU level.

> This communication is a first step in implementing the new CBRN-E Agenda. It aims to bring about progress in the area of detection of CBRN-E threats, and put effective measures in place for detecting and mitigating these threats and risks at EU level.

Later on in the document (Background and Objectives), it is acknowledged that the challenges posed by CBRN materials and explosives remain important and evolving. Specifically, it is said that (Ibid.):

> While work at national level continues to play a vital role in the fight against terrorism, a robust, better designed, and proportionate strategy to anticipate and deter future CBRN-E risks at EU level is needed, including tackling illegal methods of production, handling, concealing and storing these materials.
>
> It is therefore important to adopt a proactive approach and to put effective, proportional safeguards in place, including prevention, preparedness and response measures at EU level, while respecting fundamental rights.

Also, the importance of developing practical tools meant to be used by practitioners is underlined in the text.

> The EU can add value by developing practical and effective tools for practitioners, ranging from workshops, guidance materials, training and awareness raising to supporting research and testing activities. One example is the support provided for the collaboration — under the auspices of the ATLAS network — of the EU police special intervention forces which train and operate together.

PROACTIVE aims at developing toolkits meant to be used by citizens and practitioners in the event of CBRNe attacks. An App intended to be used for such purposes will also be developed as part of the project. The main part of the text is the section titled “A new approach to the detection and mitigation of CBRN-E risks”. Five goals are identified within it:

1. Better Detection
2. Using better research, testing, and validation
3. Training, awareness and capacity building
4. Promote more lead country initiatives and work with industry
5. The external dimension

Broadly speaking, all of these objectives are relevant to PROACTIVE in some way. However, the focus of the text is in prevention, not response to CBRNe attacks or the needs of vulnerable citizens. The third objective is the most applicable one to the PROACTIVE project.

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (2013)

This piece of legislation is probably the most important one as far as crisis response is concerned. This decision was issued in 2013, but it remains in force at present. The latest consolidated version is from the 21/03/2019. It creates the whole structure of the Union Civil Protection Mechanism, whose aims are described in its Article 1.1.

Article 1.1

The Union Civil Protection Mechanism ("the Union Mechanism") shall aim to strengthen the cooperation between the Union and the Member States and to facilitate coordination in the field of civil protection in order to improve the effectiveness of systems for preventing, preparing for and responding to natural and man-made disasters.

In terms of its scope, it is quite ambitious since it has been conceived for dealing with disasters affecting human beings but it may be competent also in crisis related to the environment, property, and cultural heritage. It can also be applicable to all types of natural and man-made disasters, including environmental disasters, marine pollution, and acute health emergencies, occurring inside or outside the Union. It also aims at enshrining the principle of solidarity between member states in the field of civil protection.

Article 1.3

The Union Mechanism shall promote solidarity between the Member States through practical cooperation and coordination, without prejudice to the Member States' primary responsibility to protect people, the environment, and property, including cultural heritage, on their territory against disasters and to provide their disaster-management systems with sufficient capabilities to enable them to cope adequately and in a consistent manner with disasters of a nature and magnitude that can reasonably be expected and prepared for.

According to this Decision, civil protection and other emergency assistance may be required in the event of one of such disasters to reinforce the response capabilities of the affected country.

At the time when it was issued, the decision was the result of a process in which previous efforts aimed at achieving an integrated approach to managing disasters finally were integrated into a legally binding text.

DECISION (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements

This decision sets up the EU Integrated Political Crisis Response (IPCR). The integrated political crisis response (IPCR) arrangement supports rapid and coordinated decision-making at EU political level for major and complex crises, including acts of terrorism.

Article 1

1. This Decision lays down the EU Integrated Political Crisis Response ('IPCR') arrangements. The IPCR enable timely coordination and response at Union political level for crises, whether they originate inside or outside the Union, which have a wide-ranging impact or political significance.

1. The IPCR shall provide the Council with the necessary tools and flexibility to decide on the handling of the response of the Union, including through rapid consultations and possible proposals for action. The political control and strategic direction for all stages of the IPCR process shall be under the leadership of the Presidency of the Council, taking full account of the competences of the Commission and the HR.

3. The IPCR shall be a single set of arrangements to respond at Union political level in a coherent, efficient and timely way to crises. The IPCR shall be used by the Council to carry out coordination at political level to the invocation of the solidarity clause as set out in Article 1(2) of Council Decision 2014/415/EU pursuant to Article 222(3) TFEU.

4. These arrangements shall not replace or duplicate existing Union mechanisms or arrangements.

This mechanism can be activated in two different ways: information sharing mode and full activation mode. In terms of the institution that is able to activate it, it is the presidency, although any member state can invite the presidency to activate it.

Article 4.1

In the event of a crisis, the decision to activate the IPCR shall be taken by the Presidency. Any Member State may invite the Presidency to do so.

The IPCR mechanism supports the Council presidency, as well as COREPER and the Council, by providing concrete tools to:

- streamline information sharing;
- facilitate collaboration;
- coordinate crisis response at the political level.

These tools include:

- an informal roundtable, which is a crisis meeting chaired by the Presidency with key actors (representatives of the Commission, the EEAS, EU agencies, the most affected member states, the cabinet of the European Council President, experts, etc.);
- analytical reports to provide decision-makers with a clear picture of the current situation;
- a web platform to exchange and collect information;
- a 24/7 contact point to ensure constant liaison with key actors.

There are three operational modes, depending on the situation:

- a monitoring mode to easily share existing crisis reports;
- an information-sharing mode triggering the creation of analytical reports and the use of the web platform to better understand the situation and prepare for a possible escalation;
- a full activation mode involving the preparation of proposals for EU action to be decided upon by the Council or European Council.

The crisis coordination mechanism can be activated for events occurring inside as well as outside of the EU.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan to enhance preparedness against Chemical, Biological, Radiological and Nuclear Security risks (2017)

This plan builds upon the 2010-2015 CBRN action plan and attempts to update the framework with which Europe is going to face CBRNe threats, especially those coming from terrorism, whose importance is underlined in the introduction.

> Terrorist organisations have not used chemical, biological, radiological and nuclear ("CBRN") agents in Europe. Still, there are credible indications suggesting that terrorist groups might have the intention of acquiring CBRN materials or weapons and are developing the knowledge and capacity to use them. Daesh has used chemical weapons in Syria and Iraq and is assessed as being able to produce and use these weapons. Smaller incidents have shown Daesh's interest in innovating and in developing biological and radiological weapons. It should be noted that whilst the term CBRN is used throughout the document, the likelihood of a nuclear weapon attack by any non-State actor is considered lower than that of chemical, biological or radiological attacks.

The objectives set out in this plan are:

- **Objective 1**: reducing the accessibility to CBRN materials;
- **Objective 2**: ensuring a more robust preparedness for and response to CBRN security incidents;
- **Objective 3**: building stronger internal-external links and engagement in CBRN security with key regional and international EU partners;
- **Objective 4**: enhancing our knowledge of CBRN risks.

The second objective is the one more directly related to the PROACTIVE project in this list.

The conclusion states the following:

> In light of the evolving threats, Europe needs to pool resources and expertise to develop innovative, sustainable and effective solutions. Cooperation efforts across the EU along the lines set out in this Action Plan can result in significant security gains and lead to tangible results.
>
> The proposals set out in this Communication will pave the way for a more effective and focused EU cooperation in the protection, preparedness and response against chemical, biological, radiological and nuclear threats. The Commission encourages Member States to take advantage of the various opportunities set out in this Communication, and invites the European Parliament and the Council to endorse this action plan and to actively engage in its implementation, in close cooperation with all relevant stakeholders. The Commission will review progress at the latest after two years.

Other relevant documents

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

This document is an EU risk assessment tool and mapping guidelines for disaster management, based on a multi-hazard and multi-risk approach, covering in principle both natural and man-made disasters. Its main objective was to contribute to establishing a coherent risk management policy by 2014. At the core, the tool attempted to standardise to a certain extent the nature of the risk assessments carried out within the different Member States so they are more comparable.

The guidelines are mostly addressed to national authorities and other actors involved in the elaboration of national risk assessments, including regional and local authorities involved in cross border cooperation. They focus on the processes and methods of national risk assessments and mapping in the prevention, preparedness and planning stages, as carried out within the broader framework of disaster risk management. The guidelines are based on a multi-hazard and multi-risk approach. They cover in principle all-natural and man-made disasters both within and outside the EU11, but excluding armed conflicts and threat assessments on terrorism and other malicious threats.

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

The EU Host Nation Support Guidelines (EU HNSG) aim at assisting the affected Participating States to receive international assistance in the most effective and efficient manner. These guidelines are not binding. Instead, their fundamental goal is to provide guidance and support. They are based on experiences and lessons learned by the Participating States during emergencies, exercises, and training and incorporate the existing relevant international documents. They also include procedures aimed at ensuring optimal

information exchange between requesting, transit and assisting the Participating States and the Monitoring and Information Centre (MIC).

All in all, the EU HNSG constitutes a remarkable attempt to provide support to Member States that are facing EU bureaucracy. It also contributes to harmonise their responses to major crises, which could facilitate a faster and more efficient approach.

- EU Parliament Resolutions

There are a few resolutions of the European Parliament that are relevant to CBRNe response. The main ones are the following:

- Resolution of 19 June 2008 on stepping up the Union's disaster response capacity,
- Resolution of 21 September 2010 on the Commission communication: A Community approach on the prevention of natural and man-made disasters.

Resolution of 19 June 2008 establishes that coherence and coordination between different policy areas and institutions at different levels (local, national, European) will lead to more effective and visible EU disaster management. Within the document it is said the following:

> [...] work planned by the Commission to develop a knowledge base on disaster scenarios, capacities needed and available, and the impacts of various options to fill any identified gaps should not be used to delay important proposals for the protection of people, property and the environment from disasters.
>
> [...] the Commission's approach should cover the full disaster cycle from prevention to recovery, and natural disasters, including extreme droughts, and man-made disasters occurring in the Union or in third countries.

Resolution of 21 September 2010 highlights the serious consequences for the economic and social development of regions and member states that natural and man-made disasters have. It is indicated that the main objective of disaster prevention is:

> to safeguard human life, the safety and physical integrity of individuals, fundamental human rights, the environment, economic and social infrastructures, including basic utilities, housing, communications, transport and cultural heritage.

Regarding the importance of a proactive approach to these phenomena, the following is established:

> a proactive approach is more effective and less costly than one based simply on reacting to disasters; takes the view that knowledge of the local geographical, economic and social context is fundamental to the prevention of natural and man-made disasters

- Member States' Preparedness for CBRNE threats (2018)

As it is said in the document, "this study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Special Committee on Terrorism outlines the threats posed by Chemical, Biological, Radiological and Nuclear (CBRN) weapons, examines how well Europe is prepared for these threats and assesses where preparedness and response could be improved" (Member States' Preparedness for CBRNE threats , 2018).

The investment in research and development in CBRNe by the European Union is addressed in section 3.5 in the following manner:

> A considerable amount of money has been invested in Research & Development (R&D) to improve preparedness and response to CBRN events. The Preparatory Action on "Enhancement of the European industrial potential in the field of Security Research 2004–2006" (PASR) focused in particular on the development of a European security research agenda to bridge the gap between civil research supported by EC Framework Programmes and national and intergovernmental security research initiatives. In this initial period, in total EUR 65 million were allocated to such research. Security research became afterwards an integral part of the 7th RTD Framework Programme (2007-2013) – FP7, with a total budget of about EUR 1.35 billion. The key activities in this area relate to restoring safety and security in case of crisis.
>
> The current EU framework programme for Research and Innovation for the period 2014–2020 (Horizon 2020) has increased the amount allocated to security to EUR 1.65 billion.
>
> This research has mainly focussed on improving methods for detection, decontamination and training. One of the biggest projects to be funded was EDEN, a demonstration project involving a consortium of 15 EU Member States. Its aim was to develop and ensure the resilience capacity of European societies and focussed on prevention, preparedness and response. The goal was to integrate and co-ordinate existing EU capacities and competences to deal with the CBRN threat.
>
> Although all of these projects have advanced European capabilities for dealing with CBRN threats they have not been focussed on the research and development of medical countermeasures for unmet needs for countering CRRN threats. In the US, the Centers for Disease Control and Prevention (CDC) and the Biomedical Advanced Research and Development Authority (BARDA) has been an instrumental tool in driving the research and development of medical countermeasures for procurement by funding companies and academics to develop products. This funding is allocated on a constantly reviewed threat perception level form the US government.
>
> Europe has, as yet, not taken such an approach. However, on 26 March 2018, the Commission published a Roadmap on protecting citizens against health threats. Even though not legally binding, the Roadmap lays out the Commission's thinking for a long term strategy based on three pillars. One of the pillars is to strengthen the impact of

> research and innovation and the development of innovative medical countermeasures including via new models of collaboration with the private sector.

The significance of the level of investment on CBRN is highlighted in this document. In fact, PROACTIVE is receiving funding from the European Commission under the H2020 funding scheme. EDEN, a project in which certain members of the PROACTIVE consortium participated, is also mentioned. It could be said that, according to this text, the project PROACTIVE does not focus on the areas within CBRNe research that are the most funded at the moment (methods for detection, decontamination, and training). This makes it even more important as it can lay the foundations for future research on preparedness and response with a focus on vulnerable individuals.

- EU preparedness against CBRN weapons [Workshop report] (2019)

This document summarises a workshop on the possible intervention of the military in CBRNe events and the challenges that would be posed by it. It is introduced in the following way:

> The European Union faces an increasingly challenging security environment, with a climate of international instability and a level of tension not seen since the end of the Cold War. Repeated chemical attacks by both State and non-state actors in the context of the Syrian conflict, the Novichok attack in Salisbury and the disruption of two ricin terror plots in Germany and in France in 2018 came all as stark reminders that the threat remains real and that Member States could be affected. In this context, the European Union (EU) continues to strengthen its capacities in the field of CBRN preparedness and response. The use of EU mechanisms and Member States' military assets is one of the possibilities for strengthening prevention capacities that must be explored more thoroughly.

The conclusion explains the difficulties and opportunities created by the use of military resources in the event of CBRNe events.

> In conclusion, the capabilities of the armed forces of EU countries could indeed prove very useful in the event of a large-scale CBRN incident on the European territory, provided they are not already engaged elsewhere. But this contribution can only be effective if some conditions are met: first, prior planning taking into account the specificities, updated capacities and therefore the real possibilities of each MS; potentially, to the extent that it is reasonable, an adjustment of the capacities held by each MS so that they can be better adapted to the needs of civil interventions; - and above all a joint preparation. This preparation should involve the governmental level of the EU Member States (Ministries in charge of relief, care, transport and defence), with a dialogue between the rescue and civil health services and armed forces specialists. It should also organise the training of military personnel in the conditions that would be encountered and according to the specific doctrines of intervention in a civilian environment.

The PROACTIVE consortium does not include any military partner. Moreover, none of the Advisory Boards established within the project have representatives coming from armies or

military institutions. However, under the framework of PROACTIVE's cooperation with the eNOTICE project, the PROACTIVE consortium has established relations with military stakeholders, such as the Italian army. In any case, the main aims of the PROACTIVE project (contributing to the standardisation of the CBRNe response procedures at the European level and creation of toolkits) do not have the potential to be used for military ends (dual-use).

