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

Deliverable D8.2

Legal and acceptability recommendations for PROACTIVE toolkit

Due date of deliverable: 30/04/2020

Actual submission date: 15/03/2021

Mariano Martín Zamorano[1], Sara Suárez Gonzalo[1],

Gemma Galdon Clavell[1]

1: ETICAS

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**ulneranbl**E** 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 acceptability recommendations for PROACTIVE toolkit
Work Package	WP8
Date of the document	15/03/2021
Version of the document	05
Responsible Partner	ETICAS
Reviewing Partner	CBRNE, RINISOFT, UIC
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	09/04/2020	First Draft
02	20/04/2020	Improvements and suggestions of the board and partners implemented
03	28/04/2020	Revised version with inputs from RINISOFT
04	30/04/2020	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
A	Annex
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
ICT	Information and Communication Technologies
PbD	Privacy by Design
PETs	Privacy Enhancement Technologies

Executive summary

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

- An operationalisation of the legal findings of D8.1;
- Concrete recommendations for the PROACTIVE toolkit;
- Standards to follow in order to enhance users' acceptability of the toolkit, including vital aspects such as awareness, knowledge and consent.

It is described in the DoA in the following way:

> *"This operationalisation of the findings of D8.1 will constitute specific concrete recommendations for the PROACTIVE toolkit. This deliverable establishes the standards to follow in order to enhance users' acceptability of the toolkit, including vital aspects such as awareness, knowledge and consent."*

Along these lines, section 2 of this document includes further analysis of legal documents and ethical principles reflected in D8.1. Section 3 develops state of the art concepts on CBRNe policies and technologies acceptability, by using both materials from the literature and outcomes from the fieldwork activities. Sections 4 and 5 of the Deliverable operationalise the application of legal and theoretical normativity to PROACTIVE conducted in previous sections into concrete recommendations for its toolkit design, development and implementation. While section 4 focuses on legal recommendations, section 5 provides strategies to increase the acceptability of PROACTIVE products and protocols. Summary conclusions are introduced after these five segments.

By considering the content included in this Deliverable, PROACTIVE partners will be able to carry out their research activities legally and ethically. This Deliverable is meant to inform the project ethical and legal grounds, along with the requirements included in WP10.

Table of Contents

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 the 1st of May 2019 and will finish 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 second deliverable within Work Package 8 (Legal, Ethical and Acceptability Requirements) and is based on work carried out in Task 8.1. The aim of this Task 8.2, Operationalisation of legal requirements, ethical requirements and acceptability study into recommendations (M8-12), is to:

Task 8.2 will boil down all the questions that will be thoroughly analysed in Task 8.1 to practical and actionable recommendations that can be of use for people with technical backgrounds. This set of recommendations will be reflected in D8.2 which will establish the legal requirements to be followed for the design of the toolkit for CBRNe Practitioners. This includes several aspects that can be integrated "by design", such as the data management protocols to be accomplished, evaluations of how the LEAs are proceeding, considerations about the participation and treatment of vulnerable citizens when implementing the system and a series of technical recommendations based on stipulations imposed by the legal framework. The second part of D8.2 will reflect the results of the acceptability study to be conducted during the PROACTIVE exercises in WP6 (including focus groups with LEAs). This analysis will focus on establishing the standards to be considered in order to enhance users' acceptability of the toolkit, focusing on awareness, knowledge and consent. These references will feed each of the guidelines proposed by the project, which are targeted to different users and agents involved, according to their concrete needs and interests (fieldwork, including focus groups with LEAs).

D8.1 focuses on framing legal and ethical aspects in both the PROACTIVE research project and toolkit. Instead, this document aims at translating those requirements concerning the development and implementation of the PROACTIVE tools into more specific guidance for their design. The Deliverable will, therefore, focus on elaborating actionable **recommendations for PROACTIVE technology and protocols design derived from the identified legal requirements**. This

examination will be complemented with **an acceptability assessment of the toolkits to produce a general framework about** specific societal aspects to be considered for its successful implementation. These two levels of analysis will allow us to go beyond legal compliance and ensure secure and effective implementation of the PROACTIVE toolkits.

The methodology of this Deliverable is based on a comprehensive literature review that included both scientific papers and the examination of Deliverables 8.1, 1.1, 1.2 and 1.3. The acceptability analysis is also based on the participation of ETICAS in the PROACTIVE Workshop with Practitioners, EU LEAs, and policymakers conducted on 19th March 2020 and the subsequent analysis of the collected information from an acceptability perspective. The document is also based on a tabletop exercise (TTX) with 12 LEAs, ethics-legal experts and practitioners, conducted on February 4th, 2021. The session aimed to gather information about preparedness and response strategies in case of data breaches and assess the effectiveness of existing policies/technologies concerning this particular risk.

Moreover, a set of questions have been integrated into a survey and interviews with practitioners, social organisation and LEAs developed by DHPOL –as part of Task 2.3-. The survey and the interviews will be conducted over 2020. This part of the study will only be partially reflected in this document since it will be completed after the exercises in 2021, where acceptability aspects will be addressed based on the analysis of human-toolkit interactions. A second register of the acceptability analysis will, therefore, be included in D8.4 addressing also the concrete material collected during the exercises with this aim. In this way, the acceptability study will continue along with the project and the information collected during the exercises will be used to capture acceptance from a broader perspective (Branson et al., 2012).

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.
>
> 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 third and fourth objectives (in bold) are the ones addressed in this deliverable. This deliverable accomplishes them in combination with D7.4, Data Management Plan and Research Ethics, and the ethical/legal requirements included in WP10.

1.2. Description and structure

This deliverable is divided into the following sections:

- **Section 1 (Introduction).**
- **Section 2 (Summary of legal requirements):** The three regulatory frameworks and groups of documents analysed in D8.1, Human Rights, Data Protection and the GDPR, and the

CBRNe guidelines and legal provisions are summarised and further applied to the PROACTIVE case.

- **Section 3 (Acceptability and its implications in PROACTIVE):** It includes state of the art on the concept of acceptability and its specific forms within the framework of CBRNe policies. Special attention is paid to technological development and the perceptions of end-users in this context.

- **Section 4 (Legal based recommendations):** Based on Section 2, concrete legal recommendations for the materials and technologies included the PROACTIVE toolkits are detailed.

- **Section 5 (Acceptability based recommendations):** Based on Section 3, concrete acceptability recommendations for the materials and technologies included PROACTIVE toolkits are detailed.

- **Section 6: (Summary of actionable recommendations by phase and stakeholder):** On the basis of the previous analysis, specific recommendations for preparedness and response are structured according to three stakeholder groups: first responders, NGOs and policymakers.

- **Section 7 (Conclusions):** A short wrap up of all the analysis and recommendations is conducted.

- **Section 8 (References).**

2. SUMMARY OF LEGAL FRAMEWORK AND REQUIREMENTS IN PROACTIVE

Legal frameworks analysed in D8.1 provide the main requirements guiding the PROACTIVE project, including human rights, privacy and data protection and CBRNe, as well as the development and implementation of the PROACTIVE toolkit. In this section, we summarise these requirements focusing on those elements that are relevant for the legal, ethical and efficiency-oriented development of the toolkit.

2.1. Overview of fundamental rights implications in PROACTIVE

PROACTIVE protocols and strategies will be significantly oriented towards increasing and enhancing the communication and knowledge mechanisms used by LEAs and policymakers before and during a CBRNe incident. These toolkits are particularly focused on meeting the interests and needs of vulnerable social groups. However, it should be noted that the data exchanges that this implies, must be extremely **respectful of the fundamental rights to privacy and personal data protection**, as the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union (2016/C 202/02) point out. Section 2.2 of this document describes the legal standards on data protection that the PROACTIVE tools must comply with.

Firstly, the Charter of Fundamental Rights of the European Union, Article 8 (Title II: Freedoms), recognises **personal data protection** as a fundamental right and in its Article 7 also recognizes the right to respect for private and family life. Under these coordinates, users of the PROACTIVE toolkits must have the option to exercise these rights concerning the data they share with the system[1].

The Charter of Fundamental Rights of the European Union (CFR), the European Convention on Human Rights and the Universal Declaration of Human Rights emphasise the relevance of the right to **non-discrimination**. In PROACTIVE, discrimination may be based on the characteristics of many of the potential collectives using PROACTIVE toolkits, including people with disabilities. Vulnerable groups, particularly those protected by international conventions on human rights, also include the elderly, pregnant women, minors and religious minorities. PROACTIVE is aimed at ensuring better adaptability of CBRNe preparedness and response to these collectives, so special attention should be put on their integrity.

Another right to be considered within PROACTIVE is the **right to the integrity of the person** (Article 3 CFR) since the use and administration of the PROACTIVE technologies and recommendations can have effects on the physical and mental wellbeing of citizens. This issue entails that the technologies' managers should foster awareness of these risks among users. Moreover, Article 6 CFR frames the rights to **liberty and security**, which can also be harmed by the use of PROACTIVE if its technologies are misused. It should also be taken into account that PROACTIVE has potential implications in terms of the **freedom of expression and information** (Art 11 CFR) the **right to environmental protection** (Art 37 CFR).

Furthermore, documents such as the aforementioned Charter of Fundamental Rights of the European Union, the European Convention on Human Rights and the Universal Declaration of Human Rights, mandate specific public protection and guarantee equal treatment of vulnerable social groups. Among these safeguards, public institutions should take the initiative in the inclusion of collectives marginalised by their socioeconomic or cultural conditions. PROACTIVE follows these requirements in the field of CBRNe by producing specific guidelines for vulnerable groups, which bring new mechanisms for guaranteeing their active inclusion and equal security standards to those not belonging to these groups. Still, PROACTIVE must pay special attention to how the toolkits integrate specific innovations and mechanisms for such purposes, without creating new risks for these social groups.

2.2. Data protection requirements in PROACTIVE

The PROACTIVE guidelines and protocols for tackling and responding to CBRNe incidents, as well as its Information and Communication Technologies (ICTs), will involve the collection and treatment of personal data. Consequently, PROACTIVE toolkits will be regulated by the General Data Protection Regulation (GDPR). However, Law Enforcement Agencies (LEAs) will use the

[1] Along these lines, Article 5 of the General Data Protection Regulation of the European Union (GDPR), mandates that personal data must only be used for those purposes for which they were initially collected: "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". Furthermore, GDPR establishes that the data-subject has the right to data **access, rectification, erasure and restriction of processing** (Arts. 15 to 18).

PROACTIVE toolkit when processing personal data, but not mostly for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This distinction means that Directive (EU) 2016/680 of the European Parliament and the Council (known as the Police Directive) applies to PROACTIVE data management only in specific circumstances.

The PROACTIVE toolkits will process -and provide guidelines about how to process- data coming from first responders, LEAs, users of its toolkit and citizens in general. The focus of the toolkit will be on ensuring the rights of the most vulnerable groups in society in case of a CBRNe incident. Personal data processing, therefore, affects vulnerable groups who are the leading target group of the project set of tools and also individuals whose data could be collected during a CBRNe related event.

PROACTIVE **will process sensitive information**, including protected categories of data as defined in the GDPR (Art. 9.1), such as biometrics. The gathering and management of these data will be oriented to preparedness in case of CBRNe incidents and also include the management of further sensitive data (pictures, video, etc.) once these events occur. In line with the GDPR, processing this type of information, which may also include racial or disability identifiers, requires the establishment of specific security safeguards. It should be noted that the legal basis for processing these special categories of data could be individual consent in the case of PROACTIVE apps for LEAs/policymakers and vulnerable citizens. The apps will include a specific Privacy Policy with this aim (see current version at: https://www.proactive-app.net/privacy). However, within a particular context, public interest, as well as legitimate treatment, may also be the legal basis for the processing of personal data in the cases of data needed during an incident (see Section 2.2.2). In all cases, special security protocols and safeguards must be taken in its treatment. The management of these data should follow the GDPR requirements and standards applicable to the toolkit aims and functionalities already identified in D8.1.

In this section, we will summarise and organise these legal requirements in four dimensions: data governance, the legal basis of the processing, data management requirements and data protection of citizens interacting with PROACTIVE.

2.2.1. Data governance requirements in PROACTIVE

When talking about new technologies, especially those that include automatic devices, there is a need for clearly determining responsibilities and establishing accountability mechanisms. This implies to plan actions so as to respond to a potentially undesirable consequence of the development and use of those technologies, both in a prospective (regarding future actions) and a retrospective (past actions) manner. Given that technologies, even those considered “artificially intelligent”, are not capable of intention and agency, and those responsibilities should be explicitly attributed to humans in charge of their design, development and implementation, these principles apply to the stakeholders involved in the PROACTIVE project as well as its toolkit.

The GDPR establishes different figures related to these mechanisms of responsibility, which are explained below:

The **data controller** of the personal data collected before, during and after an incident, can be a natural or legal person but also any public authority (in PROACTIVE, LEAs managing the system). This figure is in charge of ensuring that the purposes and means of such processing are respected

(Article 4, 7, GDPR). Data management responsibilities include the proactive setting of technical and organisational measures for ensuring this as well as other several responsibilities[2]. The controller should complement security measures with a systematic register of processing activities, which is particularly relevant in the case of special categories of data (Arts. 9 and 82 to 84).

Processors can treat personal data on behalf of the controller, as stated in Article 4(8) and can only share this data with another processor under the authorisation of the controller. Furthermore, the conditions of the relation between the controller and the processor(s) have to be reflected in a binding document (Art 28). The processors must also keep a record of their processing activities (Art 30).

In some instances, involving the processing of a certain amount of personal data, or when the processing is a special kind of entity, the GDPR mandates both controllers and processors to appoint a **Data Protection Officer** (DPO) (Article 37.1). This DPO is in charge of providing advice to data subjects and monitoring compliance.

Lastly, it should be noted that the operationalisation of data protection requirements into specific recommendations for the PROACTIVE toolkits is focused on the standards for data management and Privacy by Design in CBRNe events. However, the implementation of the PROACTIVE toolkits will have to be based on an assessment of each data governance and legal frameworks in place. This data governance scheme will also depend on national, European or third countries legal frameworks. These case-specific aspects also concern the responsibility of controllers based in Europe in their relationships with third parties in third countries who may act as data processors established in Article 44 of the GDPR.

2.2.2. Legal basis for the processing of personal data in PROACTIVE

In PROACTIVE, the processing of personal data by the legal subjects described in the previous section may be mostly conducted on the basis of (Article 6 GDPR) explicit consent (a). A Privacy Policy has already been developed with this purpose and integrated into D4.1 It includes all mandatory information such as voluntariness, users' rights and DPO contact point. Informed consent must be provided by the data subject for one or more specific purposes. However, in certain scenarios, for instance, when the App is reused with law enforcement purposes, the legal basis for the processing could be one or more of the following conditions contemplated in the GDPR (in particular d and e):

[2] 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).

> *"b. processing is necessary for **the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
>
> *c. processing is necessary for **compliance with a legal obligation** to which the controller is subject;*
>
> *d. processing is necessary in order to **protect the vital interests** of the data subject or of another natural person;*
>
> *e. processing is necessary for the performance of a task carried out in the **public interest or in the exercise of official authority** vested in the controller;*
>
> *f. processing is necessary for the purposes of the **legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."*

The processing of personal data as part of the implementation of first response strategies and mechanisms integrated into the PROACTIVE toolkits will be based on many of the legal bases above, depending on the scenario, context and responsible person in charge. While consent is vital in both GDPR and public engagement in preparation actions, public interest will be one of the legal basis for the intervention of LEAs in response actions. At the same time, the processing of users' personal data by PROACTIVE App will have to be based on informed consent. However, points d (vital interest) and e (public interest) in Article 6 give room for other processing actions to be fostered by the PROACTIVE guidance tools or for certain usages of its technologies by public authorities.

As a general principle, respect for the purposes of data collection described in the consent forms and privacy policies of the PROACTIVE platform and Apps must be followed. Competent authorities **must consider the primary purpose for the processing**. However, they can also **identify whether the processing of personal data can be conducted under the GDPR rules or satisfies the criteria of the law enforcement purposes under national transpositions of the Law Enforcement Directive (LED)** (2016/680) (de Hert and Papakonstantinou, 2016). The GDPR defines the overall rules for public and private personal data processing and thus can be viewed as *lex generalis*[3] and the Directive 2016/680 addresses the specifics of the law enforcement domain and works as *lex specialis*.

[3] It comes from the legal maxim in Latin: "*Lex specialis derogat legi generali*". In international law and some specific cases, if two laws govern the same factual circumstance, a law ruling a specific subject matter (*lex specialis*) overrides a law governing only global matters (*lex generalis*). In the context of this Deliverable, we use lex generalis to frame the GDPR to illustrate that applies to the more specific goal of the PROACTIVE toolkit, which is raising awareness about CBRNe events and ensures the safety of citizens in front of these situations.

In the LED, data controllers identified as "competent authorities" processing personal data for "law enforcement purposes" fall outside of the scope of the GDPR. Competent authorities include the police, national courts, and other judicial authorities, prosecution, customs and border guards. Depending on the country, other authorities may be specialised agencies having investigatory powers or other departments with similar competences. **The applicability of this regime, concerning the national definitions of competent authorities and how the purposes of the data collection are defined and secured, will need to be assessed on a case-by-case basis**. Still, in case that the data controller of the PROACTIVE toolkit is a competent national authority and the purposes of the processing are the prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties (Articles 2(1) and 1(1), then the processing falls under the LED.

The definitions of competencies and responsibilities in the management of the PROACTIVE technologies in a particular country will have to consider that certain forms of data processing within PROACTIVE, such as first responders storing information of the platform in their servers, could be framed as being 'on behalf of' law enforcement authorities qualifying them as 'data processors' under the Directive 2016/680 (Caruana, 2017). In this regard, due to the characteristics of the PROACTIVE toolkits, data collected with prevention purposes may have to be used to resolve other criminal offences or conduct criminal investigations making a strict application of the purpose limitation principle difficult. Directive 2016/680 thus allows the use of data for purposes other than those for which they have been gathered as long as the processing is in line with three requirements described below:

- the general purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,
- the controller is authorised to process such data by law,
- and the processing is necessary and proportionate (Article 4.2).

Having provided this overview of the legal frameworks around PROACTIVE, the data protection analysis in this deliverable is guided by the *lex generalis* approach provided by the GDPR.

2.2.3. Data management requirements in PROACTIVE

The processing of personal data must be based on **accountable, transparent and explicit information** about the purposes (Article 13 GDPR), means and aims of the processing. Both controllers and processors should provide appropriate information to data subjects so they can make their rights respected. In case **informed individual consent** is the legal basis for the processing, targeted strategies to guarantee the decision-making capacity of vulnerable groups will be produced. Moreover, assent strategies for the ones that are not capable of providing consent will be established. In many cases, this involves having mechanisms in place for targeting minors, disabled people or other social groups who may not be able or allowed to consent by themselves. PROACTIVE is aimed at filling these gaps, so it is expected to consider how specific social groups will benefit from new and multi-level strategies of inclusion in CBRNe scenarios. Moreover, a certain level **of harmonisation of these processes across EU nations** is expected, which means considering, for instance, the minimum legal requirements for minors across countries, which would be accessing explicit consent of both parents of minors below 18 years old, always when possible.

Information to be provided to users and practitioners includes the types of personal data to be processed, the **contact information of the data processors and controllers**, the recipients of the data and potentially third parties involved in the processing. In a scenario of an incident, this information may not be collected before data collection as mandated by the GDPR when processing is based on consent, but measures to ensure these standards can be included in on-going and post-events frameworks. In this context, the right to access, rectify and erase personal data should also be considered, when appropriate (see section 2.2.4).

Furthermore**, integrity and confidentiality (Article 5.1,f) of personal data** must be ensured both through by-design strategies and once the PROACTIVE guidelines and technologies are implemented. In line with the above explanation, measures to avoid both unauthorised access and data breaches are multiple and range from correct anonymisation of personal information to data erasure respecting the data minimisation principle. Security strategies to prevent personal data misuse or abuse are an essential aspect of data protection legislation and the GDPR (Article 32.1). This involves producing systematic security assessments which must be adapted to the PROACTIVE specific processes and performance.

Data breaches should be prevented proactively both in terms of data governance and regarding technological design. The GDPR Article 33.1 mandates to notify data subjects about data breaches without undue delay and where possible “not later than 72 hours after having become aware of it”. Since CBRNe attacks are often accompanied by personal data breaches and fake news dissemination, the strategy for addressing these breaches should have a holistic perspective. Notification of breaches in PROACTIVE should, therefore, be integrated into a broader scope of action and address the relations to “external” stakeholders such as the media or vulnerable organisations. Since the GDPR do not specifically determine how notifications have to be produced, one of the activities of PROACTIVE may be the development of effective communication strategies not only for CBRNe events as expected but also concerning data breaches.

Moreover, Article 33.5 GDPR mandates to register personal data breaches properly. This register should include all relevant information about the infringement such as data subjects involved and the remedial actions are taken. Additional measures to be made by the data controller in case of breaches include notification to the supervisory authority as mandated in Article 34.1. Specific mechanisms to ensure these actions to be taken will need to be embedded in both the guidelines and Apps of the project. Privacy by Design (PbD) and Privacy Enhancement Technologies (PETs) are also essential to ensure the above principles. The requirements included by design in Task 4.4 by ETICAS, RINISOFT and other partners are aimed at fulfilling these standards.

One specific measure to be considered is the establishment of mechanisms to **ensure algorithmic fairness** in data processing. This is expected in the GDPR to avoid profiling of data subjects as mandated by Article 22(1) and (4). This requirement is also relevant for the PROACTIVE Apps since they will include by-design automated solutions for categorising information. In this regard, mechanisms for avoiding the transmission of information leading to false positives or the stigmatisation of protected groups may be considered.

Other methods for securing data in the GDPR are **pseudonymisation and anonymisation**. Following Article 4(5) GDPR, pseudonymisation should always be applied when allowed by achieving the purposes of data collection and where it is in line with the protocols or technological systems at hand. Pseudonymised data is data that can no longer be attributed to a specific data

subject without the use of additional information. Following this principle, PROACTIVE tools pseudonymising personal data should ensure that additional information can be kept separately. It should also be subjected to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Moreover, when applicable, personal data stored by the PROACTIVE App or any other information to be used by LEAs or first responders as part of their duties should be **anonymised**. This criterion should also be reflected in the PROACTIVE guidelines, according to the standards established by Working Party P29 (2014). Anonymisation consists of altering the dataset containing personal data in a manner that makes it theoretically impossible to re-identify individuals. PROACTIVE should establish mechanisms to ensure the highest accuracy of its tools and technologies while minimising the collection and processing of sensitive data. With this aim in mind, personal data may be anonymised at some point after its collection for first response preparedness or activation purposes. Anonymisation is the most secure data protection method, and it is particularly recommended when sharing information with third parties (legal subjects beyond the controller and processors).

Both controllers and processors must develop protocols in line with the **data minimisation** principle (Article 5,1,c). In PROACTIVE, the minimum amount of personal data needed to achieve the functionalities of its toolkit should be collected. Aims behind these functionalities include increasing practitioner effectiveness in the management of a large group of people in CBRNe, enhancing preparedness against and response to these events and facilitating subsequent decontamination procedures by better articulating the different stakeholders. The set of legitimate and technically required purposes of the processing should be delimited in advance and take into account in the above aims.

Moreover, following Article 5.1 (d), GDPR, efforts must be made to ensure that the information collected and provided by processors and controllers in PROACTIVE is **accurate**. Accuracy involves both classical methods for ensuring data quality, such as proper classification or erasure methodologies, but also protocols for guaranteeing the veracity of provided data. It is expected that PROACTIVE will contribute to data quality in CBRNe events through the dynamisation and systematisation of communication between LEAs, policymakers and citizens. This goal will also be reached by producing guidance for preparedness and response to CBRE events, such as those concerning false positives about suspects of human harm. Contributions of PROACTIVE in this regard relate to specific guidelines integrated into the PROACTIVE toolkits with this purpose but also concern the App used for promoting PROACTIVE aims. Such an App should also incorporate a mechanism for assessing and filtering fake news or unreliable collected information, including systems for avoiding algorithmic discrimination. These mechanisms also include forms of ensuring that data subjects can ask the controller to erase or rectify the data that it has regarding them (Articles 16 and 17 GDPR). In the case of non-trustable data[4] do not involve personal data, this issue is out of the scope of GDPR, but this issue is still relevant for PROACTIVE efficiency and aims.

Guidelines and recommendations produced by PROACTIVE should also consider that data collection and management must follow Article 5.1(e) on **storage limitation**. The data controllers

[4] Namely, data that is taken from non-well-selected sources, managed without taking into account its legal and ethical intended use, and delivered in non-appropriate formats and time frames.

and processors must not keep personal data collected before and after a CBRNe incident for any longer than is reasonable for achieving the purposes for which they were collected in the first place. These original purposes, which may include providing better guidance to vulnerable groups, will determine the legal and legitimate data retention period. Still, the rationale behind data storage must be accompanied by a proportionate and rationally justifiable data storage policy in all cases, including those where the system retains data subjected to a criminal investigation

The Data Controller and the DPO must also monitor the need for conducting a Data Protection Impact Assessment as mandated in Article 35.1 GDPR. The evaluation of this need must be based on the characteristics and the amount of personal data to be processed as well as on the integration of new technologies to personal data processing. Even though this is case-specific, contingency plans should be established as part of the PROACTIVE project to anticipate potential scenarios where these conditions may be accomplished. The PROACTIVE toolkits should, therefore, include references for the evaluation of these monitoring activities before and after an incident. This framework should also include recommendations for the adoption and implementation of the PROACTIVE platform and apps.

Lastly, other recommended data security measures suggested in the GDPR include **encryption, access control and password protection**.

2.2.4. Data protection rights of stakeholders interacting with PROACTIVE toolkit

Besides the above data governance, normative and security requirements, the GDPR regulates many relevant aspects for PROACTIVE concerning the toolkit-users interaction. It establishes specific data protection rights of individuals and social groups using the toolkits and the PROACTIVE platform and Apps. LEAs, policymakers and citizens must have all data protection rights guaranteed when sharing their data with other citizens, the police and other first responders who may be acting as data controllers. Examined from the perspective of subjective rights, PROACTIVE must be able to tackle many challenges concerning the use of personal data as part of a CBRNe incident management and ensure further control of personal data for citizens within these disruptive conditions. In the following section, rights stipulated in the GDPR (chapter III) and their implications for PROACTIVE are listed:

- **Right to transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12):** “The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means”. Moreover: “The controller shall facilitate the exercise of data subject rights under Articles 15 to 22.” PROACTIVE has the obligation to be transparent and provide relevant information about the data processing involved in the process and the toolkits, as well as to ensure the data rights of users and stakeholders.

- **Right to information and access to personal data**. The GDPR establishes a list of information to be provided where personal data are collected from the data subject (see: Article 13), as well as that what is expected to be provided where personal data have not been obtained from the data subject (see: Article 14). In compliance with those requirements, PROACTIVE should guarantee the means so as to properly provide this information to users and stakeholders.

- **Right of access (Article 15):** "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". The PROACTIVE toolkits will, therefore, have to establish technical and managerial instruments to guarantee that the collected personal information can be available and accessible to data subjects before and after an incident.

- **Right to rectification (Article 16):** "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." PROACTIVE will have to integrate into its guidelines protocols to ensure that data provided or obtained from citizens and first responders can be rectified when this depends on the controllers. Such protocols must also be embedded in the PROACTIVE apps technical capabilities. This right relates to the management of false positives based on PROACTIVE toolkits. PROACTIVE must improve first response protocols and the collection of personal information in this context -such as pictures in public spaces- concerning the filtering of wrong information. In the case that individuals targeted as victims or perpetrators of CBRNe offences are inaccurately identified, rectification mechanisms should be in place.

- **Right to erasure (the right to be forgotten) (Article 17):** "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" Point 2 of this article indicates that the controller must establish the technical capabilities for ensuring that erasure of personal data can be conducted appropriately. This condition applies under concrete ground detailed in Article 17. It includes those cases where data is no longer needed for pursuing the aims for which was collected. PROACTIVE should distinguish in this regard between data to be used to prevent or tackle incidents and those data related to criminal offences in the context of CBRNe incidents. In this regard, it should be taken into account that public interest is an exception to this right in Article 17, 3 and those cases where the PROACTIVE technology falls under the LED.