3. PROACTIVE ETHICAL FRAMEWORK

3.1. Introduction

The main objective of the PROACTIVE ethical framework is to support the consortium partners in identifying ethics requirements in regard to CBRNe response at the EU level, focusing on emergency assistance for vulnerable groups. In establishing the PROACTIVE ethical framework, we draw from the results of a comprehensive literature review of ethics of disaster done under Task 8.1. The ethical framework aims to provide input to the scenario development and evaluation methodology (WP6) and to inform the consortium partners of the ethical governance framework that will guide the research activities and evaluations of procedures and tools (WP8 and WP10).

Medical articles for general audiences often use the terms "in vitro" and "in vivo" to describe medical research and studies. *In vitro* is Latin for "in glass": it describes medical procedures, tests and experiments that researchers perform in a controlled environment, such as a test tube or petri dish. *In vivo* is Latin for "with the living": it refers to tests, experiments and procedures that researchers perform in or on a whole living organism, such as a person, laboratory animal or plant (Eldridge, 2019).

This terminology is useful to clarify the distinction between research ethics and subject matter ethics in the context of PROACTIVE: *research ethics*, as "in vitro" represents the moral principles and the procedures that govern how researchers carry out studies and simulations with people, for research purposes; *subject matter ethics,* as "in vivo" represents the moral principles and the procedures that govern the real life circumstances of practitioners dealing with citizens.

This PROACTIVE Ethical Framework supports the consortium partners to identify the subject matter ethics, the "in vivo" ethics requirements regarding CBRNe response at the EU level, focusing on the emergency assistance of vulnerable groups. In addition, deliverable

8.3 *Materials and briefings for PROACTIVE exercises* and D7.4 *Data management Plan and Research ethics* underline the “in vitro” aspects for PROACTIVE activities.

3.2. Methodology

3.2.1. Literature search

The literature for the ethics section was collected from a variety of sources in a number of stages:

- Keyword searches in relevant academic databases;
- Follow up author searches;
- Official documents and legislation from Websites;
- Key Word Web Searches;
- European Projects related with the fields of research (CBRNe, disaster management, ethics of disaster).

Keyword searches in relevant academic databases: two academic databases were searched using keywords (PROQUEST Central and Web of Science). The list of keywords used is shown in the Table 3. The keywords shown in the Table 3 were combined in a variety of ways, depending on the database being searched.

From each relevant academic database, references were identified and imported into a bibliographic database.

Table 3 Keywords used in the ethics literature review

Category	Keywords
CBRNe	CBRNe incidents, CBRNe disasters, ethics
Disaster management and emergency management	Disaster response, disaster preparedness, emergency management,
Vulnerability	Vulnerable citizens, vulnerability, ethics, resilience
Ethics	Ethics Research ethics Ethics decision making Human rights Ethics principles

Follow-up author search: Using the bibliographic database, key papers and books were identified. Follow-up database searches and Web searches were then performed for the key authors associated with these papers and books, as were those referenced in the text and deemed central to the objectives of the Deliverable. Systematic reviews of documents and dedicated book chapters were particularly useful to identify the main areas of ethics research in disaster studies. These include:

- Etkin and Timmerman (2013). Emergency management and ethics, in International Journal of Emergency Management, Vol 9, No4, pp 277-297.
- Jennings, B., & Arras, J. (2008). Ethical Guidance for Public Health Emergency Preparedness and Response: Highlighting Ethics and Values in a Vital Public Health Service.
- Leider et al., (2017). Ethical Guidance for Disaster Response, Specifically around Crisis Standards of Care: a systematic review, American Journal of Public Health (AJPH) 107(9):e1-e9.
- Mitrovic, V.L., O'Mathuna, D.P., & Nola, I.A. (2019). Ethics and floods: a systematic review In Disaster Med Public Health Prep; 13(4) 817-828.
- O'Mathuna, D.P., & Beriain, I.M. (ed) (2019). Ethics and Law for Chemical, Biological, Radiological, Nuclear and Explosive Crises, Springer.
- Rebera, A., Rafalowski, C. (2014). On the spot ethical decision-making in CBRN response In Science and Engineering Ethics 20(3):735-752.
- ten Have, H. (2018). Disasters, Vulnerability and Human Rights In Mathuna, D.P., Dranseika, V., Gordijn, B. (ed) (2018) Disasters: Core Concepts and Ethical Theories, Springer
- Zack, N. (2009). Ethics for Disaster, Cambridge Scholar Publishing, Newcastle upon Tyne, UK.

Official documents and guidelines from websites: International Organisations' websites were used to gather information from official reports on the ethics of disaster management, relevant legislation related International Human Rights Law, European Convention of Human Rights, Convention on the Rights of Persons with Disabilities and its Optional Protocol. These included:

- Council of Europe (http://hub.coe.int/what-we-do/human-rights/european-convention),
- United Nation Human Rights Council (https://search.ohchr.org/results.aspx?k=ethics#k=disaster%20ethics),
- International Federation of Red Cross and Red Crescent Societies (IFRC), (https://www.ifrc.org/en/what-we-do/disaster-management/responding/ethics-in-disaster-response/)
- EUR-OPA Major Hazard Agreement (https://publicsearch.coe.int/#k=ethics#f=%5B%5D#s=51).
- United Nation Department of Economic and Social Affairs ((https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html)
- World Health Organisation (WHO) (https://www.who.int/emergencies/training)
- World Health Organisation, Institutional Repository for Information sharing (https://apps.who.int/iris/discover?query=ethics)

Web-Searches; Relevant keyword searches (see Table 3) were also carried out using the Web Search Engine Google Scholar and Google. The searches revealed further resources including news reports and conference proceedings.

European projects: The CORDIS database search revealed a list of relevant projects for this review:

- CATO (CBRNE crisis management architecture, technologies and operational procedures) ID 261693
- IF-REACT (Improved First Responder Ensembles Against CBRN Terrorism) ID 285034
- SAFE-ZONE (Fully integrated CBRN incident management system for public safety and private venues with large crowds) ID 816230
- OPSIC (Operationalising psychosocial support in crisis) ID 312783
- ISAR+ (Online and mobile Communication for crisis response and search and rescue) ID 312852
- A4A (Allert for All) ID 261732
- CARISMAND (Culture and risk management in man-made and natural disasters) ID 653 784
- BuildERS (Building European Communities Resilience and Social Capital) ID 833496
- PSYCRIS (Psycho-social support in Crisis Management) ID 312395
- DARWIN (Expecting the Unexpected and how to respond) ID 653289
- TACTIC (Tools, methods and crisis) ID 608058
- PRACTICE (Preparedness and Resilience Against CBRN Terrorism using Integrated Concepts and Equipment) ID 261728
- EDEN (End-user driven demo for CBRNE) ID313077

Reports on ethics and research ethics from Project PRACTICE and Project EDEN have informed the PROACTIVE ethical framework.

3.3. Introduction to applied ethics

Ethics may be defined as the systematic reflection on what is moral, where 'morality' is defined as the totality of opinions, decisions and actions with which people express what they think is good or right (Van de Poel and Royakkers, 2011). The ethical questions are related to the 'good life', moral obligations and 'just' society (Gert 2002).

One of the sub-disciplines of ethics is normative ethics, the specific discipline within which is found the domain of disaster ethics. Normative ethics involves prescribing what is right and wrong, good and bad, or just and unjust in specific cases, and it concerns the full range of ethical questions that people and society face. Van de Poel and Royyakers (2011) present a summary of the three main theoretical frameworks in normative ethics: consequentialism, deontology, and virtue ethics showing how each propose a different way of reasoning about what is 'right' or 'wrong':

> **Consequentialism** is represented by the class of ethical theories which hold that the consequences of actions are central to the moral judgement of those actions. The most known type of consequentialism is utilitarianism, based on two principles: *utility principle* (Jeremy Bentham) – one should choose those actions that result in the greatest happiness for the greatest number, and *freedom principle* (John Stuart Mill) –

everyone is free to strive for his/her own pleasure as long as they do not deny or hinder the pleasure of others. The freedom principle is known also as no harm principle – one is free to do what one wishes, as long as no harm is done to others.

Deontology, also known as **duty ethics**, is represented by the class of approaches in ethics in which an action is considered morally right if it is in agreement with a certain moral rule (law, norm or principle).The best known system of duty ethics has been developed by Immanuel Kant; in his opinion, man himself should be able to determine what is morally correct through reasoning and independent of external norms, such as religious norms. The idea behind this is to place a moral norm upon ourselves and obey it as our duty. It is only then that we are acting with good will. There is one universal principle from which all moral norms can be derived: *categorical imperative*. An imperative is a prescribed action or an obligatory rule. The categorical imperative was formulated by Kant in different ways, but the most known is *reciprocity principle*: "act as to treat humanity, whatever in your own person or in that of any other, in every case as an end, never as a means only". His reflection on autonomy and self-legislation leads him to argue that the free will of all rational beings is the fundamental ground of human rights. Kant stresses the rational nature of humans as free, intelligent, self-directed beings. The reciprocity principle tells us that we should respect people as people and not "use" them.

Utilitarianism and Kantian theory are both theories about criteria concerning action. **Virtue ethics** focuses on the nature of the acting person. This theory indicates which good or desirable characteristic people should have or develop and how people can achieve this. Virtue ethics is based on the notion of humankind in which people's characters can be shaped by proper nurture and education, and by following good examples. The central theme is good lives. To this purpose, developing good character traits, both intellectual and personal character traits, is essential. These characteristics are called virtues. The virtues have traditionally been classified into intellectual virtues such as practical wisdom, and moral virtues such as courage, justice, honesty and integrity (MacIntyre 1984).

Applied ethics can be considered a sub-discipline of normative ethics as it is concerned with questions of what is right and wrong, good and bad, just and unjust in a specific social domain; examples are bioethics, environmental ethics, healthcare ethics, ethics and war, ethics and technology, etc. Professional ethics is a form of applied ethics that is concerned with specialists – such as doctors, nurses and lawyers – as opposed to their field (Almond 2005).

Applied ethics involves deliberating over specific situations. According to Beauchamp, 'principles must be made specific for the context; otherwise moral guidelines will be empty and ineffectual' (Beauchamp, 2003). For example, healthcare professionals have a duty to care for individuals; emergency professionals, on the other hand, are arguably more likely to compromise the security of one individual in order to safeguard that of many others. In

this sense, professional ethical considerations are more oriented towards the well-being of others, although the interpretation and scope of well-being may differ between professional domains.

To deliberate over specific situations often leads to a conflict of moral values. For example, human rights are basically moral values and they often contradict each other – the privacy of a public figure and free speech of a journalist is an example. It's not obvious to claim that some human rights are more important than others and, therefore, one will have difficult choices to make between respecting the rights of one person or another. The prioritisation of moral values is therefore at the heart of the discipline of applied ethics.

The perspective from which an individual considers a situation is likely to determine what constitutes an ethical problem. For example, those who draft policy may not face the same problems as first responders who implement a policy. Policymakers and managers are responsible for maximising the impact of their resources, whereas frontline staff are responsible for maximising the outcome of every action. Van de Poel and Royakkers (2011) have characterised an ethical problem as follows: (1) the problem cannot be thoroughly described before it arises; (2) the problem unfolds concurrently with the decision-making process; (3) the problem does not lead to a single best solution; and (4) the possible alternatives for action are widespread.

3.4. State of the art: Ethics in emergency management related fields: disaster response, public health, CBRNe incidents & vulnerability

3.4.1. Disaster ethics: understanding broader ethical themes

Disease outbreaks, CBRNe incidents and other natural hazards based and man-made disasters have pushed emergency management systems to identify and refine preparedness protocols for disaster response. Ethical guidance, alongside legal and medical frameworks, are an increasingly common component of disaster response plans (Leider et al., 2017).

Disaster ethics is a developing field of applied ethics that identifies and explores the ethical issues related to disasters (Phillips et al., 2009). It includes a number of fields, including preventive ethics, ethics of response, and post-disaster ethics (Hanfling et al., 2012). Preventive ethics, for example, elaborates a set of ethical principles for disaster protocols aimed at preventing disasters, reducing damages or injuries from disasters, and overcoming existing vulnerabilities (Christian et al., 2014).

During disasters, ethics can be perceived and prioritised differently by the community, emergency teams, volunteers, medical professionals, engineers, politicians, and so forth (Mitrovic et al., 2019). Disasters vary with respect to the place, time and consequences, and such ethical questions do not always have a 'one-size-fits all' answer (Karadag and Hakan 2012). Ethical dilemmas arise when concerns about whole populations conflict with

individual concerns. How will ethical disagreements be resolved? Does each disaster type need a distinct ethics, leading to, for example, a distinct type ethics? How will ethical principles be applied? (Mitrovic et al., 2019). Most ethical dilemmas involve choices between conflicting moral codes and sometimes equally undesirable alternatives (Jenson (ed),1997).

In a systematic review of disaster ethics related to floods, Mitrovic et al. (2019) has identified 10 ethical themes, each with related ethical subthemes: (1) Communication; (2) Environmental Ethics; (3) Ethical Reflection; (4) Flood Risk Management; (5) Health and wellbeing; (6) Justice; (7) Professional Ethics; (8) Research Ethics; (9) Virtue ethics; and (10) Vulnerability. We will adapt and present them briefly (including the bibliographical references) as they provide a good summary of the ethical challenges related to the broader field of disaster ethics.

- **Communication** is an important theme due to the ethical responsibility to provide information that is "essential, truthful, and useful" (Srinivasan, 2005). Communication should be clear and effective, explaining the technical terms, and should also convey care and compassion (Gaitonde and Gopichandran, 2016). Communication breakdowns lead to anxiety and contribute to damages and losses. Poor communication can create confusion and even conflict between agencies involved in response. Three subthemes are identified within communication. One is how the ethical principle of *autonomy* underlies the requirement to provide accurate information and thereby, allow decision-makers to make informed decisions (Morss and Wahl, 2007).The second subtheme addresses *community engagement*: this is related to a paradigm shift within risk management from a "top-down" approach to communication, where experts provide information to citizens, to active engagement between experts and citizens throughout planning. (Parkash, 2012). The third subtheme underlines the importance of *cultural values* in communication. Cultural differences contribute to ethical conflicts. Understanding different cultural values is crucial for effective communication in multicultural situations (Moatty and Vinet, 2016).

- **Environmental ethics** underlines the broad concern of how human activities influence the environment. Environmental ethics overlaps with justice and shows how human decisions are leading to environmental issues such as deforestation, soil degradation or chaotic urbanisation (Glantz and Jamieson, 2000). The main important subtheme is the link between development and sustainability (Hugo, 1996).

- **Ethical reflection** is sound decision-making that ensures the right thing is done for the right reasons (Fahey, 2007). Disaster management requires technical knowledge but is incomplete without ethical knowledge to maximise public goods, minimise harm, and make disaster mitigation and management systems fair and equitable (Simpson et al., 2015) Ethical reflection develops the capacity to act responsibly toward others, particularly the vulnerable (Fahey, 2007). Ethical reflection can be complex and messy when undertaken with imperfect knowledge and in the midst of

uncertainty. Some professionals are less familiar with conflicts of values and need to develop ethical reflection skills, along with their "moral imagination" (Lane, 2012).

- **Flood risk management** covers the aspects of reducing the likelihood and impact of floods. If adapted to the general aspects of risk management, the ethical issues frequently raised are linked with preparedness: better preparedness brings better responses, generating an ethical obligation to prepare well so that communities become "resilient, responsive, and adequately equipped" (Gaitonde and Gopichandran, 2016).