- **Right to restriction of processing (Article 18):** The data controller is mandated to restrict the processing of personal data when the data subject questions their accuracy or the data is no longer needed for the aims of the processing. As with other subjective rights in the GDPR, the controller must be technically and logistically able to ensure such restriction. The PROACTIVE toolkit should, therefore, propose a scheme for the use of personal data that facilities such a restriction from the managerial and technical standpoints.

- **Right to be notified regarding the rectification or erasure of personal data or the restriction of processing (Article 19):** 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 PROACTIVE controller shall be able to inform the data subject about those recipients if the data subject requests it.

- **Right to data portability (not for public authorities) (Article 20**): "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...". In line with the above, the PROACTIVE App and data collection strategies for incidents, as well as subsequent data management steps, should ensure data quality and systematic formatting of personal data. Such efforts should be focused on guaranteeing its efficient transmission in the case it is required by the data subject.

- **Right to object the processing (Article 21):** "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." As with the right to be forgotten or the right to rectification, practical protocols and technical mechanisms for ensuring that personal data can be erased, rectified or removed if there are legal grounds for it should be established.

Some authors, like Mora (2019: 147), have mentioned that, in the exceptional circumstances of CBRNe events, "data are likely to be collected without the data subjects' consent, under highly stressful conditions, in the absence of normal infrastructure, and in the midst of political and legal uncertainty". In this framework, data protection aspects have often been relegated to a secondary level of importance. Other rights, such as the right to the integrity of individuals, are often the focus of preparedness and response strategies. In any case, it is important to remember that this should not be taken as the norm, not as a desirable action.

As we can see above, **PROACTIVE can widely contribute to establishing a new standard in the management of personal data of vulnerable groups in the context of CBRNe incidents**. There is room for improvement in each of the above-presented rights, which requires proposing specific recommendations and best practices for preparedness, response and subsequent stages of CBRNe events and taking access, rectification, cancellation and opposition (ARCO) rights perspective to the design of its app. PROACTIVE can set a framework for ensuring that gaps concerning the current legal framework on Data Protection in CBRNe crises are addressed. The PROACTIVE tools can embed data protection and privacy rights, in part by exercising existing restrictions to data processing in these scenarios (Mora, 2019) while ensuring that security and safety levels are enhanced.

2.2.5. Identified data protection requirements for the PROACTIVE technologies

The PROACTIVE toolkits include a **collaborative platform and two mobile apps** designed to support LEAS, policymakers and citizens in the case of a CBRNe event. The toolkits will facilitate bi-directional communication between stakeholders to enable pre, during and post-incident information sharing. The toolkit must allow LEAs and security policymakers to select, configure and adapt their preferred tools according to their needs and preferences. Its design is expected to be modular, flexible, adaptable, and scalable enough so as to allow users from different social groups and countries to use it effectively. It will also adapt to different event scenarios, ensuring the information available is relevant to the user. These systems will integrate inputs from the gaps, needs and requirements (WP1), and the planned workshops (WP2), as well as Ethics and Legal aspects (WP8).

The PROACTIVE platform and apps will be designed to pr**ocess personal data for a series of purposes**. All personal -or personally identifiable information (PII)- that is gathered and stored must be treated following the above-detailed GDPR requirements or administered under the LED provisions accordingly. RINISOFT and ETICAS have already established a specific list of data protection requirements for the technological systems' on-going design. An updated analysis of these requirements is set in the following sections for each of these systems

2.2.5.1. The Web Development Platform for LEAs and policymakers

LEAs and policymakers will use the Web Platform. It will provide reporting tools (including visualisation methods) for **LEAs to monitor communities, assess risks, assess threats, assess vulnerabilities, assess incidents and allocate resources**.

2.2.5.1.1. Platform data governance

The Platform will be **administered by LEA's and policymakers**. It will have restricted access via a registration method. The levels of registration are still to be confirmed and will have the necessary corresponding security levels. At present, this includes: Admin; (LEA) responsible for the overall platform, a slightly restricted user (policy maker), and a low-level user, (citizen)[5]. All User(s) will be able to customise the tool according to the context of a specific scenario (location - map-based), the type of incident and the policies required for particular events. Users will select their preferred location when they log in. The platform will use a GIS-based backend, for the geo-located data gathered, enabling the GIS-oriented data storage, management and analysis. The LEA's will be reliant on a map to record incidents, manage/ allocate resources and potentially record images to the specific incidents on a map.

The platform must be available via the Police Secure networks. The system will need to be certified and tested by Police IT & Digital teams to meet stability and security standards. In line with these specifications, **it is likely that LEAs will be data controllers of the system in most cases**.

[5] Still under discussion, during PM3, it was raised the LEA's would need a separate access from policy makers to discuss sensitive operational information.

2.2.5.1.2. Personal data to be processed

Personal data collected and shared by LEAs and practitioners will include a valid email address, organisation and Name/ position of users; geolocalisation will be applied. Also, **information collected by citizens**, including vulnerable population, before and after the event, will be processed.

2.2.5.1.3. Functionalities and aims of the processing

The platform will allow Bi-Directional Communication between LEAs and Security Based Policymakers via direct messaging and forums. The collaborative platform will include an Online Coordination Portal. Text, images, videos, audio files and PDF documents will be exchanged through the platform. LEAs and Policymakers will be able to upload and download these data. This platform will include GIS oriented data storage so LEAs can identify where an incident has occurred and also track related information.

The platform will enable LEAs and policymakers to create an FAQ page with useful advice about the website itself or about particular situations in their area. Moreover, it will enable LEAs and policymakers to provide/ signpost users to other relevant sites/ contacts for useful information, for example, accommodation, help lines, charities etc.

2.2.5.2. Mobile Application for LEAs and Policymakers

The App used by LEAs and policymakers will replicate the features in the web platform, **providing the users with remote access to the information they require in real time**. LEA's and policymakers will, therefore, be able to upload, download and also remove data, including personal information.

2.2.5.2.1. LEAs and policymakers App data governance

The Mobile Application will be administered by LEA's and used by policymakers. The App will have restricted access via a registration method, again replicating the web platform[6]. The system will need to be certified and tested by Police IT & Digital teams to meet stability and security standards. The content and credibility of the information will be up to the LEA's and policymakers. In line with these specifications, it is likely that LEAs will be data controllers of the system in most cases. First Responders, who will be provided with access to some information, will possibly act as data processors on behalf of the police.

2.2.5.2.2. Personal data to be processed by the App

The modular App administers relevant -and sensitive- information about incidents and includes references about its characteristics and management. Voice, text, video, images and PDF documents will be shared by stakeholders to dispatch emergency-related information to First

[6] I have assumed LEA's will use the App to discuss operational issues on site and therefore will have to adopt the 3 levels of registration used for the web platform.

Responders, providing the capability to access and exchange personal data. Users will have to share a valid email address, organisation and Name/ position of users; geolocalisation will be applied.

It should be noted that the App will allow access to **sensitive information about CBRNe incidents and communities in real-time**. Such information will be shared between stakeholders. It also offers the capability to access and exchange emergency-related information with their chains of command and, when useful, directly with citizens. The mobile LEA App uses the same API as the web, so the functionality provided by the mobile App is very similar. To share the data with a citizen, LEAs would have to upload the data as normal, then review it and send it off for dissemination via the public App. Pre-incident, real-time, and post-incident emergency-related information will be uploaded directly with citizens (push effect), and other LEA's/ policymakers using multiple media options.

2.2.5.2.3. Functionalities and aims of the processing

The App will offer the same functionalities as the platform, including customisation and geolocated data. The App functionalities, including visualisation methods, will allow LEA's to assist in monitoring communities, assessing risks, assessing threats, vulnerabilities, incidents and allocating resources. As for the platform, the language of the static App content will be English (to reflect NATO standards). It must be available for cache data in areas where the internet is not available and should be uploaded automatically when it becomes available.

The App must provide an option to view and validate any content uploaded to the web platform, and it must provide the ability to report and see an incident at a specific location using a map. Furthermore, it will give the users advice about the website itself or about particular situations in their area via an FAQ page. Lastly, it will signpost users to other relevant sites/ contacts for useful information, for example, accommodation, helplines or charities. The LEA's will be reliant on a map to record incidents, manage/ allocate resources and potentially record images to the specific events on a map.

2.2.5.3. Mobile App for vulnerable citizens

This **App will allow vulnerable citizens to communicate with other citizens, LEAs and security policymakers** through selecting, configuring and adapting their preferred tools according to their needs and preferences. Vulnerable citizens will **be able to download and -with filter- upload personal data** (PDF, videos, images, audio files).

2.2.5.3.1. LEAs and policymakers App data governance

The App will be administered by the corresponding data controller (LEAs or authority in charge). It will have two access levels: **Registered User** (enables citizens to report emergencies and well as view information) and **Non-registered users, which enables citizens to view information but not report**.

2.2.5.4. Personal data to be processed

Data to be processed includes personal data shared by authorised users, including LEAs, public authorities and vulnerable groups using the application, such as images, video or audio. Users will have to share a valid email address; geolocalisation will be applied.

2.2.5.5. Functionalities and aims of the processing

The App provides video (for sign language support), **real-time text, text-to-speech features and an intuitive user experience environment**, with smart buttons and visual instructions to receive pre, during and post -incident information on CBRNe incidents. It will also be able to receive automated early warnings issued by authorities. Considering VoIP, web portals, softphones and social media platforms, the vulnerable citizens' App will place significant emphasis on delivering broad accessibility and the ability to review or report an incident at a specific location using a map. **However, it will be made clear that the App is not to be used for reporting emergencies. For this, the normal protocols will be used, mainly contacting 112**.

Its static content shall be initially in English (to reflect NATO standards). It will include various settings for accessibility; Font Size & Type, Colour of Screen to support colour blindness, no flashing images will be used to reduce issues with epilepsy, audio options/ voice control for the visually impaired/ or those with dyslexia, and sign language videos for those with limited hearing.

It is expected that the App uses novelty (e.g., cartoon characters, pictograms or symbols) where appropriate to reduce the issue of language barriers. It will be available for cache data in areas where the internet is not available and should be uploaded automatically when it becomes available.

The App will enable the user to select their preferred location when they log in. Moreover, it will provide the citizens with useful advice about app's functionalities and about particular CBRNe situations in their area via an FAQ page. Included in this page will be a section prompting the information to be provided during an incident, such as the route to the event or medical symptoms. Lastly, it will signpost users to other relevant sites/ contacts for useful information, for example, accommodation, helplines or charities. It will reference existing apps (providing links when possible).

According to the preliminary analysis established in D8.1, the baseline legal criteria in Table 1 should be followed in the design and implementation of the above technologies.

Table 1 Preliminary data protection requirements for the PROACTIVE technologies

Issue	Relevant article (GDPR)	Applicability in PROACTIVE and recommendations
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.
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.

Issue	Relevant article (GDPR)	Applicability in PROACTIVE and recommendations
Record keeping	Article 30	Controllers and processors processing sensitive categories of personal data need to keep records of their processing activities.
Informed consent	Article 7	The processing of personal data within the PROACTIVE toolkit may be carried out almost exclusively on the basis of informed consent. • Users shall be required to sign a consent form and disclaimer before accessing the data. Assent, when applicable, will be sought. • Users of the system will be given the ability to opt out of the collection of personal and sensitive data about him or her. • Users will be notified of the parties to whom the data may be transferred, the conditions for transferring the data to third parties, and the rights of the individual (data subject) concerning further processing of their personal data. • Users will have a right to change their mind and withdraw any personal data which is sent.
Principles	Article 5	Data protection principles must inform the development of the different toolkits in PROACTIVE. • All data collected through the system are only to be used for the stated purposes. This must be enforced organisationally and supported programmatically.
Security	Arts 1,f and 4.12	Personal data must be processed in a secure way according to the risks created by them. • Images and videos of children can have particular data protection issues and should be reviewed carefully before being made public (purpose limitation). • Only data which is absolutely necessary for the functioning of the system are to be collected (data minimisation).
Data breach	Article 33, 34	Partners must follow the procedures established in this deliverable and the joint controller's agreement.

Issue	Relevant article (GDPR)	Applicability in PROACTIVE and recommendations
Rights of data subjects	Article 12-22	The rights of the data subjects must be ensured by communicating their existence to the research participants before they consent (when applicable). Also, each organisation's DPO needs to have the necessary resources for ensuring that the research participants' rights are respected at all times. 1. Users of the system will be made aware of the limitations of these services, the extent of data to be collected (including their IP address), their right to remain anonymous and the purposes for which this information will used 2. Images, voice recordings and video can be classed as personal data and need to be held as securely as other forms of personal data. This is especially the case if the image or voice of an individual who has not consented to using the system is inadvertently captured by a consenting user. In these cases, very careful consideration should be given before these materials are released on the public. 3. Users should not feel pressured to supply personal or sensitive information that they do not wish to share. 4. Users will have the right to access their personal data from the system and will have the right to rectify it, if needs be.
Data Protection by Design and by Default[7].	Article 25	5. The Toolkit Controller has to implement technical, organisational and security measures so as to comply with data-protection principles, respect the rights of the data subjects and meet the requirements of GDPR in an effective manner. This has to be done both at the time of definition of the means for processing and at the time of the processing itself. Besides, this has to take into account the state of the art, cost of implementation and the nature, scope, context and objectives of the data processing. 6. System should allow for both registered and anonymous users. 7. All data collected, stored, processed and retrieved by

[7] These requirements have already been defined by RINISOFT with the support of ETICAS and the rest of the project consortium.

Issue	Relevant article (GDPR)	Applicability in PROACTIVE and recommendations
		the system will be held and transferred through highly secure systems to prevent loss, damage or unauthorised access. These systems should not be based outside the EU unless absolutely necessary. 8. When (if) registering, the users profile shall not demand any personal data. All data requested must be volunteered by the user and not compulsory, except for the email address. 9. System shall not disseminate personal information of users. 10. Maps must be designed in such a way make the identification of particular home or address difficult.

Source: own elaboration.

2.3. CBRNe legal framework and international guidelines

Since 1997, when the Council of the European Union approved a major civil protection action programme through the Council Decision 98/22/EC establishing a Community action programme in the field of civil protection, efforts for better coordination of CBRNe preparedness and response at the EU level have been continuous. The need for a common European Union common framework on disaster management, with the potential to allow Member States to pool resources and improve their response, was translated into different legal provisions, guidelines and policy measures over the next decade. Actions promoted by the Member States in this framework have focused on enhancing their own response systems but also on fostering mutual assistance and even proposing common training programs.

Concerning regulations, or legally binding documents such as EU Directives, the main requirements established and measures promoted that are relevant for PROACTIVE implementation are summarised in Table 2:

Table 2 Legal CBRNe documents and relevant requirements for PROACTIVE

Regulation or legal document (by year)	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
Council Decision of October 23, 2001, establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions.	Enable cooperation within civil protection agencies.	• This document set up the Community Mechanism for Civil Protection.

Regulation or legal document (by year)	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
Treaty of Lisbon (2007).	Establishes competencies for the European Union to carry out actions to support, coordinate or supplement the actions of the Member States in civil protection.	• The "Solidarity Clause" was meant to complement the "Mutual Defense Clause" with the aim of more efficiently facing new kinds of threats (Art. 22). It imposes significant obligations upon member states and attempts to **foster cooperation during catastrophic events**, such as CBRNe attacks.
Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (2013)	It aims to strengthen the cooperation between the Union and the Member States and to facilitate coordination in the field of civil protection.	• Better cooperation and coordination, without prejudice to the Member States' primary responsibility to protect people. • To provide Member States **disaster-management systems** with sufficient capabilities to enable them to cope adequately and in a consistent manner with disasters.
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	It establishes a common definition of terrorism.	• Ensure conceptual harmonisation.
DECISION (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements	- It lays down the EU Integrated Political Crisis Response ('IPCR') arrangements.	• The IPCR enable timely coordination and response at Union political level for crises. It can be used by the Council activate the solidarity clause as set out in Article 1(2) of Council Decision 2014/415/EU. • Its tools include **analytical reports to provide decision-makers** with a clear picture of the current situation; a web platform to exchange and collect information;

Regulation or legal document (by year)	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
		and a 24/7 contact point to ensure constant liaison with key actors.

Source: own elaboration.

Besides the binding and non-binding legal texts reflected above, there is also a series of EU communications, plans and guidelines that provided a relevant framework for the PROACTIVE project requirements. Table 3 summarizes these documents described in D8.1 and identify their main requirements connected to the PROACTIVE toolkit.

Table 3 Reports, plans and communications on CBRNe relevant for PROACTIVE

Report, plan or communication	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
"Communication from the Commission to the Council and the European Parliament — Civil protection — State of preventive alert against possible emergencies"). (COM (2001) 707 final.	Facilitate reinforced cooperation in civil protection assistance intervention.	• Proposes the establishment of a Community mechanism for cooperation in this domain.
The European Counter Terrorism Strategy (2005)	To fight terrorism globally and make Europe safer.	• 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; • **Response, by preparing, managing and minimising** the consequences of a terrorist attack, is the fourth objective of the EU counter-terrorism strategy.

Report, plan or communication	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
Barnier Report (2006), -commissioned by José Manuel Barroso and Wolfgang Schüssel-.	12 measures were considered relevant as far as the enforcement of the EU's capacity to respond to a crisis.	• A European-wide civil protection force Europe Aid; • Integrated European approach to anticipate crises; • **Clear information system for European citizens;**
European CBRNe action plan (2009) and the Progress Report on the Implementation of the EU CBRN Action Plan (2012)	Aimed at reducing "the threat of and damage from CBRN incidents of accidental, natural and intentional origin, including terrorist acts."	• Further work and a structured approach at the EU level in the CBRNe field. • Continued and further streamlined research into the CBRN areas". • **Keep track on and disseminate research results in this domain by EU bodies or Member States** • Get away from a pure "shopping list" of individual actions and develop a more strategic and overarching approach to CBRN policies. • **Developing a more strategic and overarching approach to CBRN and explosives (E) policies.**
The Stockholm Programme (2010)	It calls for the development of an internal security strategy in order to make Europe more secure.	• Strengthening EU cooperation in law enforcement, border management, civil protection, disaster management as well as judicial cooperation in criminal matters.
The EU Internal security strategy (2010)	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.	• Its objective 5 is to **"Increase Europe's resilience to crises and disasters,"** used a cross-sectoral approach • Calls for improvements to long-standing crisis and disaster management practices in terms of efficiency and coherence. • **The importance of increasing the protection for individuals, especially the vulnerable ones, is underlined in the document.**

Report, plan or communication	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
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. Principles established in the conclusions on preparedness and response in the event of a CBRNe attack.	• 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**.
Council conclusions on the new CBRNE Agenda (2012)	The Council's conclusions on the new CBRNe agenda calling to a comprehensive approach to CBRNe incidents including crimes and terrorism.	• Establishment of a structured approach to prevention, detection and response, **focusing on enhanced interagency collaboration especially between law enforcement, military, civil protection**, • On-going development of close interaction on CBRNe between the public sector and private actors. • Development of prevention and detection measures, awareness raising, and research on the security of CBRN materials and explosives • Exchange, as appropriate, of information and knowledge regarding the management and handling of incidents with CBRN materials and

Report, plan or communication	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
		explosives.
Communication from the Commission - An Open and Secure Europe: making it happen (2014)	It also establishes its vision on the future agenda concerning Home Affairs. It also arranges the Commission's guidelines concerning the political direction to be taken by the EU's efforts towards a more open and safer Europe by 2020.	• The only mention of CBRNe can be found in section 5.2 **"Prevention of terrorism and addressing radicalisation and recruitment".**
The renewed European Union Internal Security Strategy (2015)	It aims at enhancing the level of protection of European citizens concerning an on-going surge of threats, particularly those posed by terrorism and serious and organised crime.	• Ensuring full compliance with fundamental rights, including those related to privacy, personal data protection, confidentiality of communication and the principles of necessity and proportionality.
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).	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.	• **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. • Developing **practical and effective tools for practitioners, ranging from workshops, guidance materials, training and awareness rising to supporting research and testing activitie**s. • It fosters better detection, using better research, testing, and validation, training, awareness and capacity building.

Report, plan or communication	Approach and aim(s)	Relevant requirements and recommendations for PROACTIVE
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)	The document points our 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.	• Reducing the accessibility to CBRN materials; • Ensuring a more robust preparedness for and response to CBRN security incidents; • Building stronger internal-external links and engagement in CBRN security with key regional and international EU partners. • **Enhancing our knowledge of CBRN risks.**

Source: own elaboration.

As we can see above, both the regulations and reports produced at the EU level have evolved from the establishment of general requirements and recommendations focused on better coordination of EU agencies in crises and disasters prevention and response to more specific institutional developments and measures, which have also put greater focus on CBRNe. Still, both groups of documents show a certain level of ambiguity regarding the definition of specific actions to be fostered by the Member States and the establishment of particular cross-national harmonisation mechanisms.

Many documents, including The European Counter-Terrorism Strategy (2005) and the Stockholm Programme (2010), underline that response protocols are likely to be the same no matter the cause of the CBRNe event in question; what has been defined as the so-called all-hazards approach. 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. While recommendations concerning technological standardisation and procedural / institutional harmonisation at the EU level are transversal to these documents, some elements are more specific to the PROACTIVE domain. In this regard, the studied regulations and documents do explicitly suggest strategies that can be summarised in the following four dimensions (Table 4):

Table 4 Summary of requirements and recommendations integrated into legal documents and institutional reports related to PROACTIVE implementation

Dimension	Goal to be achieved	Instruments within PROACTIVE
General normative framework	• Respecting human rights attending vulnerable groups • Boosting collaboration and coordination between public agencies and NGOs	Both goals are in line with the PROACTIVE design.

Production of knowledge	• Conducting research in the CBRNe field and connect criminology and other scientifically based information to public action	PROACTIVE research is in line with this goal.
Dissemination and transference of knowledge to minimise impact of these events	• Fostering the dissemination of knowledge about CBRNe incidents among citizens using public campaigns or formal training. • Dissemination materials to be clear and adapted to different groups • Train first responders, policymakers and other authorities involved in CBRNe events using several methods	Besides the two first goals, training materials for the adoption of the PROACTIVE toolkits will have to be produced.
Policies for data management and instruments validation	• Developing practical and effective tools for practitioners, including research and awareness campaigns/training • Keep record of research and policy response findings • Design strategies for securing confidential knowledge on CBRNe events and weapons • Validation and testing of adopted tools, strategies and programs	PROACTIVE tools will be validated in WP6. Data protection recommendations will be introduced and tested in WP8.

Source: own elaboration.

3. ACCEPTABILITY AND ITS IMPLICATIONS FOR PROACTIVE

The PROACTIVE protocols and technologies must respect the legal frameworks described above. Moreover, the toolkits should also be dynamic in consideration of those social aspects that determine its effectiveness. These social and cultural dimensions also have an incidence regarding the relative adaptability of its tools to legal compliance. In this section, we will define social and political acceptability and examine the implementation of these concepts to PROACTIVE toolkits, including the acceptance of its technological solutions.

3.1. The concept of acceptability in PROACTIVE

Generally, acceptability has been defined as **the explicit or tacit collective support and public endorsement of a particular policy**, authority, measure or regulation. Along these lines, policy acceptability has been framed as an "evaluative judgement" concerning new technologies or policy initiatives (Huijts et al., 2012; Poortinga et al., 2004). As in other public fields, in the case of safety strategies, policy formation involves selecting one option among a set of alternatives. This process entails assessing several factors that go beyond the identification of actual policy problems (Kingdon, 1984). One of these factors is value acceptability in a specific community, which has been identified as an essential driver of policy design as well as a framework for policy implementation. Therefore, an in-depth and participatory analysis of stakeholder acceptability is crucial for ensuring the procedural legitimacy of public policies (Wallner, 2008).

The literature on public policies has identified a set of variables determining the degree of acceptability of a policy. Even though these variables are very case-specific and dependent on the policy field, four shared elements should be considered. Firstly, "**problem perception**" concerns how a particular issue in the public agenda is perceived by society and citizens (Valeri, 2014). This broad concept defines structural trends in the valuation of a certain policy, which is commonly addressed through public perception studies.

Secondly, the "**perceived effectiveness**" and efficiency of policy is commonly considered a key predictor for acceptability (Reynolds et al., 2019). In line with the above, the expected or known impact of individual policies determines public support to it and, at the same time, conditions its implementation. The expectations of users or citizens in terms of the effectiveness of a policy are fundamental in the forms of policy and technological adoptions, for instance, orientating voters decisions based on expected outcomes.

Thirdly, **knowledge** about the addressed policy and its possible alternatives is another critical driver of acceptability (Bell et al., 1990). The degree – and positive or negative orientation – of the knowledge handled by citizens about a policy determine how they frame it and perceived it. Regarding the public debate, this factor is thus a key driver for acceptability which is addressed through policies for redistributing cultural capital in formal democracies.

Fourthly, **social norms** have been presented as a framework determining the acceptance of policy that varies depending on cultural backgrounds (Douglas, 1985). Both the above-discussed perceptions and the approach to social norms have shown to be highly dependent on cultural grounds.

These factors have been grouped into the two dominant bases of policy acceptability: the **rational cost-benefit analysis** on the one hand and the **cultural backgrounds and values** on the other (Hansis, 1996). However, as pointed out by Beck (2000: 215), risks assessments are always based on a combination of both factual claims and value claims, which requires paying attention to contextual political and ethical factors influencing public perceptions.

From the public sphere and social standpoints, acceptability cannot be considered as a uniform perception of the policy, technology or phenomenon at hand. Instead, it should be taken into account that while hegemonic trends can be identified in society concerning the perception of governments or policies, it is also important to assume that several views about the same phenomenon do coexist

(Cohn; 2016). This fact has theoretical and methodological consequences since it involves looking at structural and agential cultural, economic conditions determining acceptability.

Broad societal acceptability is crucial for the successful development of public policy and the deployment of new technologies (Rolf et al., 2007). Both aspects are addressed in PROACTIVE from an approach oriented towards ensuring a certain level of procedural "harmonisation" and technological "standardisation" in the public response to CBRNe events. But its proposed protocols should also promote that specific conditions and the acceptability of certain social groups, including vulnerable people, are captured by its toolkit. The importance of the cultural dimension, therefore, is fundamental for PROACTIVE since the toolkit developed in the context of the project should be able to effectively capture the existence of several sociocultural contexts, where its guidance can be interpreted from different angles and in different dominant perspectives from citizens and practitioners.

3.1.1. Acceptance and acceptability of technology

The concepts of **acceptability and acceptance** have been widely used in the field of technology development. However, some conceptual clarifications should be made before moving forward. The literature has stressed that the concept of acceptability involves a priori understanding and assessment capability regarding a specific policy or technology. When it comes to technology, the **concept of acceptability** implies users' willingness to use it (Février, 2001: 16), based on the social representations or perceptions before adoption or testing (Barcenilla and Bastien, 2009; Tricot et al., 2003).

Instead, **technological acceptance** relates to the actual use of a system, namely the representations derived from this process. Therefore, this concept has often been framed as a post-assessment process derived from human-machine interaction (Février, 2011; Bobillier-Chaumon and Dubois, 2009). Along these lines, and following Tricot et al. (2003), our analysis will distinguish between technological acceptance and acceptability. While the first notion defines different drivers surrounding the actual use of technology, the second one can be defined as an aprioristic representation of this use. This subsection will focus on models of technological acceptance to be considered in PROACTIVE.

During the last decades, models for technology acceptability have been developed to frame different dimensions of users' experience and determine the main factors that influence technological adoption. These variables have been examined and categorised, focusing on those factors leading to efficient and positively-perceived technological adoption and implementation (Ash, 1997; Mathieson, 1991).

The **Technology Acceptance Model (TAM)** is a model for mapping factors favouring or harming the social and users' acceptability of technological solutions. This model is based on two explanatory variables for technological adoption (Davis, 1989). On the one hand, it considers how individuals perceive the potential enhancement of their activities or duties by using a specific technology, the so-called **perceived usefulness**. On the other hand, it focuses on how individuals believe that using this technology will help them to reduce their effort in the tasks or activities, or **ease of use**. As can be seen, these models evolved from the definition of the concept in the above-reflected political and sociological theory, reproducing many of its conceptual grounds.

Even though these elements are essential for the design and implementation of the PROACTIVE toolkits and Apps, we should go beyond such framework to capture other relevant variables. Along these lines, the so-called Unified Theory of Acceptance and Use of Technology (UTAUT) proposes a broader understanding of factors influencing the adoption and use of technologies (Venkatesh and Morris, 2003; Venkatesh et al., 2012). The UTAUT explains acceptability trough four main variables, including:

1. Performance expectancy (perceived usefulness): “degree to which an individual believes that using the system will help him or her to attain gains in job” (Venkatesh and Morris, 2003:447).