- **Health and wellbeing** is a theme bringing together several related subthemes. The ethical principle of beneficence maximises benefits over risks and harms and motivates people to help after disasters (Rossano, 2016). Beneficence should be based on the needs of those impacted by disasters and take into account justice. Beneficence not only concerns individuals, but also must address social goods. This can lead to ethical dilemmas, like, for example during floods, when one area is flooded to reduce the harm to another area, or when present needs are relieved at a cost to future generations. One of the subthemes is *harm minimisation*, with "do no harm" a core ethical obligation. Particular attention should be given to those with heightened vulnerabilities and to interventions causing unintended harm (Fahey, 2007). Difficult ethical dilemmas arise when some people are harmed to reduce others' harm, as, for example, when dam spillways are opened (Simonovic, 2011). Another subtheme, *health risks*, points to an ethical obligation to prepare well for disasters. Medical and public health systems should be prepared for disasters, access should be equitable and culturally sensitive, and practice should be evidence-based (Malik, 2011). An important subtheme is *animal health* because of the close connection in some cultures between animal and human health. Sometimes animals are part of the family, and people seek help for them after disasters. On the other hand, some animal illnesses spread to humans and this should also be addressed (Macpherson and Akpinar, 2015).

- **Justice** is an important ethical principle providing context for balancing benefits and harms and addressing autonomy (Rizza and Pereira, 2014). According to Rawls's theory, justice calls for the preferential treatment of the poor (Glantz and Jamiesom, 2000). An important value in justice is fairness, but the application often leads to dilemmas. For example, decisions made to allow one region to flood to protect another region on the basis of larger social benefit are controversial, sometimes leading to unrest (Morss and Wahl, 2007). *Injustice* is a subtheme identifying ways that resources are distributed. Relief could be denied to certain people, based on discrimination, disrespecting people's dignity, and violating human rights (Malik, 2011). Minorities, the poor, and those with mental disabilities could suffer disproportionately in disasters (Dennis et al., 2006).

- **Professional ethics**. Professional ethics are important for credibility, particularly with societal and environmental issues (Parkash, 2012). When this is lacking, unethical practices undermine recovery and the willingness of others to help (Jurkiewicz, 2009). Validated competency is an important component of professional ethics (Dennis et al., 2006). *Media ethics* is a subtheme mentioned very often. The media are an important tool when they disseminate accurate information, but often cause harm with sensational stories. The media could create distortions when they attribute blame to individuals or groups. On the other hand, media reports of people helping one another can lead to positive community spirit and hope (Simpson et al., 2015).

- **Research ethics.** This theme arises less frequently. Research is needed into the psychological impacts of disasters and how to address them, which raises the usual research ethics issues to ensure participants are respected, fully informed, not harmed and recruited justly (Dennis et al., 2006). Sometimes, doing research immediately after disasters is not ethical since the event may deeply impact the victims, who should be allowed to focus on recovery (Moatty and Vinet, 2016). Further, the data generated by scientific research can lead to ethical debates over ownership and how to use data beneficially (Mezinska et al., 2016).

- **Virtue ethics** is a common theme, exemplified by people acting "wisely and even courageously" (Fahey, 2007). Virtues engage with questions of conscience, such as when the virtue of courage leads someone to speak the truth even with negative consequences. (Rich, 2006). People lacking certain virtues are often criticised, such as when people take advantage of distressful situations for personal gain (Jurkiewicz, 2009). A core element of virtue ethics is *trust,* which can be difficult to gain. Trust is gained by working together and sharing common experiences (Lane, 2012). During crises, trust must be nurtured by having good communication and empowering community members (Rizza and Pereira, 2014).

- **Vulnerability**. One of the most important themes is vulnerability, giving an ethical obligation to care for those at particularly high risk of harm from disasters. Heightened vulnerability arises for those over 75 years of age, minorities, the poor, and those with mental illnesses (Mariaselvam and Gopichandran, 2016). Those requiring wheelchairs and other medical equipment are more vulnerable during disasters, as are residents in jails, orphanages, and other institutions (Gaitonde and Gopichandran, 2016). In some situations, the vulnerable are actively discriminated against (Mariaselvam and Gopichandran, 2016). This should be seen as unethical, and active steps should be taken to overcome vulnerabilities (Morss and Wahl, 2007). It is an ethical priority to use recovery periods as opportunities to overcome vulnerabilities and address inequities (Moatty, 2017).

3.4.2. Standards of care in crisis: ethical duties

Another systematic review presents ethical guidance for disaster response, but from the point of view of public health, specifically crisis standards of care (CSCs) (Leider et al., 2017). The authors are taking a deontology approach in their analysis, underling the significance of ethical guidance for the public health response and clinical protocols that allow responding to disasters with morally appropriate means. In their analysis they include discussion of the different ethical duties of health care professionals, starting with the need for ethical guidelines in implementing standards of care, especially around triage, as well as the duty to care, professional norms, duty to plan, reciprocity, moral distress, research ethics and equity. We present them briefly (including bibliographical references), focusing on the issues that need to be addressed in ethical frameworks or guidance for CSCs.

- **The need of ethical justification for CSCs**: arguments for the moral and practical needs for CSCs ought to be promulgated and recognised at international/ national level, rather than having clinicians set standards locally only. This also includes the need for ethical guidance in establishing fundamental norms and ethical planning processes (Altevogt et al., 2009).

- **Triage** refers to the idea of sorting patients into groups by some set of criteria to determine priority for care. Ethical issues include the justification for triage and procedural justice issues (Christian et al., 2014).

- **International issues** are relating to ethical issues arising in international contexts, mainly about relative moral norms (Rosoff, 2015).

- **Duty to care** asserts clinicians have a special responsibility to provide care in crisis circumstances by virtue of their position and training and professional norms. The duty of care may conflict with duty to oneself or family as well as obligations to provide only the highest quality of care (Fahey, 2007).

- **Duty to plan** argues that government officials and hospital leaders have an obligation to plan for catastrophic response, as investment in training and resources may be needed it to minimise adverse effects (Pou, 2013).

- **Utilitarianism** refers to the consequentialist philosophy that is often used to justify disaster response when the stated goal is to save as many lives as possible (Wagner and Dahnke, 2015).

- **Allocation criteria** are the measures, rationale or means by which resources or access to care are given to individuals, typically to the exclusion of others in crisis situations (Daniel, 2012).

- **Equity** is a normative concept referring to treating individuals equally that are in the same situation. Among individuals that are not equally situated, this implies a fair

means of addressing procedural or distributive conflicts (Mariaselvam and Gopichandran, 2016).

- **Professional norms** are important as they underline stated positions on standards of care as well as other obligations of clinicians (Hodge et al., 2013).

- **Reciprocity** relates to the idea that, just as clinicians have a duty of care, society may have obligations to clinicians during disasters. This may include priority access to scarce resources, liability protection, a duty to plan, etc (Sevimili et al., 2016).

- **Duty to steward resources** refers to the obligation of governments and private actors to use resources efficiently in the context of disaster response to maximise the number of patients that can benefit (Hodge et al., 2013).

- **Social utility** includes notions of instrumental values of a patient to society during disaster response (such as key workers) as well as social worth of a patient more broadly (Sargiacomo et al., 2014).

- **Quarantine and isolation** include ethical considerations concerned with limiting individual liberty, but also including safety and other practical considerations (Rosoff, 2015).

The authors conclude their review recommending that ethical frameworks in the field of CSCs directly engage with these issues underlining the practical implications of those ethical norms for public health and health care practitioners.

3.4.3. Ethics of CBRNe incidents: on-the-spot ethical decision-making

In a volume dedicated to ethics and law issues in CBRNe incidents, the editors O'Mathuna and Beriain (2019) note that the ethical issues in CBRNe are only now beginning to be addressed. While the ethical issues in themselves are known to responders, further analysis and reflection is needed in order to understand the specific ethical dilemmas associated with CBRNe incidents. In academic literature direct references to CBRNe ethics are few, which is in part explained by the overlap between CBRNe ethics and other fields of applied ethics (disaster ethics, public health ethics, bioethics) (O'Mathuna et al., 2014). However, it is important to recognise that there are specific areas where CBRNe incidents raise specific ethical dilemmas: for example lose-lose situations for responders in which decision must be taken in conditions of time-pressure, information gaps, and other difficult factors related to decision making (Karadag and Hakan, 2012). Also, ethical challenges that are common in general disaster management or public health ethics could be magnified by the presence of hazardous material in CBRNe incidents (Rebera and Rafalowski 2014). For example, administering drugs, conducting triage, gathering patient consent are more difficult in CBRNe incidents due to the use of Personal Protective Equipment (PPE). From the point of view of responders, exposure to hazardous materials is a very serious risk. Also, as seen in

the COVID-19 pandemic, the duty of care that healthcare professionals owe to their patients cannot be assumed to outweigh personal interest nor the responsibilities to loved ones (Sokol 2006).

Considering that many of the professional values, ethical themes and dilemmas that we have explored in the previous sections are shared within the overlapping fields of emergency management, disaster medicine and CBRNe response, in this section we will present how situations in which on-the-spot ethical decisions in CBRNe contexts are required (Rebera and Rafalowski, 2014). This approach allows us to create the PROACTIVE ethical framework (see infra, section 3.5) which is guiding the work for PROACTIVE scenarios for the field exercises (T6.2 *Scenario development and specification of the evaluation methodology*) and will support the ethical evaluation of selected CBRNe tools and procedures (WP6 *Joint exercises, evaluation and validation of the tools* and T8.4 *Ethical and Societal Impact Assessment of project outputs*).

As mentioned by Schwartz et al. (2014), organisations have a general obligation to promote acceptable treatment of persons affected by CBRNe incidents, but they also have an obligation to minimise the psychological impact on responders. Considering this ethical dilemma, Rebera and Rafalowski (2014) propose a 'modified consequentialist approach' to on-the-spot ethical decision-making. A central value or principle - the authors give the example of 'saving lives' - forms the basis of a goal-oriented heuristic. Additional core rights and values are factored in as minimum standards beyond which any violation is unacceptable. In this respect the authors recommend that organisations involved in CBRNe incident management should develop an 'ethos' that sets the tone for all the activities and for all decisions taken by their representatives. This ethos could be organised around SOPs but needs to be supplemented by the most important values and principles that the organisation wishes to build into its work (mission statement, standard professional values). The organisational ethos must recognise that priorities may change during an incident; also, it is important that the values given by an ethos are able to be operationalised, translated into actions and decisions in the field. A high level ethos or code of conduct must be supplemented by guidance on how the core values and principles are to be respected in relation to key tasks as well as in novel or unexpected situations.

3.4.4. Vulnerability: human rights in practice

The concept of vulnerability has emerged as one of the main ethical principles in bioethics (UNESCO Declaration on Bioethics and Human Rights, 2005) and is especially important in the context of global disasters (ten Have, 2018). As an ethical principle, vulnerability directs the ethical discourse in directions that focus more on ameliorating the conditions that produce vulnerability, and also on emergency actions focused on saving lives.

Vulnerability could be defined as 'the state of susceptibility to harm from exposure to stresses associated with environmental and social change and from the absence of capacity to adapt' (Adger, 2006). From a functional approach, vulnerability is regarded as a function

of exposure, sensitivity and adaptive capacity (Gallopin, 2006). For example, when there is a threat of an infectious disease, the exposure is in principle the same for everyone, but the sensitivity is different: children and the elderly have more risks if they are affected. The adaptive capacity is better for persons who have access to medical care and medicines: the most vulnerable groups therefore are children and elderly with no, or only inadequate, access to the healthcare system. Another example is that in severe winter conditions, the exposure is in principle the same for everyone, as is the sensitivity. But the adaptive capacity is insufficient for homeless persons. This is what makes them vulnerable to cold injuries (ten Have 2018).

From the point of view of a human rights approach to disasters, vulnerability occurs because in disaster situations human rights are threatened (Hurst, 2010). Other types of vulnerability are social vulnerability and social inequalities: pre-existing conditions such as poverty, age, or disability make some categories more vulnerable than others (Zack 2009). Four categories of human rights are at stake in disasters. First is the right to the protection of life: this is the priority of disaster relief directly after the catastrophe has occurred. Second are the rights related to basic necessities such as food, health, shelter and education: these are needs included in the right to health. Third are rights related to more long-term economic and social needs (housing, land, property and livelihood). Fourth are rights related to other civil and political protection needs (documentation, movement, and freedom of expression). While the first two categories of rights are especially relevant during the emergency phase, the two last categories are particularly relevant in the recovery and reconstruction phases (Brookings-Bern Project on Internal Displacement 2008).

The human rights framework is particularly useful for prevention and preparedness; disasters have a disproportional effect on people and populations that are vulnerable, and marginalised populations will suffer most (Hurst, 2010). In this respect, international human rights law implies a universal duty to ensure health and human dignity and requests governments to protect the rights of individual citizens. This also implies an obligation for international cooperation and assistance. Disasters can be prevented and citizens made less vulnerable through reducing exposure, enhancing resilience, and providing effective mitigations. Failure to take feasible measures that would have prevented or mitigated the consequences of foreseeable disasters amounts to human rights violations (ten Have 2018).

3.4.5. Summary discussion

The state-of-the-art review identified articles and documents addressing ethics in the broader field of disaster management.

In the field of **disaster ethics**, the analysis led to identifying 10 ethical themes and several subthemes which allow us to better understand the broad ethical framework and the main associated ethical values and principles. Themes such as justice and vulnerability, virtue ethics and animal ethics are prominent, and others as research ethics and professional

ethics do not feature as much, although these are discussed elsewhere as for example in bioethics and emergency medicine (O'Mathuna et al., 2014).

Many articles and documents in the field of **ethics and crisis standards of care** underlined the deontological approach in professional ethics, focusing on the ethical duties of public health professionals. All the documents studied suggested that it is important to implement increased training in ethical reflection and decision-making for the various professionals working in the field of disasters. The goal, according to one included article, seems simple: Do the right thing (Fahey, 2007), but achieving it is more difficult: "Specifically, morally sound decisions involve good information, sound values, engagement of appropriate stakeholders, and the ability to make decisions. Seeking morally sound decisions is complex because situations often require decisions by a group (underpinned by individual decisions). These are made in the fog of incomplete or contradictory information by people applying different weights to sometimes competing values" (Fahey 2007).

The section on **CBRNe ethics** addressed with the question of how to best implement an ethical approach for response actions taken during CBRNe incidents. This included the need to support responders in on-the-spot ethical decision-making, amid extreme time-pressure, information gaps, and other stressors such as the presence of hazardous materials and the use of PPE, and underlined the need that any organisation involved in CBRNe should develop an 'ethos' of key ethical values and principles. Staff should be trained in how to operationalise the values and principles embedded in this ethos. This approach is intended to provide clarity and reassurance to the responders and other CBRNe professionals to make on-the-spot ethical decisions free from doubt (Rebera and Rafalowski, 2014).

Social justice is a broad area of ethical concern in the articles and studies related to the concept of **vulnerability.** This concept is strongly influenced by the human rights approach to disasters. Disasters have a disproportional effect on people and populations that are vulnerable, and marginalised populations will suffer most (Hurst, 2010). In this respect, international human rights law implies a universal duty to assure health and human dignity and requests governments to protect the rights of individual citizens. The economic and human toll of disasters alerts us to the need to constantly develop and re-evaluate ethical guidelines. The dignity and equal rights of all should be recognised and protected in disaster-prone societies.

The state-of-the-art review reveals a large variety of ethical issues and situations in disasters. The results have implications for those involved in Disaster risk reduction (DRR) and disaster risk management (DRM), showing that ethical issues should be considered carefully in planning for and responding to disasters.

3.5. PROACTIVE ethical framework: Ethical principles guiding disaster response

Ethical and legal frameworks provide systematic and practical approaches to the analysis of ethical issues and questions (WHO 2015). They aid decision-making by framing the ethical issue at hand (what type of ethical issue is this?), making relevant values and ethical principles explicit (what is at stake, and for whom?), providing a structure for determining how to address or resolve the ethical issue (what actions ought to be taken?), and ensuring consistency in similar situations and across decision-makers. Ethical frameworks consist of a set of procedures to be followed in addressing an ethical issue or a set of criteria to be factored into a decision, or both (p.22).

Disaster response, including CBRN emergencies has the effect of eclipsing existing rights in general and human rights in particular. When the impact of disaster is big, a state of emergency is declared; this is used as legal justification for setting aside the usual legal rules. In principle, fundamental human rights, because of their universal value have to be applied at all times and in all places, should be enforced including in times of disasters. Seen in this way, the human rights framework should be used to fill a legal vacuum or to strengthen the basic duties of the various parties involved in disaster, when the usual legal rules have been suspended. In a disaster parties are also faced with choices of ethical nature.

In establishing the PROACTIVE ethical framework we have adopted the human rights approach to disaster management. As seen in the literature review, the ethical themes and subthemes presented are relevant for all types of disasters, including CBRNe incidents. Further work will be performed during the course of the project to adapt the ethics requirements to the specific PROACTIVE scenarios for the field exercises (WP6) and for CBRNe tools and procedures selected for ethical evaluation. This will be conducted in WP8, (T8.4) and delivered as D8.4.

We list here in brief the main ethical values and the main ethical principles & standards of the PROACTIVE ethical framework.

Ethical values (Rice et al., 2017, p.119): equality, transparency, accountability and empowerment. Specifically, *equality* refers to ensuring those in need receive the resources they are entitled to, while *transparency* ensures those affected by the disaster have full access to information in order to make informed decisions. *Accountability* refers to holding those with power and ability to distribute those resources responsible for doing so. While distributing resources and rebuilding post disaster, it is essential that those affected are *empowered* through participation in the recovery in order to ensure sustainable effects.

In a document commissioned by Council of Europe (EUR-OPA, Resolution 2011-1) the author underlines the ethical principles of the whole disaster cycle: from prevention to reconstruction via the emergency phase, irrespective of the duration of the disaster (sudden or progressive) or its context (simple or complex emergency).

Considering the impact of disasters on human rights during response phase, in the absence of a specific universal binding legal instrument, and especially where a state of emergency

has been declared, it is imperative to formulate the essential ethical principles as part of a minimum set of ethical standards to guide the various parties in action (idem, pp 27-31).

The author underlines 9 ethical principles:

- **Humanitarian assistance:** all persons receive immediate assistance, including the benefit of basic health services. Humanitarian assistance is provided fairly, impartially and without discrimination, showing due regard for the vulnerability of victims and for individuals' and groups' specific needs.

- **Information and communication during disasters:** all persons, local and regional authorities and non-governmental organisations affected by disasters are informed of and are entitled to participate in making decisions in response to disasters. They receive, in their own language, easily understandable information about the nature and extent of the disaster, the emergency measures planned in response to it, the times and places at which food and drink will be distributed, the location of emergency medical facilities, temporary housing arrangements and the arrangements for and destination of any population movements that are planned.

- **Compulsory evacuation of population:** compulsory evacuation can only take place if a clear explanation has been given of the potential risks involved in the case of non-evacuation. Persons who refuse to evacuate do so at their own risk and should not endanger the lives of rescue workers through their conduct

- **Respect of dignity:** the dignity of all persons who are victims is respected, particularly concerning his/her security, physical safety, access to food and clean water, hygiene, temporary housing, clothing and if necessary essential emergency medical and psychological care

- **Respect of persons:** personal rights are respected, particularly the right to one's own image and the right to privacy, so that the presence of the media does not result in abuses

- **Emergency assistance for the most vulnerable persons:** allowing for local circumstances and without prejudice to the priority assistance to be given to all who have a chance of survival, priority for humanitarian assistance, first aid and emergency evacuations go in priority to the most vulnerable people, such as pregnant women, children, people with disabilities, elderly people, the ill and the wounded. States train and provide special equipment to members of the emergency services and doctors and nurses so that they are able to search for and provide first aid to the most fragile persons.

- **The importance of rescue workers:** Irrespective of their nationality, theirs status or their function and regardless of the seriousness and nature of the disaster, both

civilian and military rescue workers, including any private security forces, behave with dignity, keep their anxiety of fear under control, keep calm and ensure that they never infringe the fundamental rights of the people they are rescuing.

- States, international organisations and all institutions connected with humanitarian assistance in response to disasters take every possible measure to guarantee to rescue workers the necessary conditions for them to carry out their work properly, including the conditions needed to protect their dignity, safety, and physical and psychological integrity.

- States, regional and local authorities and rescue training establishments provide special training to rescue workers covering human rights and ethical principles in times of disaster and the special arrangements for dealing with persons with disabilities and the most vulnerable persons.

- **Measures to safeguard and rehabilitate the environment:** In view of the importance of the environment to human survival, practical measures are taken to ensure the quickest possible safeguarding and rehabilitation of environmental assets and the re-establishment of environmental quality.

- **Measures to safeguards and restore social ties:** considering the importance of social ties to human survival, practical measures are taken to ensure that social ties are restored as quickly as possible, in particular by foreseeing meeting places, place of worship and places for leisure activities.

In respect to Project PROACTIVE, we recommend that these ethical principles considered for the *Scenario development and specification for the evaluation methodology*, in the Task 6.2.

3.6. Ethics principle guiding CBRN response

In the project EDEN “Report on ethical issues of response phase” (EDEN D81.2, 2014), the authors present an ethics framework applicable to the CBRNe incidents response phase. The authors adapted the ethical model proposed by the University of Toronto Joint Centre for Bioethics Pandemic Influenza Working Group (2005) to CBRNe incidents, noting that not all the principles would be applicable to all CBRNe incidents and the balance between values might change from situation to situation.

Restriction of individual liberty: restrictions to individual liberty will probably be necessary in order to protect the public from serious harm. In these cases, public health should prevail against individual liberty. However, these restrictions should always apply:

- respect human dignity (individuals should never be considered as mere means);

- be proportional, necessary, and relevant;

- employ the least restrictive means;
- and be applied equitably (unjustified exceptions should be carefully avoided).

Proportionality: The principle of proportionality involves a balance between the level of an incident and the measures undertaken as a consequence. In terms of rights/duties balance, “Proportionality requires that restrictions to individual liberty and measures taken to protect the public from harm should not exceed what is necessary to address the actual level of risk to or critical needs of the community” (idem p.6).

Reciprocity: Reciprocity requires that society support those who face a disproportionate burden in protecting the public good, and take steps to minimise burdens as much as possible. Adopting measures which supports the first responders, taking care of their families while they accomplish with their duties, etc., are good examples of how reciprocity can be demonstrated.

Clarity, transparency and trust: Decision makers will be confronted with the challenge of maintaining stakeholders trust while simultaneously implementing various control measures during a CBRNe incident. Transparency is an essential tool in order to maintain the trust but could be difficult to achieve in a CBRNe major crisis Therefore, an adequate communication policy is both an important practical tool and a moral imperative.

Solidarity: It is important to think about solidarity in terms of humankind scope, as far as the dimension of a CBRNe major crisis situation often overwhelms the national scope. International cooperation is a key factor in building an optimal response to these incidents.

Respect for human dignity, non-discrimination and equity: According to the principle of respect for human dignity, we should never use as a human being as a means, even if this could lead to a better final result in terms of saving human lives. Respecting the human dignity involves also the principle of non-discrimination on the basis of his/her race, nationality, religious beliefs, age, etc. Respecting the principle of equity, however, ask to apply the discrimination principle in favour of vulnerable sections of the population, and also in favour of those who are especially committed to risk their lives or health in order to mitigate the consequences of the crisis.

During the planning phase and the implementation of the PROACTIVE joint field exercises, the consortium will strive to implement the seven ethical goals *designed to inform both the content of preparedness plans and the process by which they are devised, updated, and implemented (Jennings and Arras, 2008):*

1. **Harm reduction and benefit promotion.** Emergency preparedness activities should protect public safety, health, and well-being. They should minimise the extent of death, injury, disease, disability, and suffering during and after an emergency.

2. **Equal liberty and human rights.** Emergency preparedness activities should be designed so as to respect the equal liberty, autonomy and dignity of all persons.

3. **Distributive justice.** Emergency preparedness activities should be conducted so as to ensure that the benefits and burdens imposed on the population by the emergency and by the need to cope with its effects are shared equitably and fairly.

4. **Public accountability and transparency.** Emergency preparedness activities should be based on and incorporate decision-making processes that are inclusive, transparent, and sustain public trust.

5. **Community resilience and empowerment.** A principal goal of emergency preparedness should be to develop resilient, as well as safe communities. Emergency preparedness activities should strive towards the long-term goal of developing community resources that will make them more hazard-resistant and allow them to recover appropriately and effectively after emergencies.

6. **Public health professionalism.** Emergency preparedness activities should recognise the special obligations of certain public health professionals, and promote competency of and coordination among these professionals.

7. **Responsible civic response.** Emergency preparedness activities should promote a sense of personal responsibility and citizenship.

In respect to Project PROACTIVE, these ethical principles were considered in the scenario development for the field exercises in Task 6.2 are also explicitly included in D6.2.

3.7. Ethics impact assessment framework

In project PRACTICE (FP7 Project PRACTICE) one of the objectives was to evaluate from the ethics point of view the Toolbox and the tools developed during the implementation of the project. In that respect, the project ethical team developed two ethical tools aiming at technology developers, policy-makers and LEA officials in order to facilitate consideration of ethical issues that may arise in their undertaking of CBRN incidents: *PRACTICE Ethics Checklist for Toll Providers* and *PRACTICE Ethics Evaluation Template* provides the background information needed for a thorough assessment.

The *Ethics Evaluation template* (Stănciugelu et al., 2014) was constructed as a package of interdependent values that underline the work of response teams and emergency medical staff when confronted with disaster situations and was used to validate the PRACTICE Tools and Toolbox deployed during the PRACTICE Validation Exercises. The values and principles overlap with the principles drawn from fundamental rights as presented in the previous sections, as they share the same philosophy of ethics embedded in the Declaration of Human Rights.

The *Ethics Checklist for Tool Providers* (Stănciugelu et al., 2014) serves as a heuristic tool. It provides the user with a framework to identify potential ethical issues associated with CBRN response tools. As authors mentioned (idem p.1), this is important because CBRN

responses have traditionally been treated as primarily a technical and/or organisational challenge where technological advances were either generally understood as something positive or seen through a purely consequentialist ethical lens (that is: means and right secondary as long as outcome positive). However, CBRN response tools raise a wide range of issues touching upon the fields of disaster management ethics (e.g. individual liberty versus collective protection from cross-contamination), technology-related ethics (e.g. track & trace and privacy/data protection), research ethics (e.g. how to organise realistic exercises without violating rights of physical integrity), and others.

The PRACTICE check-list consists of a matrix: in the rows of the matrix, a catalogue of rights/norms is identified and categorised into six generic sections: fundamental rights, procedural rights, distributive rights, intergenerational issues, informational rights and dual use. In the columns, questions of potentially arising/observed/undertaken ethical issues and their management in relation to the concept of the goal, use of the tool and production of the tool are listed.

In respect to project PROACTIVE, both the ethics tools will be used for evaluation purposes in WP6 *Joint exercises, evaluation and validation of the tools* and in Task 8.4 *Ethical and societal assessment of PROACTIVE outputs*.

3.8. Ethics framework of emergency assistance to vulnerable people

In disaster preparedness, the terms “vulnerable” or “special needs” are used to define groups whose needs are not fully addressed by the traditional service providers (OES California, 2000 p. 2). It also includes groups that may feel they cannot comfortably or safely access and use the standard resources offered in disaster preparedness, response, and recovery. This includes, but is not limited to, those who are physically and/or mentally disabled (blind, cognitive disorders, mobility limitations), limited or not native speaking, geographically or culturally isolated, medically or chemically dependent, homeless, deaf and hard-of-hearing, frail, elderly, and children.

The Recommendation 2013 - 1 of the Committee of Permanent Correspondents on the inclusion of people with disabilities in disaster preparedness and response (EUR-OPA Recommendation 2013-1, 2013) promotes that Member States integrate specialised measures for people with disabilities into national disaster risk reduction policies, planning processes, training curricula and emergency response practice, favouring, as appropriate, investment in long-term strategies that would reduce the vulnerability and exposure to disaster for people with disabilities.

One of the General Principles in the Ethical Principles (EUR-OPA, Ethical Principles on Disaster Risk Reduction and People’s Resilience) (idem, p.17) is the principle of non-discrimination: “Measures to prevent, reduce and prepare for disasters and to distribute relief and promote recovery, and also the enjoyment of fundamental rights are secured and implemented without distinction on any ground such as gender, sexual orientation, race,

colour, language, religion, political or other opinion, ethnic group, and affiliation to a national minority, socioeconomic circumstances, birth, disability, age or other status."

The main framework to discuss the ethics of emergency assistance for vulnerable groups is European Charter of Human Rights (ECHR) and the Universal Declaration of Human Rights. Of especial relevance in a time of crisis are:

- rights related to physical security and integrity (e.g. protection of the right to life and the right to be free from assault, rape, arbitrary detention, kidnapping, and threats concerning the above);
- rights related to the basic necessities of life (e.g. the rights to food, drinking water, shelter, adequate clothing, adequate health services, and sanitation) (Brookings-Bern Project on Internal Displacement, 2008).

Another relevant multinational instrument is the Convention on the Rights of Persons with Disabilities and its Optional Protocol which entered into force in 2008. According to its Article 1:

Article 1:

persons with disabilities include those who have long-term physical, mental, intellectual or sensory impairments which in interaction with various barriers may hinder their full and effective participation in society on an equal basis with others

Article 11 of the Convention dictates that in situations of risk and humanitarian emergency:

Article 11:

"States Parties shall take, in accordance with their obligations under international law, including international humanitarian law and international human rights law, all necessary measures to ensure the protection and safety of persons with disabilities in situations of risk, including situations of armed conflict, humanitarian emergencies and the occurrence of natural disasters".

However, as presented in the previous section 3.3 of this document, adapting responses to the needs of certain groups is not a violation of the principle of non-discrimination, since some people might not need as much assistance following an incident as others. In the spirit of the equity principle, to prioritise is an appropriate safeguard of victims' human rights and reflects the fact that vulnerable groups have particular needs.