2. Effort expectancy (ease of use): “degree of ease associated with the use of the system” (Venkatesh and Morris, 2003:450).

3. Social influence: “degree to which an individual perceives that important others believe he or she should use the new system.” (Venkatesh and Morris, 2003:451).

4. Facilitating conditions: “degree to which an individual believes that an organisational and technical infrastructure exists to support use of the system.” (Venkatesh and Morris, 2003:453).

While the three first variables relate to the above-mentioned ease-of-use perception and its contextual grounds, the fourth refers to the specific technological functionalities and organisational aspects influencing technological adoption and implementation. Simultaneously, while the three first factors influence the user's behavioural intention, the fourth explains user behaviour from a functional standpoint. **Other societal elements have been considered within this theoretical framework**, such as gender equality or age factors.

As we can see, in all acceptability models, knowledge, including facts-based information, and its several interpretations and meanings, are essential in determining behaviour concerning a policy or technology. Considering the UTAUT approach, in the following section, we will analyse how acceptability and its main described factors are addressed in the CBRNe domain.

3.2. Social and political acceptability variables in the CBRNe domain

Instruments and policies to prevent and respond to CBRNe events and incidents are very **domain and case-specific** in terms of the drivers leading their acceptability. Still, beyond the concrete casuistic of each stage of CBRNe management and the type of incident at hand, there are some general implications to be considered. On the one hand, they involve addressing risks with many **social and political connotations**, such as the institutional management of confidential information or the potential stigmatisation of specific ethnic groups. On the other hand, **technologies used in this context** are often under public scrutiny due to their potentiality for misuse and other negative externalities concerning surveillance or false positives. In this section, we will frame these specificities based on the existing literature for developing our theoretical framework.

It should be noted that while it is possible to identify the below key dimensions of acceptability and general methodological considerations, there is **not an overall approach to this concept in the CBRNe field**. The diversity of threats addressed within this research domain and concrete social

conditions where they are tackled as well as the different purposes of response strategies do not allow generalisation, as reported in many research documents (Malich et al., 2016:650).

3.2.1. Main variables around CBRNe policies acceptability

In this section, we will identify the main elements framing the acceptability of CBRNE policies and technologies. The analysis will be based on a thorough literature review and Deliverable 1.3, "Guidelines and recommendations for mitigation and management of CBRNe terrorism", which summarizes the scientific literature and existing guidelines providing recommendations for effective policy and practice in the mitigation and management of CBRNe incidents (including terrorism). This synthesis is very relevant for framing best practices and main issues found in this field, and it is also very informative in terms of acceptability. This document also integrates the information about best practices and recommendations in this domain collected during a virtual focus group that took place with members of the PSAB conducted on the 12th of February 2020.

In terms of acceptability, there is a **significant difference between pieces of advice provided in the different studied documents concerning the protocol for CBRNe events response** (such as time, decontamination protocols). These discrepancies show a clear relation to national contexts, for instance, concerning their healthcare systems (Deliverable 13, 2019, p12). Along these lines, the management of acceptability in CBRNe scenarios has been based **on risk-based approaches**. Public presentation and the development of exercises of choices concerning identified threats can help communities make risk reduction choices taking their own knowledge and perception of informed options, as well as the frequency and characteristics of hazards, into account (Hales and Race, 2010). This approach requires testing the levels of vulnerability to different sort of CBRNe threats in order to identify the most suitable form of tackling the risk, addressing the capacity to address existing vulnerabilities and relevant cultural conditions (Public Safety Canada, 2017).

Taking the above case-specific dimensions into account, in the following subsections we will address the acceptability of CBRNe policies by considering four main acceptability drivers: public environment and media in CBRNe events, knowledge transference and training, cultural capital and perceived efficiency.

3.2.1.1. Public environment and media in CBRNe events

The public environment's importance in determining social understanding of bioterrorism threats and other CBRNE risks have been stressed. Along the same lines, the importance of **media events** surrounding these events is considered a critical driver of acceptability variables, such as trustable knowledge. Participation of affected groups is presented by the literature as an essential way of addressing possible gaps or distortions between policy to counteract these events and social perceptions (Mordini, 2004). It has also been recommended to involve these actors in exercises and create mechanisms to foster journalism ethics within these scenarios (Matthiessen-Guyader, 2004).

3.2.1.2. Knowledge transference and training as acceptability factors

In line with the legal and policy recommendations reviewed in previous sections, D1.3 also include references on the importance of increasing public understanding of CBRNe incidents by conducting training. Some authors have pointed out that social familiarity with CBRNe events and how to behave when they occur could be increased through systematic preparation (BESECU, 2011). Lack of clarity

in guidance is underlined as a significant limitation for an effective response by some authors (Bass, 2015; Wray, 2008). To gain acceptability, materials should be oriented and adapted to specific social groups, in terms of complexity and language (Nyaku, 2014: 36; Hellier, 2014).

Regarding style, the communication during the events should be precise and reliable, while it should show a certain level of empathy and concern around the event (Davidson et al., 2019; Reilly, 2016; Marret et al., 2017). Furthermore, it should be able to openly transmit uncertainty about unknown elements regarding the crisis or situation at stake (Reilly, 2016). Tactical and planned communication of authorities with communities based on clear and detailed information has been presented as fundamental for increasing both acceptability and resilience to CBRN events (Lucini, 2017).

Public campaigns to disseminate pre-incident information about CBRNe are more effective when transmitted through multiple platforms, and it should be coherent across them (Rubin, 2010). At the same time, it has been revealed that pre-incident information disseminated using written and specific communication may increase public acceptability (Wray, 2008; Rogers, 2013; Pearce, 2013).

3.2.1.3. Cultural capital and acceptability to CBRNe policies

A critical element for the successful implementation of response measures is the identified **under-education of the public regarding how to act during CBRNe events**, concerning aspects such as incident management strategies and shared understanding of existing guidance (Hall et al., 2019; Heath, 2016; Andrade-Rivas, 2015). Level of knowledge is a crucial driver for acceptability, which has also been related to the effectiveness of response strategies.

The literature has revealed that the public receives messages about how to react in the case of a CBRNe event in a more open way when they already have some knowledge about the phenomenon at hand (Perko, 2013). Efficient mechanisms to increase and improve knowledge about CBRNe events include TV campaigns, newspapers or the internet (Yoshida, 2016, Kanda 2014). These methods may lead to better adoption of preventative measures and also to a better response.

However, it has been underlined how the degree of engagement of individuals with informational resources conditions the access to this information (Andrade Rivas, 2015; Yoshida, 2016). Individuals' residence could also determine their knowledge about how to behave in case of a CBRNe event. This phenomenon could be explained by the frequency in which these events happen in some places (Perko, 2013; Wray, 2008). These last factors should be framed in terms of inequality since it is expected that individuals with more social and economic capitals could be better prepared for CBRNe events.

Moreover, strategies and protocols derived from empirical analysis and public engagement have also limitations. In this regard, it should also be considered that extensive knowledge has its limits in the context of CBRNe incidents since it can create conditions for dual-use and misuse (Wrightson, 2004). This so-called "security dilemma" should also be addressed by any policy to prevent or respond to CBRNe events.

3.2.1.4. Perceived efficiency of CBRNe policies and acceptability

Another essential factor around the acceptability of first response policies is the **perceived efficiency of existing policies and regulations** by both citizens and practitioners, as shown for

fire-fighters' activities on terrorism prevention in the USA (Heirston, 2010). The cognitive and agential dimensions of acceptability are essential in the field of CBRNe. The literature has addressed people perception of security and related reactions to risks and fear, which would favour more respect for preventative measures adopted (Heath et al., 2017, 2016; Andrade-Rivas, 2015). Response strategies to threats should take into account these widespread perceptions in order to capture the best ways of framing information and guidance.

Contextual and territorial factors such as the frequency of specific incidents are also essential to determine the adaptability of social groups to response strategies (Hales and Race, 2010). The resilience or capacity of a particular community of social system to restore an acceptable level of functioning after facing distresses or possible failures depends on many factors (Pinel, 2009). In the framework of preparedness to CBRNe events, "being prepared" also mean knowing and understanding that social factors can lead to failure in tackling threats. The capacity of resilience and adaptability of stakeholders must, therefore, been analyzed to ensure that response strategies are adequate (Hémond and Robert, 2012).

Concerning **response** to CBRNe emergencies, political acceptability has been considered a significant factor for decision making (Mustonen, 2018). While public acceptability of response strategies can influence in selecting one policy between different alternatives, also economic and other contextual factors are relevant. At the same time, such social acceptability should be considered from multidimensional and multicultural standpoints, as stated by Lucini (2017:85):

> *"The collective response and the nature of public resilience have become two important pillars in the face of terrorism threats. These two pillars are also directly linked to the principles of crisis management (above all, crisis communication), stressing the importance of knowing the cultural meanings and social understandings of the population at risk. This does not mean that professionals can completely control a situation, but they can limit the range and level of vulnerability."*

As already pointed out, resilience to the CBRNe events is also differential in cultural and socioeconomic terms (West 2013). This fact is reflected, for instance, reflected in different response national counterterrorism strategies (Government of Canada 2013). In PROACTIVE, this means that an essential effort of standardisation and harmonisation is needed to reach the right balance between specificity and efficiency.

Even though the main **methodological approaches to acceptability** in the CBRNe domain are in line with the above assumptions, many policies are only based on expert or policy-makers knowledge. Gaps between scientific-based data and projections and public opinion perception of threats can be very significant, as shown by Brown et al. (2018) when comparing Expert Assessment vs. Public Risk Perception on several threats, including Nuclear Emergency, Terrorism or food contamination or infection diseases. These findings stress the importance of both engaging communities and stakeholders in policy design and offering systematic, updated and extensive information about actual risks. For instance, some variables related to the acceptability of technologies addressing risk assessments in similar fields are the comprehensiveness of specific criteria, which requires a balance between simplicity and efficiency (Del Rio Vilas et al., 2013).

3.2.2. Knowledge and disinformation as acceptability drivers in CBRNe events

In line with the High Level Expert Group on Fake News and Online Disinformation of the EU Commission, we use disinformation to define **a series of forms of manipulated data among the ones fake news are the most known** (EU Commission, 2018). Fake news, a term coined in the last decade, was born as a form of public manipulation in Twitter based on bots diffusion (Akpan, 2016). Later, the concept of fake news integrated both misleading and false information created intentionally and disseminated through multiple sources (Allcott and Gentzkow, 2017). The manipulation of real events online and its replication by big media have gained increased attention in the last years since the impact of these practices has produced critical social disruptions. The other overlapping forms of false information only cover several typologies that have been classified in fabricated information, propaganda, conspiracy theories, hoaxes, biased or one-sided, rumours, clickbait and satire News (Zannettou et al., 2019).

In the field of crisis management, the extensive dissemination of fake news can significantly affect social dynamics, broadening panic and fostering problems in response (The Guardian, 2016). As we pointed out above, knowledge and the institutional and public arrangements to transmit it clearly and adequately are crucial for prevention and response strategies concerning CBRNe events. However, as addressed by the literature, intentional and unintentional distortions in disseminating information can significantly affect such aims. The production of fake news has accompanied terrorist attacks as part of the attackers' strategy (Al-khateeb and Agarwal, 2015), which has been framed under the concept of hybrid threats (NATO, 2010). Along these lines, the literature has addressed **how fake information online can negatively affect response to terrorist attacks** (Vosoughi et al., 2018; Starbird, 2013).

In this regard, one of the critical challenges in the age of digitalisation is **to monitor and limit the production and dissemination of fake news through social media in the context of crisis**. This phenomenon becomes even more critical if we consider that social media is increasingly being used for exchanging information in emergencies (Hughes and Palen, 2009). Different studies about the propagation of fake news and false information after a crisis, such as the 2010 earthquake in Chile or the Boston Marathon attacks, show that rumours present a different form of propagation online than confirmed news (Mendoza et al., 2010; Starbird et al. 2016). In the context of disaster situations, the hierarchy of tweets is shallower than in a normal state of affairs, indicating the organic replication of these data (Nadamoto et al., 2013). Gupta et al. (2013) revealed that out of the 32K accounts created during the 2013 Boston Marathon bombings, 19% of them were deleted or suspended after the event. The authors' analysis indicates that these accounts were created to disseminate false information. International organisations have been claiming strategies to counteract this phenomenon better.

Didactic **tools and strategies for distinguishing fake news and scientifically-based news** are therefore essential in this context for framing public acceptability of authorities' policies (BESECU, 2011). Differences between legitimate and fake news are often difficult to distinguish for users since fraudulent news use to derive from traditional news sources which are manipulated or have reproduced a piece of original fake information (Kumar, and G. Geethakumari,2014; Thompson,2017). The literature has identified some **key factors leading to significant acceptability of false news** and information:

- It has been determined that during a crisis, **users that are more distanced from the event, as well as anonymous users**, are more likely to share information that comes from fake or less credible sources (Thomson, 2012).

- Trust in the veracity of the information circulating on SNSs **depends on the individuals from whom the information is provided** (Zubiaga and Ji, 2014). The reputation and closeness of sharers are therefore crucial in framing acceptability to this news. However, it should be noted that factors as simple as the username of a tweet account can enhance the information provider's credibility (Morris et al., 2012).

- Close and robust online **networks in social media** can also be a factor leading to the reproduction of fake news, rumours or conspiracy theories (Zannettou et al., 2019).

- Simultaneously, having a diversity of dots in a user' network online, or a more significant social capital, can help provide different views about the same fact favouring more balanced judgment about misinformation and shaping acceptability (Kumar and Geethakumari, 2014). Exposure to social media may, therefore, also work in favour of better awareness.

In this framework, it has been suggested that public-private governance and dialogue should be established for blocking these activities during attacks (Dubey, 2018). The need for developing countermeasures to tackle these online terrorist practices, such as fake news detection and counter-narratives, has been stressed (Reuter et al., 2019). Concerning information management, public communication before and during the attacks should address this topic, by providing practical information about how to distinguish between fake news and CBRNe facts.

From the **technological perspective, emergencies and first response services still need systems to identify and remove fake news online** (Moi et al. 2015; Kaufhold et al., 2019). Different text analysis methods have been developed along these lines to determine the intervention of bots in the dissemination of fake news through social. Sentiment analysis can also be used to test the reaction of the public to social messages distributed in social media during crisis communication (Stieglitz, Bunker, et al. 2017). Zannettou et al. (2019) have identified several technological systems that successfully classify information online, supporting detection and containment of false information based on machine-learning techniques. They also found that false information can be contained by propagating accurate information and refute information through a well-established set of nodes. One of their main findings in this regard is that these mitigation processes require human-machine collaboration.