In respect to Project PROACTIVE, we recommend that this ethical framework for emergency assistance for vulnerable people be considered in the WP6 *Engagement of the civil society including vulnerable citizens* and Task 5.2 *Requirements of the mobile App for vulnerable citizens.*

3.9. Vulnerability and emergency assistance; a function-based approach

Considering the concept of 'vulnerability', in the white paper for the Center for Disease Control and Prevention (CDCP) (Jennings and Arras, 2008 p. 81) the authors note that "*vulnerability is not limited to states of special physical or emotional dependency*", but also a function of social, cultural, racial, linguistic, and geographic disadvantage. Physically able-bodied and mentally capacitated persons may nonetheless be living in a condition of social vulnerability and precariousness. This form of vulnerability can be due to such factors as racial discrimination and stigma, poverty and lack of resources, lack of access to functioning and empowering social networks, or living in an area that has lack of access to services and resources or lack of access to transportation.

The concept of social and cultural vulnerability is discussed in the deliverable D83.3 "Impact on vulnerable groups" of Project EDEN (Usher, 2014): the author is considering the component concepts of integrity, self-perception and contingency (idem, p. 19), and characterises the groups based on 7 vulnerability criteria that might apply:

Table 4 Categorisation of vulnerable people

Vulnerability / Groups	Reduced mobility	Lack of autonomy	Ignorance	Poor health	High public profile	Societal margina-lisation	Obligation towards others
Minors		✓	✓				
Older people	✓	✓		✓			
Women						✓	
Pregnant women	✓						✓
Migrants			✓			✓	
Displaced people						✓	
Low-income people			✓			✓	
Homeless people		✓		✓		✓	
Illiterate people			✓			✓	
Isolated people						✓	
Institutionalised people		✓				✓	

Vulnerability / Groups	Reduced mobility	Lack of autonomy	Ignorance	Poor health	High public profile	Societal margina-lisation	Obligation towards others
Physically disabled people	✓	✓		✓		✓	
People with learning difficulties		✓	✓			✓	
People with acute medical conditions	✓	✓		✓		✓	
Carers		✓					✓
Emergency services personnel							✓
Politicians					✓		✓

In a study on the function need approach on emergency management and planning (Kailes et al., 2007), the authors argue that the term of 'special needs' or 'vulnerability' is not appropriate as the large number of heterogeneous groups it represents is too large and too diverse for the use of any single designation. The authors recommend using the category of function-based needs, as this approach leads to a common framework that "can relate functional support to functional needs, targeted at improving resource management in any type of incident" (idem, p.232). The authors propose a flexible framework build on five function-based needs: communication, medical needs, maintaining functional independence, supervision and transportation (C-MIST). Addressing functional limitations includes both people who identify as having a disability and "the larger number of people who do not identify as having a disability but have a functional limitation in hearing, seeing, walking, learning, language and/or understanding" (idem, p.234).

The function need approach has been used by the Public Health England (Carter et al., 2016) to review and update the guidance documents for mass casualty decontamination, including vulnerable groups.

In respect to Project PROACTIVE, the function-based approach was considered in WP6 *Joint exercises, evaluation and validation of the tools*, and in particular in Task 6.2 *Scenario development and specifications of the evaluation methodology*.

3.10. Ethics Impact assessment of procedures and tools on vulnerable people

EDEN Task 83.3 explores the impact of the EDEN selected tools on 'vulnerable groups' (Usher, 2014). It considers the causes, nature and extent of the impact, and examines whether it is possible to predict its social and cultural aspects. The author created a protocol that support the impact assessment process and also provides recommendations for mitigating any negative effect of the tool on vulnerable people. The impact assessment protocol consists of a scoring matrix that uses the analogy with the Hazard Identification (HAZID) process used in safety engineering. Direct impacts are considered and possible effects in the long-term are acknowledged.

The following table provides an example of the impact assessment, where impact, effect and outcome of the tools are taken into consideration in regards to vulnerable people (idem, pp 23-24).

Table 5 Example impact assessment for vulnerable groups

	Impact	Effect	Outcome	Example	Human rights implication
1.	The Tool cannot be used by vulnerable people	Vulnerable people are left exposed to the hazard	More casualties among vulnerable people	Public address systems are ineffective for hearing-impaired people	The right to life has been violated
2.	The Tool causes offence to vulnerable people, or diminishes their self-esteem, dignity or personal integrity	The negative reaction of vulnerable people disrupts proceedings and contributes to disaffection in the longer term	More casualties overall, because the Tool cannot be exercised fully and its benefits are not delivered.	Racist language or images used in information leaflets or public announcements (causing offence among immigrants)	The principle of non-discrimination has been violated

	Impact	Effect	Outcome	Example	Human rights implication
3.	The Tool stigmatises vulnerable people in the eyes of others	The negative reaction of vulnerable people and others prevents the Tool being deployed effectively	More casualties and disaffection among vulnerable people; increased negative reaction by others towards them	An evacuation procedure that appears to favour or disfavour immigrants	Principle of non-discrimination has not been applied
4.	The Tool does not recognise people's vulnerabilities	The Tool injures vulnerable people	More casualties among vulnerable people, both in short and long term	Distributing food rations that cause allergic reaction	Right to health has been violated. The principle of non-discrimination has not been applied
5.	The Tool becomes more difficult to deploy if vulnerable people are among those it affects	The difficulty of using the Tool if vulnerable people are affected means that its benefits are felt by fewer people or later than the optimum time	More casualties overall	A protocol in which decontamination starts only when everyone affected by the incident is accounted for (reduced agility of older people causes delay)	Principle of non-discrimination has not been applied
6.	The Tool provides particular assistance for vulnerable groups	The Tool reduces the effect of the vulnerability	Fewer casualties among vulnerable people	Psychological counselling	The rights of vulnerable groups have been prioritised over others.

	Impact	Effect	Outcome	Example	Human rights implication
7.	The Tool increases the risk to some people affected	A new vulnerability is created: the number of vulnerable people is increased	More casualties among vulnerable people	An evacuation procedure might increase the toxic dose received by those it delays	The right to life has been violated. The principle of non-discrimination has not been applied

In respect to Project PROACTIVE, this impact assessment protocol of CBRN procedures and tools on vulnerable people will be used for evaluation purposes in WP6 *Joint exercises, evaluation and validation of the tools* and reflected in Task 8.4 *Ethical and societal assessment of PROACTIVE outputs*.

3.11. Ethical governance framework that will guide the research activities in project PROACTIVE

Project PROACTIVE has built ethical, legal and social safeguards regarding the ethical management of volunteers (including vulnerable groups) and the proposed technical solutions and methodologies (see Deliverable 7.4 *Data Management Plan and Research Ethics)*. More specifically:

- Legal and ethical state of the art
    - Task 8.1 reviews the state of the art regarding legal and privacy issues, and relevant input will be provided in WP8 through this current deliverable D8.1.
- Ethical and societal Impact assessment for project outputs
    - Task 8.4 assesses the ethical risks associated with PROACTIVE technical solutions and methodologies, including all its resulting guidelines. The ethical and societal risk assessment methodology, conceived as a practical risk management tool, will be applied to both the results of WP3, WP4, WP5, and also to the outputs of the exercises in WP6 (ethical governance of the technology and/or value sensitive design approach). It will also contain forms for recording ethical risk assessment.
- Advisory activities in WP8
    - Task 8.2: Operationalisation of legal requirements, ethical requirements and acceptability study into recommendations and Task 8.3 Ethics briefing for project field work) complemented with a monitoring procedure (Project Ethics Officer and External Ethics Advisory Board ensures that the collection, recording, storage and any other form of use of personal data on persons identified or identifiable, even indirectly, will be made on the basis of a rigorous ethics guideline, without injuring the rights of citizens and without affecting the fundamental freedoms of the persons concerned.
- Identification and organisation of the vulnerable groups participating
    - Task 3.2 will uphold the legal requirements of confidentiality as set out in the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, GDPR). Under this Act, a person's disability status is regarded as sensitive personal information, which should enjoy higher standards of protection. All the safeguards will be included in task T8.3 *Ethics Briefing for project fieldwork*.
- Ethical screening of PROACTIVE research and deliverables

- Project PROACTIVE attributes equal importance to the ethics, legal and scientific aspects of the research process. The PEO aims to inform and advise project participants of the ethics issues which might impact the research process. Furthermore, ethical, privacy and data protection issues relevant to research and development activities must be accurately identified and addressed throughout the duration of the project.

4. NATIONAL CBRNE GUIDELINES. THE CASE OF GERMANY

This section includes a number of strategic guidelines related to CBRNe events in Germany. The reason why the PROACTIVE consortium has decided to dive deeper into the German case study has to do with the fact that one of the field exercises will take place in Dortmund (Germany). In addition to that, the consortium counts with two German partners, which has facilitated access to the guidelines examined in this section. Table 6 provides an overview of the strategies that includes their name, the organisation that issued them, the year of publication, and the type of strategy.

Table 6 Summary of CBRNe Guidelines

Name	Organisation	Year	Type of Strategy
Psychosoziales Krisenmanagement in CBRN-Lagen (Psychosocial crisis management in CBRN situations)	Bundesamt für Bevölkerungsschutz und katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance)	2009	Lock down Evacuation Disrobe Decontamination
Nationales Krisenmanagement im Bevölkerungsschutz (National Crisis Management in Civil Protection)	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance)	2008	Crisis communication
Bevölkerungsverhalten und Möglichkeiten des Krisenmanagements und	Bundesamt für Bevölkerungsschutz und katastrophenhilfe	2010	Crisis communication

Katastrophenmanagements in multikulturellen Gesellschaften (Population behavior and opportunities for crisis management and disaster management in multicultural societies)	(Federal Office for Civil Protection and Disaster Assistance)		
Risiko- und Krisenkommunikation am Beispiel von terroristisch motivierten Schadenslagen und Schadstoffunglücken: Einflussfaktoren auf dieReaktion nach Warnmeldungen (Risk and crisis communication using the example of terroristically motivated damage situations and pollutant deficiencies: Factors influencing the Reaction after warning messages)	Dr. Vanessa Schneider	2015	Risk communication in CBRN incidents
Experimentelle Untersuchung und Optimierung der Dekontamination von Verletzten bei einer C(B)RN-Gefahrenlage durch Organisationen der nichtpolizeilichen Gefahrenabwehr (Experimental investigation and optimisation of decontamination of casualties in C (B) RN threats by non-policing organisations)	Patrick Sudhoff	2016	Self-decontamination Preliminary hazard assessments (exercise) Additional safety instruction with instructions on how to behave (exercise)

Verhalten bei besonderen Gefahrenlagen (Behavior in special danger situations)	Bundesamt für Bevölkerungsschutz und katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance)	2018	Strenghtening the behaviour of affected civilians in CBRN incidents
FwDV_500 - Units in ABC-scenarios	Ausschuss Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung (AFKzV) (Committee on Fire Fighting, Civil Protection and Civil Defense (AFKzV))	2012	Disrobe Decontamination Isolation
Biological hazards I: Handbook for the civil protection. 3rd edition	Federal Office of Civil Protection and Disaster Assistance (BBK) and Robert Koch Institute	2007	Isolation of civilians suspected of decontamination Information of further treatment Evacuation Disrobe Decontamination Rerobe
SKK DV 500	Permanent conference on disaster preparedness and population protection	2008	Risk communication in CBRN incidents Disrobe Decontamination

Civil defence concept	Bundesministerium des Innern (Federal Ministry of the Interior)	2016	Decontamination Vaccines/antibiotics Potassium iodine tablets
Guide for emergency preparedness and correct action in emergency situations	Federal office of civil protection and disaster assistance	2018	
Health protection against CBRN hazard; epidemics control management	Federal Office of Civil Protection and Disaster Assistance		Evacuation Decontamination Epidemic emergency management Targeted therapy Vaccinations Disrobe
Guidance for the creation of hospital alarm and operational plans	No author	2006	Evacuation Isolation
Acting in a CBRN event. Citizen information flyer	Federal office of civil protection and disaster assistance	2018	Inform yourself Disrobe Decontaminate Enter a safe building and do not leave

THW DV 500 - Deployment in CBRN scenarios	THW	2014	Disrobe Decontamination

4.1. Psychosoziales Krisenmanagement in CBRN-Lagen (Psychosocial crisis management in CBRN situations)

Public/Responder: Responder.

Organisation: Bundesamt für Bevölkerungsschutz und katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance).

Year: 2009.

Type of incident: CBRN.

Type of strategy: Lock down, Evacuation, Disrobe, Decontamination

Summary of strategy:

Adequate medical care for those affected always has the highest priority and thus always takes precedence over psychosocial support.

Lockdown the area! In the case of mass attacks of contaminated persons, it´s a particular challenge to keep those affected at the site of the damage, to prevent the uncontrolled removal of contaminated persons as far as possible and to prepare people for waiting times.

Large-scale evacuation should be carried out.

Prepare those affected for decontamination: Contaminated people should remove their outer clothing. Delegate tasks to those who are able to do so.

Prepare affected persons for further help in the shut-off area.

Strategy for communication: No content.

Summary of communication strategy:

- Say you're there, who you are and what's happening.
- Speak, keep up the conversation, and listen actively.
- Search/offer careful body contact (hand, arm, and shoulder).
- Strengthen the self-efficacy feeling of the patient, give him/her simple tasks.

- Give information about injuries and further measures in understandable language.
- Do not lie to the patient.
- Say that everything humanly possible is being done.
- Involve family members as much as possible.
- Say when you have to leave the patient.

Under no circumstances carry out the following actions:

- make accusations,
- express alarming assessments or diagnoses,
- discuss causes,
- And minimise processes.

Rapid and comprehensive information networking of citizens, including through internet forums and telephones. Public statements can be expected from associations, federations, political parties etc. which use the damage situation to underpin their social, political or ideological positions and interests. It is expected that special interest groups will be formed as a result of the CBRN damage situation (victim protection groups, protest groups, etc.), which will appear more or less expressively in public.

It is important to give those affected an overview of the situation and to communicate what steps are being taken to improve the situation and the purpose of individual measures. Other instructions are:

- Give clear and repeated instructions to ensure that people are able to implement them, e.g. during waiting times or evacuations;
- Use positively formulated statements such as "you are safe", exclude negatively spoken words such as "danger" or "fear";
- Talk to affected persons in the danger area;
- Use body language and gestures to implement instructions and measures;
- Inform those affected promptly and credibly! It is important that information is provided promptly, directly and truthfully.

Likely public response:

Different individual reactions, range from calm behaviour to quiet or violent expressions of worry and despair to hectic activity or aggressive behaviour. Affected people wish to be brought out of the danger zone as quickly as possible or to flee Special agents or substances that can cause psychological symptoms (e.g. memory disorders, impairments in perception of thinking). Uniform reactions should not be expected, distinguishing from subgroups (e.g. children, young people, old people, migrants, religious communities, social or political interest groups/lobbyists, political representatives, media representatives, etc.).

Depending on the damage situation and which groups are directly affected, reactions will vary. People show social, cooperative, prudent and helpful behaviour rather than destructive behaviour in the event of serious accidents and extreme threats. Very rarely uncontrolled panic or even mass panic occurs. The extent of plundering in catastrophes is clearly smaller than assumed. The necessary delivery of personal belongings afflicts those affected additionally to the undressing in public. Both are associated with feelings of shame and embarrassment. Sensations such as loss of privacy and personal vulnerability as well as ethical and moral problems can lead to massive stress reactions in affected persons. Insecurity and fears as dominant feelings include the following:

- fear of infirmity and death;
- fear of damage through contact with other people;
- fear for the health and safety of relatives and friends;
- fear of harming other people (biological, radiological/nuclear);
- anxiety as to whether sufficient treatment/care options are available;
- fear of long-term consequences (e.g. health restrictions, irreversible physical damage, cancer, hereditary damage).