It is also highly recommendable for PROACTIVE to have a **regular and clear relation with the media**, since they play a central role both in the acceptance of a certain technology (Spicer, 2005) and for the communication of risks and uncertainties to the public, especially in situations of crisis and emergency (Pont Sorribes and Cortiñas Rovira, 2011).

3.3. Acceptability variables in PROACTIVE

For this report, we define the **acceptability of PROACTIVE to the general public and social conditions, driving more significant support and better adopting its guidelines, protocols and technologies**. An acceptability approach does not suppose a passive position of citizens and practitioners dealing with PROACTIVE but focus on the social and cultural preconditions for its

successful deployment. The PROACTIVE safety and acceptability framework should, therefore, be able to capture the elements leading to better protection and care of the public at times of vulnerability and enhance leadership in a time of crisis. It should be able to ensure that differential knowledge and cultural-based factors leading to more appropriate response and efficient and coordinated operations are identified and integrated into its tools. The PROACTIVE toolkits should also ensure a transparent and accountable system of emergency management, safe working and integrated mechanisms for promoting community resilience. In this section, we will address the main variables identified during the project development that may lead to these outcomes.

Acceptability is essential to ensure the correct adoption of standards and best practices proposed by the project. In this section, we will reflect the information collected during the Workshop[8] conducted online on 19th March 2020, where we identified those dimensions of acceptability that are relevant for the PROACTIVE toolkit design and successful implementation.

One of the aspects addressed by end-users during the meeting **is the forms of harmonisation to be potentially used in this domain**. This register was identified as a critical factor for many stakeholders involved in the project (participants 1,3,5[9]). One issue that concerns the acceptability of end-users is both the terminology and the actual design of harmonisation or standardisation protocols. Many participants in the workshop considered that "harmonisation is more related to standardisation when general recommendations are for dummy people" (1). Another participant (2) proposed to balance generalised procedures for multiple countries and actual harmonisation. Some experts understand that widespread procedures and organisation as well as communication, language and technical aspects should be grouped under the concept of harmonisation (1 and 2). Under these coordinates, harmonisation is essential for acceptability (3). Moreover, for many participants, while procedures are harmonised, technology is standardised. At the same time, technological standardisation has been distinguished from common operational procedures (COP) (4). **Harmonisation is therefore defined as the act of making different people, plans, situations, suitable for each other, or the result of this**.

In **methodological** terms, it was recommended to examine **best practices and conduct exercises** to establish common responses and reactions to these strategies (1). Generalised procedures could also be useful for emergency training and education (4). It was noted that current regulation and soft law in CBRNe allows for flexibility when developing these response strategies (15). This is in line with the analysis of legal texts and EU reports reflected in section 2.

However, policy development could find **limitations in establishing generalised procedures** taking into account differential social scenarios and factors (4) as well as legal aspects (3). Other barriers would be different forms of intervention and approaches of various agencies as well as human and material resources, training or competencies (5, 6). Best practice to guide policy could be developed but harmonised (standardised) procedures in a specific method would be difficult (11).

[8] The minutes of the meeting “PROACTIVE 3rd Progress Meeting (PM3), 2nd General Assembly (GA 2), 2nd Executive Board (EB), 17 - 18 March 2020, Online Meeting, Zoom” are reflected in WP9/Task9.1/PM3/V2

[9] Numbers correspond to anonymised participants.

It has also been pointed out that (participant 3) that **communication and social networks** are critical for an effective international response, so it is vital to have communication channels to ensure this. Communication is seen as needed at the EU level (3). However, it has also been indicated that for developing common strategies, the official restriction of info in a CBRNe incident should be considered (5, 3). Lessons learned from other fields such as defence or military have been framed as possible (3).

In terms of the differential **sociocultural aspects determining acceptability within preparedness and response actions**, situational awareness, self-awareness and cultural awareness are seen as crucial factors in understanding the incidents (3). Moreover, cultural and religious aspects are essential for communication with the population and between agencies (1), mostly for communication (6). Religion and values of stakeholders have been underlined in this framework. Instead, for the actual incidents, this has not been considered very relevant (6), except for decontamination, where religion can play a role concerning the management of clothes (7, 8, 10, 1, 4, 11, 6, 1). Still, it was stressed that necessary information should be available for other languages (available in the city, region) (6), which is crucial from the acceptability standpoint (a local, national and supranational criteria should be established for this). For instance, Turkish was seen as key in Germany. It is also recommended to disseminate guidelines and Information using visual media (2) such as pictograms for persons with communication problems. Lastly, minorities and disadvantaged groups such as homeless or disabled were also mentioned in this regard (9).

Concerning **knowledge**, it was stated that nowadays people could find information quickly (e.g., on the Internet). Although many experts pointed out that not all the information circulating online are correct, it was also said that the public is not scientifically ignorant (1). In this framework, some points concerning communication that are relevant concerning the acceptability of PROACTIVE were pointed out:

- It was mentioned that **institutional reputation and legitimacy** should be a ground for providing a trustable and reliable understanding of situations. Official sources, quick communication and credibility are seen as crucial tools for fighting fake news (1, 5).

- For some participants, COVID-19 has demonstrated that civil society is very dependent on **social media** and looking for short guidelines online. In COVID-19, it took time to set up this channel of communication (4).

- At the same time, it was pointed out that "**fake news" are a challenge** for the management of communication, which should be addressed with specific strategies (5). There is a growing exchange of non-scientifically backed information from non-credible resources. To tackle this, experts propose to foster authorities to release understandable but evidence-based information.

- Concerning media, it was mentioned that the Internet might not be available everywhere during the incident and that the digital gap should be considered. So, elderly people and other non-IT skilled people must be taken into account for risk communication. **Having a hard copy of instructions** is still necessary (4, 16).

- Thus, communication with particular groups of victims (e.g., disabled) is seen as a challenge (6). **Notifications to the civil society must always be "multichannel"** to reach people from

traditional means of communication to social networks (1) and counteract fake news. So, it should be adequate to the variety of audience (teenagers, senior citizens), technical resources (possibility or capability to access or use) and to the level of use of them (TICs) (5).

It was also mentioned that other **media or technologies** could support didactic strategies needed to ensure that all social groups access the right information in a plural and effective manner. Proposals include the Internet of Things or games to produce simulations of scenarios or instructions about how to proceed after the event (14). In the same line, it was underlined that risk awareness should be embedded in national education systems, which could address CBRNe in didactic and pedagogical ways, such as games (3, 2, 1). The approach could be similar to first aid/fire/earthquake exercises taking place in all education levels. According to some experts, this could help to improve the relationship between practitioners and citizens during the incident. Training should also be provided to decision-makers, including politicians in charge of tackling these events (4, 17).

These **informative mechanisms** could reduce public panic during the incident (2). However, it was also said that correct information does not imply that people will react predictably during the event. Instructions should be provided in a practical manner, such as involving action or simulations (1) to tackle this phenomenon and ensure self-protection.

3.3.1. Acceptability of PROACTIVE technologies

As detailed in section 2, PROACTIVE will deliver two types of technologies aimed at guiding to improve crisis communication for enhanced early warning, situational awareness and better response coordination during CBRNe incidents. A Web-Based Platform with iOS and Android Apps will be developed, which will include a shared functionality for LEAs and Citizens (for a description of these solutions, see section 2.2.5). In this section, we will frame the acceptability of these technologies under an extended technology acceptance model.

The literature has described an increasing technology adoption in the field of crisis information and management during the last decades (Kim et al., 2012). On the one hand, technology is framed as a way to address many of the existing gaps in response to disasters, such as poor communication and lack of quality data about the events (Dorasamy and Raman, 2011). On the other hand, the adoption of technological solutions for ensuring fast response and addressing potential consequences of human or natural disasters, such as the need for social distancing, have been recommended after the 2001 US attacks (Locke et al., 2004). Along these lines, it has been suggested that technological solutions used in CBRNe related crisis should be targeted to local/community level and must communicate based on the community needs. Trustability of the messenger has also been stressed as an acceptability factor. Lastly, a multipronged strategy, including multiple technologies, has been proposed (Locke et al., 2004: 10).

In this context, security apps have specific security and ethics challenges but also acceptability implications. As discussed by Kolliarakis (2017), the development and implementation of digital solutions in CBRNe and related domains should be based on a proportionality assessment. This assessment has implications for the public legitimacy of security policies since not anticipating possible negative externalities of preparedness and response ICT tools can lead to widening the gap between citizens and public authorities. These negative externalities include privacy breaches, the production of false negatives or the unexpected propagation of disinformation.

PROACTIVE addresses these issues by design since it involves specific mechanisms for enhancing data quality to be exchanged before and during the events and targets vulnerable populations in the development of the tools. These aspects are also addressed through specific Ethics WP and the intervention of Civil and Society Advisory Boards. It also includes different tasks aimed at embedding Privacy by Design (PbD) approaches and solutions in the project approach, ensuring the adoption of security measures such as data minimisation, anonymisation or encryption.

To provide a preliminary understanding of the acceptability implication of PROACTIVE technologies is relevant to identify their role concerning the communication between the stakeholders involved in the CBRNe domain. Based on the UTAUT approach, the characteristics and functionalities of these technologies present the following acceptability implications (Table 5):

Table 5 Framing of technology acceptance criteria regarding the PROACTIVE platform for LEAs and policymakers

Technology acceptance variable	Definition: variable applied to the platform use by LEAs and policymakers	Drivers for increasing the PROACTIVE platform acceptance
Performance expectancy	• would improve my understanding of the CBRNe incident at stake • would increase my chances of achieving better preparedness and response coordination • would allow me to accomplish CBRNe tasks more quickly • would enhance the effectiveness of preparedness and response actions	❑ Scientifically-based guidance must be provided for each preparedness/response scenario at stake ❑ Scientifically-based and updated information and sources about CBRNe incidents must be offered ❑ Information tailored to local sources ❑ Information should contain facts or proof to provide robustness
Effort expectancy	• would provide a clear and intelligible overview of the crisis scenario • would offer concrete and targeted functionalities for easily collecting and sharing information	❑ Manageable maps with location of events ❑ Navigation should be meaningful with large and clear sections for each function ❑ Content adapted to each user: LEAs/policymakers ❑ Appropriate feedback from web components ❑ Multiple languages available ❑ Information must be easily edited and uploaded/downloaded ❑ Branding should be intelligible
Social influence	• would better engage with other first response	❑ Visualisation and communication methods should be inclusive in terms of gender,

Technology acceptance variable	Definition: variable applied to the platform use by LEAs and policymakers	Drivers for increasing the PROACTIVE platform acceptance
	agencies and authorities • would increase public acceptance and knowledge of LEAs task during CBRNe events	disability and age ❑ High quality in terms of harmonisation, clarity, guidance and adaptability concerning how to manage vulnerable citizens ❑ Information should be delivered to the public using multiple sources ❑ Communication should focus on ensuring the protection of the public's health ❑ Communication should aim to influence the perceived efficacy of recommended behaviours ❑ Information should incorporate factual proof and use a credible spokesperson ❑ Limit material and information provided to prevent the possibility in provoking worry ❑ Limitations to the uploading and accessing to pre-incident, real-time and post-incident must be made explicit
Facilitating conditions	• competent authorities would acquire the software • training and organisational aspects will be established • the adoption will fit existing legal and political frameworks • technical capabilities are available and fit the purpose of the systems	❑ Provide corresponding manuals and training materials

Source: own elaboration.

The PROACTIVE technological toolkits must be understood as a whole since it integrates three systems to be articulated under the same goals, which share most of the collected information. However, both the platform and the Apps for LEAs and policymakers must be framed from the angle of the competent authorities. This perspective means that the acceptability must be assessed by considering the view of the end-users about the effectiveness and efficiency of the system. The analysis should also consider the position of this technological policy within the potential socio-political setting where it will be implemented; the so-called social influence and facilitating conditions.

As we can see in Table 5, the main acceptability challenges for the platform relate to its capacity to work as a communication space able to organise and articulate relevant information among stakeholders. However, at the social level, the system should also be able to ensure high transparency and security, so it is privacy compliant and welcomed by the public in these terms. It should be noted that collecting sensitive information in the public space by Law Enforcement agencies and public authorities could harm the social influence of technology if these measures are not taken into consideration. Lastly, it is essential to provide clear guidelines about how to use these technologies.

As with the Web platform, the App's acceptability (Table 6) is framed by its capacity to make preparedness and response to CBRNe incidents more informed, fast and coordinated. Both practical and perceived dimensions of efficiency must be tackled by adequately explaining the aims and characteristics of the system to the public. Moreover, the App for LEAs and policymakers entails the development of well-established governance and security mechanisms for data processing. Along these lines, besides providing training tools for users, measures for minimising risks of data breaches that may harm the acceptability of the system should consider the additional risks posed by mobile solutions. Mobile devices could get lost or reached by individuals looking to misuse their information.

Table 6 Framing of technology acceptance criteria regarding the PROACTIVE App for LEAs and policymakers

Technology acceptance variable	Definition: variable applied to the App use by LEAs and policymakers	Drivers for increasing the PROACTIVE App for LEAs and policymakers
Performance expectancy	• would improve my understanding of the CBRNe incident at stake • would increase my chances of achieving better preparedness and response coordination • would allow me to accomplish CBRNe tasks more quickly • would enhance the effectiveness of preparedness and response actions	❑ Scientifically-based guidance must be provided for each preparedness/response scenario at stake ❑ Scientifically-based and updated information and sources about CBRNe incidents must be offered ❑ Information tailored to local sources ❑ Information should contain facts or proof to provide robustness
Effort expectancy	• would provide a clear and intelligible overview of the crisis scenario • would offer concrete and targeted functionalities for easily collecting and sharing information	❑ Manageable maps with location of events ❑ Navigation should be meaningful with large and clear sections for each function ❑ Content adapted to each user: LEAs/policymakers ❑ Multiple languages available ❑ Information must be easily edited and

Technology acceptance variable	Definition: variable applied to the App use by LEAs and policymakers	Drivers for increasing the PROACTIVE App for LEAs and policymakers
		uploaded/downloaded ❏ Branding should be intelligible
Social influence	• would better engage with other first response agencies and authorities • would more directly connect to citizens • would help to increase public acceptance and knowledge of LEAs task during CBRNe events	❏ Visualisation and communication methods should be inclusive in terms of gender, disability and age ❏ High quality in terms of harmonisation, clarity, guidance and adaptability concerning how to manage vulnerable citizens ❏ Information should be delivered to the public using multiple sources ❏ Communication should focus on ensuring the protection of the public's health ❏ Communication should aim to influence the perceived efficacy of recommended behaviours ❏ Integrate security mechanisms of avoiding unauthorised access to pre-incident, real-time and post-incident information
Facilitating conditions	• competent authorities would acquire the software • training and organisational aspects will be established • the adoption will fit existing legal and political frameworks • technical capabilities are available and fit the purpose of the systems	❏ Explain to the public the functionalities and goals of the app ❏ Describe security conditions and restrictions to the processing of personal data ❏ Information about the use of location data and its implications should be made public ❏ Explain security conditions for ensuring the integrity of personal information stored in mobile phones ❏ Provide corresponding manuals and training materials

Source: own elaboration.

In Table 7, the acceptability of the App for vulnerable groups entails many challenges. Firstly, the capacity of the App to provide highly interactive communication between users, other users and authorities, is highly dependent on the ability of the system to be targeted to each user group. Secondly, the App a double-layer approach, where both related cultural aspects and the specificities of each addressed vulnerability should be taken in its design. User-independent layout and functionalities for each targeted group should be designed and tested. Notifying users about the

features or training tasks would be an appropriate form of ensuring human-machine interaction and meaningfulness of the App in line with the findings of Torbjørnsen (2019).

Table 7 Framing of technology acceptance criteria regarding the PROACTIVE App for vulnerable groups

Technology acceptance variable	Definition: variable applied to the App use by citizens	Drivers for increasing the PROACTIVE App for citizens
Performance expectancy	• would allow me (citizens and, in particular, vulnerable groups) to better prepare and respond to a CBRNe incident • would facilitate my training and provide accurate/updated information on CBRNe issues and events • would foster communication capabilities (among vulnerable groups) in case of a CBRNe event	❑ Communication should aim to influence the perceived efficacy of recommended behaviours ❑ The system should allow for a certain level of interaction between users and public authorities ❑ Information should be tailored to local communities and their respective relevant groups ❑ Information should contain facts or proof to provide robustness ❑ A trusted spokesperson should disseminate communication
Effort expectancy	• would provide a clear and intelligible overview of the crisis scenario • would offer concrete and engaging functionalities for easily collecting and sharing information • would foster communication in the case of vulnerable groups, including the elderly and children and also those with the following disabilities: deafness, blindness, intellectual disability, autism, epilepsy, post-traumatic stress disorder, and	❑ Information should be culturally appropriate (system adaptable to local backgrounds), easy to understand, and non-complex allowing the information to be accessible for all- Multiple languages should be available and will be the responsibility of the LEA ❑ Include independent user-functionalities such as hearing amplifier (deaf people), address feelings (feeling scale) for autistic people, a voice assistant for blind people (Be My Eyes model), maps for people with disability (Wheelmate model), or text-to-speech aspect for people with difficulties for reading ❑ Design for colour blindness, captions and alternative text, avoid features that frequently flashes on the screen (epilepsy) ❑ Incorporate novelty in the dissemination of information (e.g., using a cartoon character) ❑ Each layer of shared data should be differentiated (location, images, videos)

Technology acceptance variable	Definition: variable applied to the App use by citizens	Drivers for increasing the PROACTIVE App for citizens
	schizophrenia	❑ Include a limited but specific number of meaningful notifications for tasks related to CBRNe preparedness
Social influence	• would better engage with other citizens and support them before and after a CBRNe event • would help to visualise vulnerable groups needs at the social level • would better articulate support of non-vulnerable citizens to vulnerable citizens before and during CBRNe events	❑ Information should meet the needs of the intended audience ❑ Visualisation and communication methods should be inclusive in terms gender, disability and age ❑ High quality in terms of harmonisation, clarity, guidance and adaptability concerning how to manage vulnerable citizens ❑ Monitor the ethical grounds and examine the possible social impact of entertainment offered (e.g., topic of games, addiction to video games). ❑ Limit material to prevent the possibility in provoking worry ❑ Consequences of reporting CBRNe events should be clearly and fully explained ❑ The privacy policy and consent form materials should explain the processing and securing of sensitive data
Facilitating conditions	• open source software could foster access • open Manual for the app • public support for training vulnerable groups in how to use the app • public promotion of the app, its aims and functionalities	❑ Integrate functionalities for easy downloading and installing the app ❑ Integrate mechanisms for ensuring consent/assent of targeted groups ❑ Describe security conditions for ensuring the integrity of personal information stored in mobile phones and restrictions to the processing of personal data in an adapted/friendly manner ❑ Provide corresponding and adapted manuals and training materials

Source: own elaboration.

Lastly, concerning social influence and other facilitating conditions, the importance of providing **highly transparent information about the aims, characteristics and methods of the App** in the context of its related systems (web platform and LEAs app) should be publicly available and published by the authorities. It should be considered that before an incident, authorities may be collecting highly sensitive information of vulnerable groups, which must be assessed from

proportionality and security standpoints. To ensure this, also targeted training material should be provided.

4. LEGAL AND ETHICAL BASED RECOMMENDATIONS

In this section, we will summarise the legal recommendations for the PROACTIVE consortium about the design and implementation of its guidelines and technologies. Based on the above analysis, we will focus on some aspects to be considered during the toolkit's development and implementation.

4.1. Data management within the toolkit and PROACTIVE technologies

As we saw in section 2, the PROACTIVE toolkits will, in any case, strive for protecting the fundamental rights to privacy and personal data protection, concerning the general wellbeing of vulnerable populations as reflected in the Charter of Fundamental Rights of the European Union. However, even though PROACTIVE toolkits have many externalities and implications concerning the rights to integrity and liberty of users, the focus of our analysis regarding legal compliance is on its -more direct- impact over the right to privacy. In this regard, both the set of guidelines to be produced as part of the project and the PROACTIVE technologies are mainly aimed at facilitating knowledge production, standardisation and spreading. In this framework, most of the rights to be directly assessed in its framework are bound to data protection.

In Table 8, we summarise the requirements to be achieved in PROACTIVE and its implementation for each of the dimensions addressed in section 2.

Table 8 Summary of data protection requirements and recommendations

Variable	Requirement in PROACTIVE	Observations for implementation
Data governance	• Identify the **data controller and processors** and frame their responsibilities**, ensuring that functionalities and the adoption of technology are fully in line with the proposed governance.** • Establish the framework for the definition of a **DPO** within PROACTIVE best practices.	• Measures for ensuring the active role of data controllers in the definition and monitoring of technical and managerial protocols for data protection should be considered. • Controllers and processors should document their corresponding processing activities concerning personal data.
Legal basis for the processing	• Set the conceptual framework for defining the **legal basis for personal data processing** in the context of the protocols and strategies proposed by the	• While informed consent is expected to be the primary basis for personal data collection the within preparedness activities, other legal grounds such as the

Variable	Requirement in PROACTIVE	Observations for implementation
	PROACTIVE toolkit.	LED, or public or vital interest within the GDPR, could be also the basis for some response actions established by the toolkit.
Data management	• Apply **data minimisation** to data collection within both the PROACTIVE guidelines and its communication strategies. The latest is being achieved by integrating PbD in the technical requirements of the App.	• It is recommended to develop a template with the minimum personal data needed for achieving the PROACTIVE recommended protocols for prevention, preparedness, response and recovery activities.
	• Produce protocols and tools for **securing the integrity and confidentiality** of personal data.	• **Data breaches**: establish security mechanisms, tools and protocols such as data pseudonymisation, anonymisation and encryption, to avoid data breaches. Establish a protocol for notifying breaches to both users and supervisory authorities within a maximum of 72hs after an incident. • Special care must be taken with PDF, audios, videos and other files shared using the Apps/Web, since the systems may not be able to identify that they contain PII, and therefore complying with a request for content or deletion may be difficult -or impossible-. • Embed data security measures suggested in the GDPR such as access control and password protection in the PROACTIVE toolkit. • **Monitor and prevent algorithmic bias and discrimination**, as well as possible false positives/negatives, in particular those related to protected attributes. • Develop tools and protocols for removing personal data, once they are not needed for primary uses.

Variable	Requirement in PROACTIVE	Observations for implementation
	• The PROACTIVE toolkit, which will have a strong focus on communication, will have to integrated protocols for **explicability and accountability** concerning the management of personal and sensitive data in the context of CBRNe events. All data processing activities involving personal data must be documented. • Follow harmonised and European criteria for applying the obligation of **informed consent for vulnerable groups**. Furthermore, strategies and tools targeted to vulnerable groups will guarantee both information and consent, when applicable.	• Establish and communicate a proportional data retention period for all data collected as part of the PROACTIVE toolkit. • Develop a PROACTIVE template on the processing of personal data before, during and after a CBRNe incident. It will be provided to citizens and end-users. • Evaluate the need for conducting a DPIA.
Data protection rights	Establish mechanisms, managerial protocols and the technical capabilities within the PROACTIVE toolkit to guarantee: • The collected **personal information is available and accessible for data subjects** before and after an incident. • Data provided or obtained from citizens and first responders **can be rectified when this depends on the controllers**. • **Erasure of data subjects' data** can be conducted appropriately when these data is no longer needed for pursuing the aims for which they were collected. PROACTIVE should distinguish between data to be used to prevent or tackle incidents and those data related to criminal offences in the context of CBRNe incidents. • Users can **restrict the processing**	• Develop tools and protocols for examining the accuracy, quality and veracity of personal data used in CBRNe incidents.

Variable	Requirement in PROACTIVE	Observations for implementation
	of personal data when the data subject questions their accuracy or the data is no longer needed for aims of the processing. • **Ensure systematic formatting of personal data** so it can be accessible and shareable by data subjects when needed and can adequately request the objection or rectification of its processing. • **Rectifying and erasing personal data**.	
	• **Ensure data quality and accuracy**	• Integrate an algorithm for filtering misinformation and minimise false positive rates. • In case an algorithm is used it should be audited so as to effectively comply with the protection of personal data.

Source: own elaboration.

As shown in Table 8, the adoption of a data protection approach in PROACTIVE has two dimensions. On the one hand, it relates to the **integration of data protection principles reflected in the GDPR into the set of guidelines to be produced by the project**. The project should, therefore, be able to develop strategies aimed at ensuring the integrity of personal data within the processes of preparedness and response to a CBRNe event. These mechanisms involve producing recommendations and protocols for gathering, processing and removing personal data. This should be considered as an added value to the toolkit. On the other hand, the **PROACTIVE derived materials should adopt a privacy by design and by default approach** (Art 25 GDPR), ensuring that once the guidelines and technologies have been made available to end-users and citizens, the strictest privacy settings will be applied, without any manual input from the LEAs or policymakers.

In this regard, the instructions for the application of PROACTIVE must include recommendations and guidelines about how to establish a data governance process aligned with data protection law. The toolkit should provide references for clearly framing the responsibility of each actor in case of a CBRNe incident. In particular, the figures of the controller, processor and DPO.

Secondly, taking into account that sensitive data will be processed, a set of security standards must be respected:

a) It is recommended to develop a set of **templates on data protection as part of the materials to be integrated into the toolkits**. These should establish a standard criterion for personal data processing, identifying **potential and minimum categories of personal and sensitive data involved**. Moreover, it should include a

clear reference to the data retention period, when applicable. This document should be provided to both end-users and citizens interacting with the toolkit during the preparedness phase. Most of this information should be reflected in the Privacy Policy and the consent of the Apps for both LEAs/policymakers and vulnerable groups. **Standard criteria for consent** should take into consideration the requirements included in the GDPR (Article 7, Recitals 32, 42): consent must be freely given, unambiguous, informed, specific (concerning the aim and the characteristics of the processing) and it can be revoked at any time[10].It is also recommended to **map the anonymisation points** along the personal data-lifecycle, including procedures conducted before and after the events (such as pre-incident training sessions or post-incident data management). The criteria for the design of this map should be reducing the amount of personal data to be processed based on a proportionality assessment that should take into account the effectiveness of the tools/protocols at hand. When the identity of users or citizens must be kept under a legal basis and with legitimate purposes, such as public interest, law enforcement or under the LED, **pseudonymisation may be applied as a security strategy**. Pseudonymisation means separating the direct identifiers from the data, while the data utility remains the same. It is still personal data (under the GDPR) but adds an extra security layer.

b) Protocols should be established -and embedded in the Web/Apps- for **monitoring data quality**. The analysis of data sources, maintenance of equipment as well as checks of accessibility and portability of data should be translated into specific recommendations in PROACTIVE. Some of these protocols should also be standardised through the development of specific functionalities within PROACTIVE technologies. Tools for filtering data sources, algorithms for filtering illegal information and notifications for the removal of dispensable information should be integrated.

c) One of the most important protocols to be established for PROACTIVE is the one concerning **data breaches**. 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: "*a) Nature, sensitivity, and categories of personal data affected; b) Legible/illegible data; c) Volume of personal data; d) Ease of identifying individuals; e) Severity of the consequences for individuals; f) Individuals with special characteristics; g) Number of individuals affected; h) Data controllers with special characteristics (the entity itself); i) Profile of the users affected; j) Number and classification of the systems affected; k) 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*". When a breach is identified under these criteria, supervisory authorities must be notified within a maximum of 72hs. Law Enforcement non-involved in the management of the system must be informed in the

[10] See Deliverable 8.1 for further information.

event of a crime. Lastly, all directly affected data subjects must also be informed without undue delay.

d) Protocols for data protection in PROACTIVE should include **dynamic forms of securing data,** such as end-to-end encryption and secure logging policy, as well as on-going forms for monitoring compliance of security standards. This includes evaluating the need for the development of Data Protection Impact Assessment as mandated in Article 35.1 GDPR in those cases that should pose a high risk for individuals' rights to privacy and personal data protection.

e) In line with the PROACTIVE privacy policy, specific protocols for **ensuring the rights of users** should be integrated into the toolkit. Following a scheme as proposed in Annex 1, users (data subjects) must be able to request the access, rectification, objection, cancellation, portability and removal of their data. Upon receiving one of these requests from a PROACTIVE user -sent to the email of the DPO included in the Privacy Policy-, the request should be passed to the data controller. The identity of the data subject submitting the access request is therefore confirmed by the controller team, by matching data provided by the user within the request template to biographic data stored in the system. Protocols for ensuring that these procedures can be properly conducted once the identity of the claimer is confirmed, and its claim is deemed legitimate, should be established. These protocols involve many actors, such as the technical staff of the organisation administering the database, the legal staff in charge of the claim verification. The information provided to users must be structured in a concise, explicit language, as well as in a comprehensible and effortlessly manageable format.