Vulnerable groups: Children, Culture-religious groups, young people, old people, migrants, religious communities, social or political interest groups/lobbyists, political representatives, media representatives. If it´s necessary e.g. to decontaminate Muslim citizens, this can become difficult due to cultural-religious commandments: They are prohibited from undressing in public.

There are several possible courses of action:

(1) They can refer to the central legal principle of Islam "necessity breaks commandment": In emergency situations. Muslims are allowed to take actions that are not otherwise permitted.

(2) Secure the support and the permission to undress by male escorts of the Muslim woman. Preferably turn to a respectable person of the family or the group (e.g. the family elder).

(3) If possible, ensure that a religious respected person (Imam) is called in in the cordoned-off area by the psychosocial acute helpers (emergency pastors, KIT) there. But: The time required to convince people who refuse to decontaminate must not be at the expense of those who are willing to decontaminate. Shield patients from spectators when disrobing and decontaminating. Leave groups together if possible - Groups of people who belong together (families, friends, colleagues, etc.) usually calm each other down in a threatening situation and look after each other. In the case of death, relatives in the decontamination should get the chance to see their relatives before decontamination. Relatives should be allowed to stay with dying relatives.

4.2. Nationales Krisenmanagement im Bevölkerungsschutz (National Crisis Management in Civil Protection)

Public/Responder: Blank.

Organisation: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance).

Year: 2008.

Type of incident: Hazardous materials.

Type of strategy: Crisis communication.

Summary of strategy:

Communication needs preparation. The better an organisation responds to the crisis, the more prepared it is and the faster it recovers. For crisis communication that means:

- Communication plans,
- Development of good organisational and technical working conditions,
- Careful selection of personnel. Appropriate training policy. Schedule of reinforcements.

Strategy for communication: Blank.

Summary of communication strategy:

1. Credibility: It is a basic condition of any crisis communication. It is difficult to regain trust once it has been lost. Defects and mistakes must not be concealed; appeasing, embellishing

or even covering up exacerbates every crisis and undermines confidence in crisis management.

2. Creating trust: The feeling of not knowing creates powerlessness and fear. Therefore, every communication strategy in a crisis must aim to create trust in crisis management.

3. Act, don't react: In a psychologically difficult crisis situation, active information work must be established from the start. The more up-to-date and reliable the "official" information is, the better the chance that it will be present in the media. If the organisation does not communicate or does not communicate openly, journalists tap into other, usually less reliable, sources. If information deficits have already arisen, the aim must be to regain "information sovereignty" and the trust of the general public through appropriate, open information.

4. Communication is leadership: Crisis communication must always be a matter for the boss. This sentence sounds unimportant, but it is even more important in a crisis than in routine operations. Decision-makers are the most important communicators as they have the "highest competence" regarding the perception of the public - both positive and negative.

5. Communication needs networks: In a crisis, strategic impact can only be optimally achieved through a networked, coordinated information policy that includes all levels (federal government, Länder, local level, organisations, associations, companies, etc.).

6. Information needs coordination: important information measures should be continuously coordinated horizontally and vertically in order to be able to speak with one voice.

7. Winning the media as partners: In a crisis, the media are the most important "intermediaries" with the public. They have a broad impact and are "close to the people". The aim must, therefore, be to involve their opinion leaders (editors-in-chief/chief editors, etc.) in "responsibility" by providing as much background information as possible and to inform journalists "on the spot" as much as possible about the current situation during the crisis. Internet portals for journalists with up-to-date information relieve the burden on the press offices and support uniform language regulations. The basic line of a credible information strategy: factual, honest information, combined with the emotional canvassing for trust in crisis management.

Likely public response: Unfortunately, there is a serious knowledge gap, which is also filled with speculations about reactions that so far have no empirical content. It is assumed that panic is spreading, that people react unreasonably and even criminally. In fact, however, all of this is not the case, with deviations of at most 3 percent, while more than 80 percent of all affected persons behave "normally", mostly even "pro-actively". However, hardly any exercise scenario paints population reactions in this positive light. On the contrary: the population is always synonymous with mass hysteria, rumours, aggression, looting and all other deviant behaviour that has to be dealt with on the basis of what the penal code establishes.

Vulnerable groups: Every single person, intercultural communication with non-native speakers.

4.3. Bevölkerungsverhalten und Möglichkeiten des Krisenmanagements und Katastrophenmanagements in multikulturellen Gesellschaften (Population behaviour and opportunities for crisis management and disaster management in multicultural societies)

Public/Responder: Blank

Organisation: Bundesamt für Bevölkerungsschutz und katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance).

Year: 2010.

Type of incident: Hazardous materials.

Type of strategy: Crisis communication.

Summary of strategy: Blank.

Strategy for communication: Blank

Summary of communication strategy:

With regard to the design of a warning, it must be ensured that as many as possible of those who are on the move for various reasons also receive the warning. It makes sense to use it as far-reaching and diversified communication channels and to pay attention to multilingualism. Since the interviewees complained that the warnings were incomprehensible to them, their wording must be designed in such a way that even people unfamiliar with the place can use them as a guide. Due to the lack of local knowledge, descriptions of locations and directions, e.g. to emergency accommodation that only locals can understand, are of little help to non-natives. In order to avoid or reduce possible scepticism, the warning should also mention that the emergency accommodation available is actually sheltered and is usually optimally equipped. There is another problem with illegal residents. In the event of a disaster, these people may also need care, medical or other care, or possibly decontamination. In such a situation, illegal residents face the serious problem that their status of illegality could become obvious if they seek care, advice, care or decontamination. Any official procedure chosen must be sufficiently credible and convincing for the people and groups concerned.

Targeted actions are only successful if people in their vicinity can encourage them to gain sufficient trust and follow public recommendations or instructions, or if they could gain trust on their own initiative. The following two approaches are seen as solutions to the problem

outlined. There are no checks on identification papers (identity cards, etc.). The recently passed law which establishes that illegal residents can use the services of hospitals without their data being passed on to the Aliens Department could be ground-breaking in this respect. It is recommended that in crisis situations, emergencies and disasters, which also affect members of minorities, communication should be as open as possible and in the different mother tongues. It is recommended that information on events (in understandable language) be provided as truthfully and completely as possible. It is in no way sensible to trivialise the release of radioactive or other harmful substances (possibly to avoid panic), as irretrievable damage to confidence is to be expected if what is concealed is circulated in the form of rumours or scandalised by the mass media.

When migrants or asylum seekers come from non-democracies where censorship is practised, the concealment of information that seems relevant to their own security may remind them of the regime of the country of origin and of what was suffered there. This can lead to serious and lasting losses of trust, possibly even to the intensification of traumas experienced in the country of origin. Here it can be seen that people whose trust is fragile anyway due to experiences of violence are on the one hand particularly dependent on an environment that creates trust, and on the other hand, can easily lose the trust newly gained in Germany. It is also recommended that risk-related information and warnings should be disseminated using media that are also widely used in everyday life. If the publication of the warning message were to be routed via traffic radio, for example and designed accordingly, it would be possible to reach large sections of the population. That is the case because of the following reasons: The reception of traffic radio is independent of the failure of regional power grids (the transmitters presumably have emergency power generators). Many drivers (cars/trucks) will have mobile phones to inform friends, relatives, and neighbours.

The announcements could be made in three languages: German, Turkish and English. If you want to reach Francophone people (France, Tunisia, Morocco, some of the Africans living in Germany), it would also be useful to warn them in French. A fifth language would be Russian or Polish. With the first four languages, most transit travellers could also be reached. It is therefore recommended that when passing on risk-related information, warnings and alerts, care be taken to ensure that men and women are reached in the target groups.

Likely public response:

1. Ethnic-cultural minorities in multicultural societies: It is to be feared that migrants from southern countries (Greece, Turkey, African states), at least in the first generation of migration, will react with anxiety when events occur that threaten them because they have no confidence that the local organisations involved in security are up to the task. Such mistrust usually results from previous experience with a lack of competence on the part of the relevant organisations in the country of origin. Another problem may be a lack of confidence in rescue workers and obstruction of access if rescue workers cooperate too

closely with police forces. This is particularly the case for minorities when they were confronted with violence by law enforcement forces in their country of origin.

2. Tourists: All respondents stated that their behaviour had resulted from ignorance of local conditions, with earthquake victims responding differently than those affected by hurricanes. Tourists in urban areas were more likely to use public shelters than those visiting rural areas. The former were less likely to return home immediately. Most respondents were relieved to leave their respective disaster areas but found that those working in the tourism industry should be better prepared for the disaster.

Vulnerable groups:

1. Ethnic-cultural minorities in multicultural societies: It is recommended that migrants enrich their knowledge of the functioning and trustworthiness of rescue and aid organisations in Germany. In addition to schools, churches or mosques, organisations, institutionalised meeting places of the respective minority, contacts could be in particular business people from whom migrants of both sexes shop, in particular food and general merchandise traders (this applies not only to migrants of Turkish origin but also to migrants from the former Soviet Union (FSU), the East Asian region and Africa). The owners of such shops should be seen as multipliers of information and may know more about the migrant population in their neighbourhood than minority organisations (it is part of their business to know their customers and have their trust). It might also be possible to plan joint information events with them. It is recommended to negotiate on an equal footing, as this creates trust. Therefore, too close a link between law enforcement and firefighters (including other organisations involved in S&R) should be avoided where possible. In order to maintain confidence in forces involved in rescue and disaster relief, neutrality is essential. For example, by negotiating on an equal footing and maintaining neutrality, the fire service can gain access in situations and to groups of people who have a problematic or anxious relationship with police forces. Unimpeded access is an indispensable prerequisite for firefighters to avert danger in situations where danger is imminent (especially fires). It is recommended that care be taken not to discriminate against members of ethnic and cultural minorities. In addition, they should be adequately involved in regional or local planning groups and should be given as many opportunities as possible for participation and promotion in disaster management and aid organisations. Enarson and Fordham (2000) point out that migrant women, in particular, are well informed about their own needs and those of their socio-cultural group during and after a disaster.

2. Tourists: Tourism entrepreneurs should invest more in disaster preparedness and emergency preparedness. If the tourism industry were better prepared, it might be worthwhile to refer travellers to staff in the tourism sector and strengthen confidence in them, as they are often multilingual and have better local knowledge. If staff in the sector are trained, they can provide additional support by being informed about organisational processes.

4.4. Risiko- und Krisenkommunikation am Beispiel von terroristisch motivierten Schadenslagen und Schadstoffunglücken: Einflussfaktoren auf die Reaktion nach Warnmeldungen (Risk and crisis communication using the example of terrorist motivated damage situations and pollutant deficiencies: Factors influencing the Reaction after warning messages)

Public/Responder: Responder.

Organisation: Dr. Vanessa Schneider.

Year: 2015

Type of incident: Hazardous materials.

Type of strategy: Self-decontamination, Preliminary hazard assessments (exercise), Additional safety instruction with instructions on how to behave (exercise)

Summary of strategy: Blank

Strategy for communication: Pre-incident.

Summary of communication strategy

Give clear instructions and define protective measures: For the warned persons, the warning message must generate a minimum level of hazard awareness so that preventive measures of protection can be implemented. Inform those affected. For those affected it is important to receive information on the potential health effects in order to understand, recognise and avoid them. This includes information on the radius and extent of the radioactive material to understand whether they are in the danger zone and information on what signs and symptoms would occur in the event of contamination and when medical attention would be needed. Furthermore, affected people like to get concrete information on who committed the attack, why it was committed, whether there is still danger or not, what destruction the attack has caused and how long rescue operations will take.

Likely public response

Following a CBRN event, an increase in the number of contacts between the population and the health system can be expected. This can lead to a full utilisation of the health care system. Most people concerned to be contaminated are not directly affected in a CBRN incident. Many people do not respond appropriately to warning messages or do not immediately take the recommended protective measures following the warning message.

Vulnerable groups: Everybody.

4.5. Experimentelle Untersuchung und Optimierung der Dekontamination von Verletzten bei einer C(B)RN-Gefahrenlage durch Organisationen der nichtpolizeilichen Gefahrenabwehr (Experimental investigation and optimisation of decontamination of casualties in C (B) RN threats by non-policing organisations)

Public/Responder: Responder.

Author: Patrick Sudhoff.

Year: 2016.

Type of incident: CBRN

Type of strategy: Self-decontamination, Preliminary hazard assessments (exercise), Additional safety instruction with instructions on how to behave (exercise)

Summary of strategy: For a mass decontamination of ambulatory people usually, cold water of hydrants is used for this purpose.

To identify possible sources of accidents in good time and to reduce the risk for all parties involved (e.g. hypothermia)

Registration and signing of the consent form

Assignment of an identification number (ID)

Measurement of body temperature and documentation of the time of day

Spraying the test persons with fluorescent LUMILUX® mixture

Photography on both sides under UV light

Strategy for communication: Pre-incident.

Summary of communication strategy: Providing self-protection training like self-decontamination as part of first aid courses to provide the emergency services with a tactical time gain and to increase the surviving rate.

Likely public response: Affected people will arrive at treatment points with little or no warning time. Up to 80 % of those affected react self-centred and unpredictable. Those affected will go to the nearest treatment centres (e.g. hospitals) independently and without decontamination. - 83.8 % stated that they could well understand the first responders under their protective clothing - the majority felt communication was problem-free and that

questions were answered satisfactorily - 40.5 % stated that they were not or not sufficiently informed about the next step to be taken.

Vulnerable groups: Those affected by a CBRN incident.

4.6. Verhalten bei besonderen Gefahrenlagen (Behaviour in special danger situations)

Public/Responder: Public.

Organisation: Bundesamt für Bevölkerungsschutz und katastrophenhilfe (Federal Office for Civil Protection and Disaster Assistance).

Year: 2018.

Type of incident: Hazardous materials.

Type of strategy: Strengthening the behaviour of affected civilians in CBRN incidents.

Summary of strategy: Those affected should be encouraged to psychologically support each other in the danger area.

Strategy for communication: Yes

Summary of communication strategy:

Civilians:

- Make contact and, if necessary, go to the same height as those affected
- Talk to those affected! So they perceive that they are not alone in this situation.
- Listen patiently and speak as calmly as possible.
- Slightly touches on arm, shoulder or hand (even without words) are perceived as pleasant and calming by those affected. Do not make any stroking movements and avoid touching the head, legs, stomach, upper body, and hips.

Children:

- Create an environment of security by staying with the child or search for a possible caregiver.
- Make sure you have a friendly voice and facial expression.
- Try to find parents or other caregivers as soon as possible.

- Ask about acute needs (e.g. a warm blanket, something to drink or a telephone call).
- Try to protect those affected by prying eyes.

Immigrants:

- Speak in a calm and friendly voice.
- Pay attention to friendly gestures and facial expressions.
- Use body language to make yourself understood.
- Involve family members or if possible interpreters to maintain communication.

Likely public response: Not discussed

Vulnerable groups: Those directly affected by a CBRN incident, children, immigrants.

4.7. FwDV_500 - Units in ABC-scenarios

Public/Responder: Responders.

Organisation: Ausschuss Feuerwehrangelegenheiten, Katastrophenschutz und zivile Verteidigung (AFKzV) (Committee on Fire Fighting, Civil Protection and Civil Defense (AFKzV)).

Year: 2012.

Type of incident: Hazardous materials.

Type of strategy: Disrobe, Decontamination, Isolation

Summary of strategy: Contaminated persons are, as far as possible and medically necessary, decontaminated or disinfected on site. Non-injured affected people suspected of incorporation or severe radiation exposure are mediated to an authorised doctor or a regional radiation protection centre.

Everyone in the danger area has to be namely recorded.

Everyone in the danger area is considered contaminated until it proves otherwise.

Dealing with contaminated suspects: Civilians suspected of contamination must take off the clothes at the decontamination place.

Hands, face, hair and wetted body parts are disinfected and cleaned.

The decontamination success must be proven by measurement.

Civilians (suspected) with pathogens of risk group 4 are isolated on site.

Strategy for communication: Yes

Summary of communication strategy: Provide information to affected people about behaviour instructions.

Likely public response: Not discussed.

Vulnerable groups: Those directly affected by a CBRN incident.

4.8. Biological hazards I: Handbook for the civil protection. 3rd edition

Public/Responder: Responder.

Organisation: Federal Office of Civil Protection and Disaster Assistance (BBK) and Robert Koch Institute.

Year: 2007.

Type of incident: Biological.

Type of strategy: Isolation of civilians suspected of decontamination, Information on further treatment, Evacuation, Disrobe, Decontamination, Rerobe

Summary of strategy: Everyone nearby or in contact with a suspicious item is separated from non-contaminated people and held by the police until the public health officer comes. This does not include life-threatening situations requiring immediate medical treatment. Emergency teams should:

- Keep at least a safe distance of 50 meters
- Give and pass on continuous information about the situation
- Consider CBR contamination
- Do not enter the danger area without orders
- Consider PPE, take cover
- Prepare routes of withdrawal for self-protection
- Ensure technical communication in the danger area
- Evacuate the danger area

- Order the location (contamination area, patient area, decontamination)
- Report suspicious items
- Only act after the approval of the police

Warn new arriving emergency teams, affected people should disrobe. They should wash their bodies in soap and water. In cases of higher contamination level, affected people should take a shower, if possible using operational showers on-site. Do not move dead body remains, explosive devices or items

Strategy for communication: Yes

Summary of communication strategy:

At the beginning of an incident, all affected people should be warned. In Berlin, all affected people immediately get an information paper that explains the further procedure and contains contact details, phone numbers and general information about the hazardous substance, it's effects and treatment possibilities The transport process should be explained to the patient, the designation and the specific protective measures facilitates the situation. The agreement on a basic communication using simple sign language allows the patient and the crew to stay "in touch" despite insulating conditions. The patient must be comprehensively and intelligibly informed and has to agree formally to all therapy decisions. As long as the patient is in full possession of his mental judgment, the patient can generally decline every treatment decision even if this endangers his/her health or life. This includes preventive vaccinations. An exception to this is the infection protection law (IfSG). It states that the government and the federal states can direct the vaccination (and other preventive measures) of highly endangered population groups [for example children]. These groups can only refuse by showing a medical dispensation. Especially important in dealing with emergency survivors is the high information need of the affected people. They are concerned and they sense a strong need for regaining control over the situation. A short message about the nature of the injury and the type and duration of the measures taken may support a higher pain tolerance of an injured person. In the emergency situation, the farewell should be offered and accompanied by a qualified contact person. The injured body can be covered and an uninjured body part is seen and touched. Sometimes the survivors can also say goodbye to clothes or over jewellery worn by the deceased. Cultural specific forms of farewell should also be considered and respected as far as possible.

Likely public response:

A survivor, who is left alone without hope of recognizable help, may experience a strong powerlessness. That is why the social support of survivors immediately after an event is of great importance. It has also proven to be helpful if survivors get simple tasks to draw attention to something else and to strengthen the lost self-competence. Survivors have a strong need for regaining control over the situation. The PPE worn by emergency

responders can cause hysteria and panic to members of the public so use should be carefully considered.

Vulnerable groups: Those directly affected by a CBRN incident. Cultural specific forms of farewell should also be considered and respected as far as possible. As part of the decontamination process, the creation of the greatest possible privacy of the affected people is important, taking into account ethical and moral principles. Furthermore, a sex separation (and if only by a privacy shield) should always be possible.

4.9. SKK DV 500

Public/Responder: Responder.

Organisation: Permanent conference on disaster preparedness and population protection.

Year: 2008.

Type of incident: Hazardous materials.

Type of strategy: Risk communication in CBRN incidents, Disrobe, Decontamination

Summary of strategy: Possible actions in the decontamination area:

- Establishing and maintaining an area for medical and psychological treatment next to the entrance of the decontamination area.
- Performing emergency decontamination of face, injuries, breathing area and basic life support including antidotes.
- Support the undressing of affected people and safe the clothes to prevent the spread of contamination. - Define the decontamination chronology of the patients – if possible by a doctor.
- Offer medical and psychosocial support during the decontamination process.
- Only emergency staff members wearing PPE conduct admission, medical treatment, and transportation.

Strategy for communication: Yes

Summary of communication strategy: The procedure should be explained to the patient.

Likely public response: Not discussed.

Vulnerable groups: Those directly affected by a CBRN incident.

4.10. Civil defence concept

Public/Responder: Responder.

Organisation: Bundesministerium des Innern (Federal Ministry of the Interior).

Year: 2016.

Type of incident: Hazardous materials.

Type of strategy: Decontamination, Vaccines/antibiotics, Potassium iodine tablets

Summary of strategy: The contaminant should be rapidly detected Decontamination abilities should be readily available and emergency decontamination should take place of persons, surface areas, infrastructure, and equipment. The capability of decontamination is provided by the states' water supply units, such as fire service water tenders. For biological agents, no decontamination is necessary, but self-protection and hygiene measures must be planned to prevent the spread of contamination. For biological hazards, the state maintains reserves of smallpox vaccines and antibiotics. The state also maintains reserves of potassium iodide tablets to distribute in case of accidents releasing radioactive iodine.

Strategy for communication: Yes

Summary of communication strategy: The population should be prepared in how to respond to situations through having basic knowledge in safe shelter in threat situations, what to do in case of a CBRN incident, self-sufficiency, first aid, fire-fighting Timely warnings should be issued to ensure people are able to take appropriate measures to protect themselves - the state should provide reliable, timely and nationwide public alerts recommending appropriate action - these alerts are given on multiple devices such as radio, television, internet and telecommunications providers.

Likely public response: Not discussed.

Vulnerable groups: Not discussed.

4.11. Guide for emergency preparedness and correct action in emergency situations

Public/Responder: Public.

Organisation: Federal office of civil protection and disaster assistance.

Year: 2018.

Type of incident: CBRN.

Type of strategy: Blank

Summary of strategy:

Aimed at the public: Stay in the building, temporarily take in endangered passers-by, inform other occupants of the building, close windows and doors, turn off fans and air conditioning systems, close the ventilation slots in window frames, seek out a protected internal room in your apartment ideally one which has no windows outside. If indoors: in the event of a radioactive substance being released, seek out a cellar, avoid unnecessary consumption of oxygen by candles or similar, turn on the radio or try to get info, only make telephone calls in emergencies, use available respiratory protective devices, if necessary an improvised face mask If outdoors: pay attention to the announcements by the police and fire brigade, move across the direction of the wind, if possible breathe through a respiratory protection device, seek out nearest closed building, if you have come into contact with a hazardous substance, change your outer clothing and shoes, pack contaminated outer clothing and shoes in plastic bags and place them outside of living area, first wash hands thoroughly and then face and hair as well as nose and ears with soap and water. If a biological substance has been released, the disinfection of hands is important and follows the shelter in buildings advice as above. If in-car, switch of ventilation and close windows, listen to the radio and follow instructions of the authorities and emergency personnel, seek out nearest closed building, request admission and observe the instructions for sheltering in buildings there.

Strategy for communication: Yes

Summary of communication strategy: In the event of an incident, people should pay attention to announcements on the radio, television or from loudspeaker vehicles, seek information from the internet and inform other occupants of the building.

Likely public response: Not discussed

Vulnerable groups: Not discussed

4.12. Health protection against CBRN hazard; epidemics control management

Public/Responder: Responder.

Organisation: Federal Office of Civil Protection and Disaster Assistance.

Year: Blank

Type of incident: CBRN.

Type of strategy: Evacuation, Decontamination, Epidemic emergency management, Targeted therapy, Vaccinations, Disrobe

Summary of strategy:

Radiological incidents: remove persons from the hazard zone ASAP; the persons must be decontaminated.

Biological hazards: specific measures such as epidemic emergency management (e.g. sequestration) and targeted therapy (e.g. administration of antibiotics) ranging from preventive measures (e.g. vaccination) to be implemented.

Chemical hazards: evacuate from danger zone immediately; inhalation of the chemical must be avoided; contaminated clothing must be removed; decontamination (e.g. extensive showering) should take place; if a large number of people are also injured then the fire services must provide help.

Strategy for communication: Not discussed

Summary of communication strategy: Not discussed.

Likely public response: Not discussed.

Vulnerable groups: Not discussed.

4.13. Guidance for the creation of hospital alarm and operational plans

Public/Responder: Responder.

Organisation: No author.

Year: 2006.

Type of incident: CBRN.

Type of strategy: Evacuation, Isolation

Summary of strategy:

For gas or vapour incidents: leave the danger area and create a large-scale shutdown, do not use any electrical systems, provide venting and fresh air for emissions in the building, keep doors and windows as tight as possible in case of external emissions and switch off supply air systems for radioactive incidents: stay in the unaffected building or visit unaffected buildings, avoid contact with radioactive substances, seal doors and windows of unaffected buildings, switch off supply air systems of not affected buildings

Pandemic: suspected contaminated patients must be separated and will get specialist medical treatment

Strategy for communication: Not discussed

Summary of communication strategy: Not discussed.

Likely public response: Not discussed.

Vulnerable groups: Not discussed.

4.14. Acting in a CBRN event. Citizen information flyer

Public/Responder: Public.

Organisation: Federal office of civil protection and disaster assistance.

Year: 2018.

Type of incident: CBRN.

Type of strategy: Inform yourself, Disrobe, Decontaminate, Enter a safe building and do not leave

Summary of strategy: Keep calm, self-protection is the highest priority, inform the emergency services, give aid, follow instructions of emergency response teams, only make a private call if it is necessary, report any observation to the police.

To prepare yourself: get informed about evacuation routes, refresh your knowledge about first aid, always a fully charged phone, use federal warning apps, if you are not next to the danger area then inform yourself using the television, radio or internet

in a CBRN incident: listen to information provided by emergency services, move crossways the wind, breathe only inside a tissue or a shirt, if you are in a car, disconnect the air conditioning and close the window, seek a closed building, if you have been in contact with a hazardous substances, undress before entering the building and leave everything outside, wash yourself - first your hands then your face, hair nose and ears, inform yourself via radio, television, and radio, stay in the building so long as there are no other threats.

Strategy for communication: Yes

Summary of communication strategy: If you have been a victim, witness or observer and feel like you can help by offering psychological first aid: Search for eye contact and if possible to speak on eye-level. Speak with affected people. Listen carefully and speak in a calm voice. Soft touches on arms, shoulder, and hand can be comforting but avoid stroking movements. Ask for acute needs. Try to cover affected people against curious views.

Likely public response: Not discussed.

Vulnerable groups: If children are affected: Ensure a sense of safety with the child Use a friendly voice and face Try to find parents If immigrants are affected: Speak in a calm and

friendly voice Take attention to a friendly gesture and facial expression Use body language to communicate Use significant others or if possible interpreters to secure communication.

4.15. THW DV 500 - Deployment in CBRN scenarios

Public/Responder: Responder.

Organisation: THW.

Year: 2014.

Type of incident: CBRN

Type of strategy: Disrobe, Decontamination

Summary of strategy: Biological scenario: non-injured persons are to be brought to an authorised doctor; affected people should remove their clothes; hands, face, hair and wet body parts disinfected and cleaned.

Strategy for communication: Not discussed.

Summary of communication strategy: Not discussed.

Likely public response: Not discussed.

Vulnerable groups: Not discussed.

5. CONCLUSION

This document lays down the legal, policy and ethical frameworks that are relevant in PROACTIVE. Some of the questions have been only partially addressed, such as:

- Extra preventative measures put in place to prevent unauthorised access to sensitive data;
- Application for civil society;
- Assent from minors.

These topics will be addressed once partners make headway on how to go about these issues. The updates will be included in D7.4 (on M18), D8.2 (Legal and acceptability recommendations for PROACTIVE toolkits), and D8.3 (Materials and briefing for PROACTIVE exercises). Such deliverables will take into account what has been established in this deliverable. At the same time, D8.4 (Ethical and Societal Impact Assessment of project outputs) will evaluate the impact of the project and provide guidelines for the

PROACTIVE system management in such a way that the potential issues identified in this deliverable are taken into consideration.

To recap, in this document a variety of issues have been addressed. First, the legal framework that is relevant for PROACTIVE is fleshed out, specifically concerning human rights and data protection. Second, the legal and policy framework on CBRNe at the European level is established. Last, a set of ethical frameworks is put forward in order for its content to inform D8.2 and D8.3.

The legal framework tackled the human rights that are the most relevant for the PROACTIVE project, namely the right to integrity, the right to privacy, and the right to data protection. All these rights are examined in the light of the most relevant international treaties, such as the Universal Declaration of Human Rights, the European Union Charter of Human Rights, and the European Convention on Human Rights. As well, the data protection rights of research participants and members of the advisory boards. Last, a series of legal and soft law documents help understand the role that CBRNe plays within the European Union, as well as the place that PROACTIVE occupies within the CBRNe European framework.

The legal framework on privacy and data protection (mainly the GDPR) is the one that establishes the bulk of the legal requirements. It is necessary for partners to read the section on data protection in this deliverable along with the relevant ethical and legal requirements in WP10 in order to get a good grasp of their obligations. That is particularly true for partners that have a vital role in data processing. Nevertheless, the table below presents the main obligations concerning privacy and data protection and summarises the most important measures adopted by the consortium in order to carry them out.

Table 7 Main legal requirements concerning privacy and data protection

Issue	Relevant article (GDPR)	Applicability in PROACTIVE and recommendations (deliverables, risk assessment, etc.)
Anonymisation	Recital 26	Data subjects cannot be recognised in order for a data set to be considered as anonymised. Anonymisation must be carried out as it is established in D10.5.
Special categories of data	Article 9	Special categories of data must be stored following procedures that set in place additional safeguards, which will be included in D10.2 and in forthcoming versions of D7.4.

Roles	Chapter IV (especially Article 28)	Processors must be adequately identified. Also, the relationship between them and the controllers has to be regulated through a contract that includes privacy and data protection clauses. Overall, controllers must ensure that processors are compliant with the GDPR.
Record keeping	Article 30	Partners processing sensitive categories of personal data need to keep records of their processing activities.
Informed consent	Article 7	The processing of personal data within PROACTIVE will be carried out almost exclusively on the basis of informed consent, which makes it very important for partners to ensure that consent is gathered as established in D10.6.
Principles	Article 5	Data protection principles must inform the research activities and the development of the different toolkits in PROACTIVE. In particular, D10.4 establishes how the various partners comply with the principle of data minimisation.
Security	Article	Personal data must be processed in a secure way according to the risks created by them and the state of the art. D10.2 establishes the security measures that have been put in place by the partners.
Data breach	Article 33, Article 34	Partners must follow the procedures established in this deliverable and the joint controller's agreement.
Rights of data subjects	Article 15, Article 16, Article 17, Article 18, Article 20,	The rights of the data subjects must be ensured by communicating their existence to the research participants before they consent. Also each organisation's DPO needs to have the necessary

	Article 21, Article 22	resources for ensuring that the research participants rights are respected at all times.
App	Article 25	Ongoing communications must be established between RINISOFT and ETICAS in order for the applications developed within PROACTIVE to comply with the principle of Data Protection by Design and by Default.

The main objective of the ethics section is to support the consortium partners in identify the ethics requirements in regards to CBRNe response at the EU level, focusing on emergency assistance for vulnerable groups. It draws from a comprehensive literature review of disaster ethics (including CBRNe incidents) and aims to provide input to the scenario development and evaluation methodology (WP6) and to inform the consortium partners of the ethical governance framework that will guide the research activities and evaluations of procedures and tools (WP8 and WP10).

On a different note, the selection of German frameworks that have been put forward in section 4 are aimed at providing an overview of previous CBRNe guidelines that should be used in order to anticipate possible issues that may arise during the exercises. Therefore, D8.3 (Materials and briefing for PROACTIVE exercises) can greatly benefit from taking into consideration the lessons learned in the guidelines.

In conclusion, this deliverable is meant to provide a solid basis for D8.2 and D8.3, which will need to account for legal and ethical issues.

6. REFERENCES

Adger, W.N. (2006). Vulnerability. Global Environmental Change 16:268-281.

Agencia Española de Protección de Datos. (n.d.). Guide on personal data breach management and notification.

Almond, B., 'Applied Ethics', in Craig, E., (ed.) (2005), *The Shorter Routledge Encyclopedia of Philosophy*, New York: Routledge.

Altevoght, B.M., Stroud, C., Hanson, S.L., Hanfling, D., & Gostin, L.O. (2009). Guidance for Establising Crisis Standards of Care for Use in Disaster Situation: A Letter Report. Washington, DC: National Academies Press.

Beauchamp, T.L., 'The Nature of Applied Ethics,' (2003) in R.G. Frey, ed., *A Companion to Applied Ethics*, Oxford: Blackwell; 12-13.

Brookings-Bern Project on Internal Displacement (2008). Human rights and natural disasters. Operational guidelines and field manual on human rights protection in situations of natural disaster, available at http://www.refworld.org/pdfid/49a2b8f72.pdf.

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

Caesar, P. L. (n.d.). GDPR & Brexit: Is there a need for an adequacy decision? Retrieved from https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-and-brexit-is-there-a-need-for-an-adequacy-decision.html

California Governor's Office of Emergency Services (Cal OES) (2000) Hazard Mitigation Planning.

Carter, H., & Amlôt, R. (2016). Mass Casualty Decontamination Guidance and Psychosocial Aspects of CBRN Incident Management: A Review and Synthesis. PLOS Currents Disasters. Edition 1. doi: 10.1371/currents.dis.c2d3d652d9d07a2a620ed5429e017ef5.

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

Christian, M.D., Sprung, C.L., King, M.A., et al. (2014). Triage: care of the critically ill and injured during pandemics and disasters: CHEST consensus statement. Chest; 146(4, suppl):e61S–e74S.

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

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

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

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

Communication from the Commission to the European Parliament and the Council the EU Internal Security Strategy in Action: Five steps towards a more secure Europe. (2010).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Action Plan to enhance preparedness against Chemical, Biological, Radiological and Nuclear Security risk. (2017).

Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on a new EU approach to the detection and mitigation of CBRN-E risks. (2014).

Conclusions on preparedness and response in the event of a CBRN attack. (2010).

Consolidated version of the Treaty on the Functioning of the European Union. (2009).

Council conclusions on the new CBRNE Agenda. (2012).

Council Decision 98/22/EC of 19 December 1997 establishing a Community action programme in the field of civil protection. (1997).

Council Decision of October 23, 2001, establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions. (2001).

Council of Europe, European and Mediterranean Major Hazards Agreement (EUR-OPA), Resolution 2011 – 1 of the Committee of Permanent Correspondents on Ethical Principles relating to Disaster Risk Reduction and contributing to People's Resilience to Disasters, adopted at the 60th Meeting of the Committee of Permanent Correspondents, Strasbourg, France, 15 April 2011, 27-31.

Daniel, M. (2012). Bedside resources stewardhip in disasters: a provider's dilemma practicing in a ethical gap, in J clinical Ethics:23(4):331-335.

DECISION (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements. (2018).

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism. (2013).

Dennis, M.R., Kunkel, A.D., Woods, G., & Schrodt, P. (2006). Making sense of New Orleans flood trauma recovery: ethics, research design, and policy considerations for future disasters. Anal Soc Iss Public Policy;6 (1):191–213.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. (2016).

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

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

Eldridge, L. (2019). What does in vivo and in vitro mean, available at https://www.verywellhealth.com/what-does-in-vivo-and-in-vitro-mean-2249118

Enarson, E. & Fordham, M. (2000). Lines that divide, ties that bind: Race, class, and gender in women's flood recovery in the US and UK. Australian Journal of Emergency Management 15 (4): 43-53.

Etkin, D., & Timmerman, P. (2013) Emergency management and ethics, *International Journal of Emergency Management, 9(4)*, 277-297.

EU preparedness against CBRNE weapons. (2019).

European CBRNE action plan. (2009).

European Convention on Human Rights. (1950).

European Security Strategy. (2003).

European Union Agency for Fundamental Rights. (n.d.). Consent to use data on children. Retrieved from https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/use-consent

European Union Internal Security Strategy. (2015).

Fahey, C.J. (2007). Ethics and disasters: mapping the moral territory. Generation: 61–65.

Gaitonde, R., & Gopichandran, V. (2016). The Chennai floods of 2015 and the health system response. Ind J Med Ethics 1(2):71–75

Gallopin, G.C. (2006) Linkages between vulnerability, resilience and adaptive capacity in Global Environmental Change 16:293-303.

Gert, B. (2002). The Definition of Morality, *The Stanford Encyclopedia of Philosophy*.

Glantz, M., & Jamieson, D. (2000). Societal response to Hurricane Mitch and intra/versus intergenerational equity issues: whose norms should apply? Risk Anal;20(6):869–882.

Hanfling, D., Altevogt, B., Viswanathan, K., & Gostin, L. (2012) Committee on Guidance for Establishing Crisis Standards of Care for Use in Disaster Situations; Institute of Medicine. Crisis Standards of Care: A Systems Framework for Catastrophic Disaster Response. Washington, DC: National Academies Press.

Hodge, J.G., Hanfling, D., & Powell, T.P. (2013). Practical, ethical and legal challenges underlying crisis standards of care, in J Law Med Ethics;41/suppl1:50-55.

Hugo, G. (1996). Environmental concerns and international migration in Int Migr Rsv, 30(1):105-131.

Hurst, J.L. (2010). Establishing human rights protection in post-disaster context In Journal of Emergency Management 8(6):7-14.

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

Jennings, B., & Arras, J., (2008). Ethical Guidance for Public Health Emergency Preparedness and Response: Highlighting Ethics and Values in a Vital Public Health Service, available at https://www.semanticscholar.org/paper/Ethical-guidance-for-public-health-emergency-and-%3A-Jennings-Arras/01430218c871b8df2d0d41be63617dab415301ed

Jenson, E., (1997). Disaster Management Ethics, UNDP Disaster Management Training programme, available at http://www.disaster-info.net/lideres/spanish/mexico/biblio/eng/doc13980.pdf

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

Jurkiewicz, C.L. (2009). Political leadership, cultural ethics and recovery: Louisiana post-Katrina. Public Organ Rev; 9:353–366.

Kailes, J.I. & Enders, A. (2007). Moving beyond "special needs": A function-based framework for emergency management and planning, in Journal of Disability Policy Studies, 17(4): 230-237.

Karadag, C.O., & Hakan, A.K. (2012). Ethical dilemmas in disaster medicine. Iran Red Crescent Med J;14(10):602–612.

Lane, S.N. (2012). Ethical risk management, but without risk communication? In: Kearnes M, Klauser F, Lane S. Critical Risk Research: Practices, Politics and Ethics. Oxford, UK: Wiley; 151–172.

Leider et al. (2017). Ethical Guidance for Disaster Response, Specifically around Crisis Standards of Care: a systematic review, American Journal of Public Health (AJPH) 107(9):e1-e9.

MacIntyre, A. (1984). A*fter Virtue: a Study in Moral Theory,* Notre Dame, Indiana: University of Notre Dame Press.

Macpherson, C.C., & Akpinar-Elci, M. (2015). Caribbean heat threatens health, well-being and the future of humanity. Public Health Ethics;8 (2):196–208.

Malik, A.M. (2011) Denial of flood aid to members of the Ahmadiyya Muslim community in Pakistan. Health Hum Rights;13(1):62–69.

Mariaselvam, S., & Gopichandran, V. (2016) The Chennai floods of 2015: urgent need for ethical disaster management guidelines. Ind J Med Ethics;1 (2):91–95.

Member States' Preparedness for CBRNE threats . (2018).

Mezinska, S., Kakuk, P., Mijaljica, G., et al. (2016) Research in disaster settings: a systematic qualitative review of ethical guidelines. BMC Med Ethics;17(1):1–11.

Mitrovic, V.L., O'Mathuna, D.P., & Nola, I.A. (2019). Ethics and floods: a systematic review In Disaster Med Public Health Prep; 13(4) 817-828.

Moatty, A., Vinet, F. (2016) Post-disaster recovery: the challenge of anticipation. E3S Web Conf, 7:17003.

Moatty, A. (2017) Post-flood recovery: an opportunity for disaster risk reduction? In: Vinet F, ed. Floods. Volume 2 – Risk Management. London: ISTE Press and Elsevier:349–363.

Morss, R.E., & Wahl, E. (2007) An ethical analysis of hydrometeorological prediction and decision making: the case of the 1997 Red River flood. Environ Haz;7:342–352.

Narayanan, A. a. (2008). Robust de-anonymization of large datasets (how to break anonymity of the Netflix prize dataset).

O'Mathuna, D.P., & Beriain, I.M. (ed) (2019). Ethics and Law for Chemical, Biological, Radiological, Nuclear and Explosive Crises, Springer.

O'Mathúna, D.P., Gordijn, B., & Clarke, M., eds. (2014). Disaster Bioeth, Dordrecht: Springer.

Parkash, S. (2012) Ethics in disaster management. Ann Geophys, 55 (3):383–387.

Phillips, S., Knebel, A., & Johnson, K. (2009). Mass medical care ith scarce resources: the essentials. Agency for Healthcare Research and Quality. 2009. AHRQ Publication 09–0016.

Pou, A.M. (2013). Ethical and legal challenges in disaster medicine: are you ready in South Med J:106(1):27-30.

PROACTIVE Consortium. (2019). Grant Agreement.

Progress Report on the Implementation of the EU CBRN Action Plan . (2012).

Rebera, A., & Rafalowski, C. (2014) On the spot ethical decision-making in CBRN response In Science and Engineering Ethics 20(3):735-752.

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

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

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

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

Resolution of the Council and the representatives of the Governments of the Member States, meeting within the Council of 13 February 1989 on the new developments in Community cooperation on civil protection. (1989).

Resolution of the Council and the representatives of the Governments of the Member States, meeting within the Council of 23 November 1990 on Community cooperation on civil protection. (1990).

Resolution of the Council and the representatives of the Governments of the Member States, meeting within the Council of 25 June 1987 on the introduction of Community Cooperation on Civil Protection. (1987).

Rice et al. (2017). Human Rights-Based approach to disaster Management, Journal of Human Rights and Social Work, Springer- 2: 117:127.

Rizza, C., & Pereira, A.G. (2011). Building a resilient community through social network: ethical considerations. In: Hiltz SR, Pfaff MS, Plotnick L, Shih PC, eds. Proceedings of the 11th International ISCRAM. 2014:289–293.

Rosoff, P.M. (2015) In defence of (some) altered standards of care for Ebola infections in developed countries In HEC Forum:27(1):1-9.

Rossano, F. (2015). From absolute protection to controlled disaster, J. Landsc Archit;10(1):16–25.

Sargiacomo, M., Ianni, L., & Everett, J. (2014). Accounting for suffering: Calculative practices in the field of disaster relief in critical Perspective on Accounting:25(7):652:669.

Schwartz, L., Hunt, M., Redwood-Campbell, L., & de Laat, S. (2014). Ethics and emergency disaster response. Normative approaches and training needs for humanitarian healthcare providers. In Disaster bioethics: Normative issues when nothing is normal, ed. Dónal P. O'Mathúna et al., 33–48. Dordrecht: Springer.

Sevimili, S., Karadas, S., & Dulger, A.C. (2016). Issues affecting health professions during and after catastrophic earthquakes in Van-Turkey in J Pak Med Assoc:66(2):129-134.

Simonovic, S.P. (2011). Two new floods, climate change, and ethics. J Flood Risk Manag;4:141–142.

Simpson, A.V., Cunha, M.P., & Clegg, S. (2015). Hybridity, sociomateriality and compassion: what happens when a river floods and a city's organizations respond? Scand J Manag;31:375–386.

Sokol, D.K. (2006). Virulent epidemics and scope of healthcare workers' duty of care In Emerging Infectious Diseases12(8):1238-1241.

Srinivasan, S. (2005). After the floods: health services' responsibilities in a crisis. J Med Ethics; 2(4):108–109.

Stănciugelu, I., & Krieger, K. (2014). *PRACTICE Ethics Checklist for Tool Providers*, Project PRACTICE, contract no 261728.

Stănciugelu, I., & Krieger, K. (2014). *PRACTICE Ethics Impact Evaluation Template*, Project PRACTICE, contract no 261728.

Stockholm Programme. (2010).

ten Have, H. (2018). Disasters, Vulnerability and Human Rights In Mathuna DP, Dranseika V, Gordijn B (ed) (2018) Disasters: Core Concepts and Ethical Theories, Springer.

The European Counter Terrorism Strategy . (2005).

The renewed European Union Internal Security Strategy . (2015).

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

UNESCO Declaration on Bioethics and Human Rights, 2005, available at https://en.unesco.org/themes/ethics-science-and-technology/bioethics-and-human-rights

Universal Declaration of Human Rights. (1948).

University of Toronto, Joint Centre for Bioethics Pandemic Influenza Group (2005) Pandemic Influenza Planning: Ethical Framework, available at http://jcb.utoronto.ca/publications/documents/pandemic_influenza.pdf

Usher D., (2016) D83.3 Impact on Vulnerable Groups, Project EDEN contract no 313077

Van de Poel, I., & Royakkers, L. (2011). *Ethics, Technology, and Engineering*, Wiley-Blackwell: 71-72.

Wagner, J.M., & Dahnke, M.D. (2015). Nursing ethics and disaster triage: applying utilitarian ethical theory in J Emerg Nurs:41(4):300-306.

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

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

World Health Organisation (WHO) (2015). Global Health Ethics – Key issues, Luxembourg.

Zack, N. (2009). Ethics for Disaster, Cambridge Scholar Publishing, Newcastle upon Tyne, UK.