4.1.1. Data breaches prevention and response strategies: results from a tabletop exercise

One of the most important protocols to be established for PROACTIVE concerns **data breaches due to their potential impact on users and citizens' privacy and integrity**. Following this rationale, on March 4th, 2021, the PROACTIVE consortium conducted a Tabletop exercise specifically oriented towards identifying preparedness and response tools, strategies and protocols when using the current version of the PROACTIVE technologies. The discussed scenario consisted of the data breach situation in Figure 1.

As a **background for the scenario**, participants were informed that: the Rieti police oversee PROACTIVE in the city and are its data controller. PROACTIVE data is not shared with other LEAs. Rieti is a town from comune in Lazio, central Italy, with a population of 47,700. The town has recently experienced events related to parcel bombs. The Rieti Polizia di Stato, managed at the provincial level by the Rieti Questore, has implemented the PROACTIVE system to monitor railways, bridges, and waterways. Social organisations representing vulnerable populations in Rieti city have promoted the mobile app's use among their members.

- 9 am morning, Rieti train station. Data is collected by passengers using the PROACTIVE mobile app during an apparent emergency on the station when the train stops after hearing an explosion.
- These data, including pictures and videos of people identified as migrants and terrorists by PROACTIVE users, are shared through the app by two passengers. PROACTIVE managers authorize this information, so it is stored in the system and circulated among other Polizia di Stato units, but not with the public.
- Later that day (1 pm), the incident is clarified as a false alarm due to a gas leak and solved by firefighters. Still, images shared trough PROACTIVE are found in social media and reproduced by media outlets tagging recorded individuals as criminals.

Figure 1 Data Breach Scenario used in the PROACTIVE Table Top Exercise

The **following two injects** were used to discuss informational and physical leaks:

i. On-site, units are aware of data subjects being tagged as terrorists online. They are also informed that a Rieti Police Officer's device has been reported as stolen during the morning after the incident (11:00 am).

ii. A false alarm is confirmed. The Rieti Police Officer's mobile phone is found. However, access to the PROACTIVE system using official credentials, but from an unknown location, is identified during the system logs analysis (1 pm).

Based on this, the following aspects were discussed:

- Unauthorised access-attacks or non-intentional breaches, which might be partial or complete. Possible psychical access and/or informational violations. This could potentially have other implications, such as false positives, discrimination and/or misinformation. Other aspects included source identification and mitigation, technical (i.e., automatic alerts) and operational capacities (i.e., identification) response mechanisms.

- The management and mitigation of these issues, technical and operational response scenarios, including automated and human filtering, were addressed.

Participants underlined that, in these conditions, the **exchange of personal information into social media** could affect people falsely identified as terrorists. In the UK, this case would be reported to the Information Commissioners Office. There might also be criminal charges against the person who released the information. Moreover, the LEA would need to issue a statement about the publication of false data. It would need to provide protection for the individuals and talk to the media platforms about taking the information down.

According to one of the participants, it is challenging to prevent a **widespread circulation of false information** if a platform is being used to disseminate information about an incident. LEAs need to be aware of these problems and ensure regular press briefings to counter false information.

Legal and ethical experts stressed that, under these circumstances, data protection law would require **LEAs using the tool to communicate the breach to their supervisory authority and the data subjects (the citizens) under certain circumstances**. When a breach is identified under certain criteria, supervisory authorities must be notified within a maximum of 72hs. 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[11]. Moreover, law Enforcement non-involved in the management of the system must be informed in the event of a crime. All directly affected data subjects must also be informed without undue delay.

Different LEAS underlined that existing institutional mechanisms for ensuring the correct use of personal data mostly consist of severing disciplinary measures for those officers misusing personal data. However, **no specific training on how to deal with data breaches was mentioned**.

Preparedness strategies mentioned by first responders included:

- **Training** on management of data leaks for all end-users, including the system managers. This training should address aspects including informational risks, such as possible attacks and physical problems, such as precautions to be taken in case of lost devices;

- A tool within the App to **rapidly report leaks to users**;

- A mechanism for the **rapid assessment of the protocol to be followed in case of data leaks** could be included in the system Manual or integrated into it. It should categorise high and low risks events according to the type and amount of leaked personal data. According to

[11] These criteria are the following: "a) Nature, sensitivity, and categories of personal data affected; b) Legible/illegible data; c) Volume of personal data; d) Ease of identifying individuals; e) Severity of the consequences for individuals; f) Individuals with special characteristics; g) Number of individuals affected; h) Data controllers with special characteristics (the entity itself); i) Profile of the users affected; j) Number and classification of the systems affected; k) 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 experts, this assessment should accurately identify the likelihood of the breach resulting in a risk to citizens' rights and freedoms. For example:

- Low risk = it's leaked that an anonymous user reports an event at a certain location;
- High risk = the name, address, phone details and pictures taken of an identifiable person are leaked.

Proposed response strategies included:

- Try and track the **source of the leak**. This could include using technology to try and trace stolen devices in case of physical privacy breaches;
- Put out a **statement to counter the false information**;
- **Speak to the media** to counter the information;
- **Provide protection** to the people falsely identified.

To ensure prompt identification of the data breach, units on-site will need information about its potential source from the system managers and then switch off the false data source. In this regard, different options for using PROACTIVE collaborative web and Apps to identify the source of the data were proposed. Fast time information about the data breach and data subjects involved is crucial for effective response. As system managers should be able to rapidly establish whether the case is about human error, misuse or an intentional attack, participants pointed out that the PROACTIVE system could:

- Include a **system to catalogue received information according to the source in some way**;
- Use specific **tools and protocols for mapping and registering logs to the system** to be integrated into the platform;
- Establish **data breach communication protocols** for a) data subjects involved, b) supervisor authorities, c) media. This should be adapted to each type of scenario.

Along these lines, it was mentioned that it is indeed important that the tool has the functionality **to preserve the leak's circumstances**, as preservation is a key aspect of digital forensics. Ideally, there would exist the possibility of "freezing" a snapshot of the system over a certain period once a data breach is identified. In this way, nothing is lost, overwritten or potentially deleted that could be used to identify the culprit or understand how the breach happened.

4.1.2. The PROACTIVE technologies requirements

Table 9 summarizes the preliminary strategies established for the implementation of data protection principles and requirements detailed in section 2 within the three above-described technological solutions.

Table 9 Data protection principles and implementation in PROACTIVE technologies

Data protection principles	Established data protection requirement(s)	Concrete indicators for compliance[12]
Data governance	The scheme of decision rights and accountabilities for personal data-related processes. Who, how and with under which specific conditions can manage personal data.	• Admin and user(s) of the platform should clearly differentiate the functionality and security/access conditions: (admin) and processors (users). • Legal competences of each participant authority (LEAs and policymakers) should be in line with access control. In this regard, given the sensitive character of the system, in the case of criminal information, LEAs should be the controllers of the system. • Pre-incident information should be delivered by a credible spokesperson.
Informed consent	*"Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* (Article 4(11), GDPR).	• Users of the Platform must read and verify (tick a box) a Privacy Policy, regarding data protection measures and rights, access to personal data, consent form and disclaimer electronically before they can access the system. • Every service user will be explicitly told, in advance, what PII will be gathered and what, specifically, it will be used for. • List the data points used by the App and reflect this list of in the Privacy Policy (all categories should be mentioned). • All personal data managed by the systems, their use and the data subjects rights will be thoroughly explained. • Assent mechanisms should be ensured for those who are not able to provide consent. Ensure consent of persons in charge of vulnerable individuals who are no allowed or able to provide consent (minors, etc.).
Purpose limitation and data minimisation (Art 5, GDPR).	Only information that is necessary to the functionality of the service and is in line with the purposes of data collection will be	• Users of the platform will be required to provide a valid email address, organisation and Name/ position to use the system. Lastly, geolocalisation will be applied for the platform and LEAs App. No other personal information will be collected. • **Users of Mobile Application for vulnerable**

[12] It should be noted that many of these measures have already been addressed by design.

Data protection principles	Established data protection requirement(s)	Concrete indicators for compliance[12]
	gathered, handled and stored.	**citizens will only be required to provide a valid email address to use the system**. They will receive a response welcoming them to the system. This is optional, only required if they wish to submit information. **No other personal information will be collected**. • Users of the Mobile App for vulnerable citizens will have the option to subscribe to emails and text notifications. This will be a generic message sent to all users, not targeted to the needs and requirements of the individual as this would require substantial personal data to be collected.
Security (Arts. 5 and 32 GDPR).	*"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…*" (Art 32, GDPR).	• Personal data stored in this platform is restricted to authorised users. • Pay attention to sensitive categories of personal data (biometrics, information about disability, religion, etc.). Their processing is prohibited (GDPR Art 9), but depending on the amount and type of data, exceptions include consent and security as a legal basis. So, consent and security systems should be proportionate. • NoSQL database technologies will be used for data storage and management. A relational SQL database will be used for most of the application's information. • 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. • Include different security policies for different stakeholders. • Use anonymisation and encryption when applicable. • Integration of the App for vulnerable groups directly with apps will be avoided to prevent privacy and security issues.
Accuracy (Art 5 GDPR)	*d) "accurate and, where necessary, kept up to date; every reasonable*	• Images and videos of individuals, particularly concerning vulnerable groups such as children, will have particular data protection issues. They should

Data protection principles	Established data protection requirement(s)	Concrete indicators for compliance[12]
	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"	manually or automatically be reviewed carefully before being made public.
ARCO rights (Arts. 12-22)	Data subjects have the right to the access, rectification, cancellation and opposition on their personal data.	• Each user may request an export of all PII stored relating to them, which will be provided to them in digital format in a timely manner. • These rights should be reflected in the Privacy Policy and consent forms. Contact information of the Data Protection Officer must be provided in each case. • Ensure availability, traceability, portability and accessibility of all personal data tough a combination of technical and administrative measures.
Storage limitation	*"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*	• 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.

Data protection principles	Established data protection requirement(s)	Concrete indicators for compliance[12]
	Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');"	

Source: own elaboration.

The above data protection requirements should be followed by design and by default in PROACTIVE technologies. As shown in Table 9, the **data governance requirements** pointed out in the previous section (4.1) should be reflected in the policy of access control of controllers and processors (end-users and citizens). This must ensure that each user profile has only limited capabilities in line with his/her legal responsibilities. Controllers must also ensure that technical and organisational basis for ensuring the systems security compliance are in place and maintained.

The Apps/Web must also integrate **appropriate functionalities for informed consent**. These tools should first determine the eligibility of the person who will use the app/web (+ 18 years old, the competent authority, etc.). Then the responsible for data processing should be able to ensure clear and conspicuous notice by thoroughly explaining the proposed uses of the data. Long consent forms should be broken into easily digestible sections. It should take the form of a detailed just-in-time notice, which is provided prior to the use of platform-provided consent mechanisms. All purposes for data processing, the nature of the processing, and whether personal data will be shared with partners (if it will be), are among the details to be provided[13]. Moreover, advice, with an opt-out option, such as the following, should be given:

> We may use your location, and share it with third parties, for the purposes of providing you useful advice and information. To do so, we need your permission:
>
> ❑ Allow
> ❑ Don't Allow
> To learn more, visit our Privacy Policy.

Data points used by the App from the mobile phone, included light or geolocation, should be included in the consent form information. Given the nature of the App for vulnerable groups, such as children or people with specific disabilities, a specific assent protocol should be integrated directly with the App. Vulnerable groups include individuals who are entirely or relatively incapable of protecting their interests. Obtaining users' informed consent is critical when they use the App. Thus, **the App should include functionalities for providing an audio and/or written explanation of**

[13] See a full list of requirements in D8.1.

the system. The content of the assent should be simple and short in length. Functionality that allows the user to assent orally should be included.

Current requirements on users' data to be collected by the platform and the apps are aligned with data minimisation and purpose limitation principles. They also are proportional to the aim and features of the systems. All data to be provided by users, including their email address, organisation, name, position and location, are properly justified under the purposes of the processing. It should be noted that the definition of "personal data" in the GDPR, includes location data as one of the elements by reference to which a person can be identified.

The management of the above personal information, as well as the access to the personal (sensitive) data to be shared through the PROACTIVE technologies, requires **encrypting both communications and data before algorithmic processing** so as to ensure both data quality and those only authorised users can access these data.

Moreover, **software to monitor and detect access and personal data transferences to third parties** should be integrated into the systems. Secondly, in the case of the App for vulnerable populations, **location information may be replaced by "areas" information** to minimise privacy risks associated with the use of the App. Thirdly, **a system to check users' credentials**, so this can be monitored, could be developed. This would facilitate that they can be revoked if needed. Fourthly, **attention should be paid to access security standards** (e.g. log files) and federated security of these systems and the associated authentication and authorisation procedures should be monitored.

Concerning data accuracy and the management of sensitive information, it is recommended to include **an algorithm to classify images and text as objectionable**, detect them and avoid their exchange, in line with existing models (Yu, 2017). This would be useful since false positives could expose individuals. At the same time, **algorithms for filtering disinformation and detecting fake news** could be considered for ensuring automated identification of threats and problematic data (Stieglitz, Bunker, et al. 2017; Zannettou et al. 2019).

Each action of managers and users should be registered, as well as rectification or modification of data during the data breach response process. Once the system is implemented, **a crisis simulation should be conducted**. In particular, it is recommended to conduct a tabletop exercise, where the incident response team addresses a data breach process, testing their performance. In this way, problems can be identified without interrupting the App workflow.

The integration of these requirements will be fostered and monitored through two Tasks: The Privacy by Design recommendations to be provided in D3.3 (M24), and the Privacy Impact Assessment in D3.4 (M40), which is meant to review the efficacy of the measures put in place to ensure privacy.

5. INCREASING PROACTIVE'S ACCEPTABILITY

In this section, we will summarise the acceptability requirements to be followed by both the guidelines and technologies produced by PROACTIVE and translate them into recommendations. This will ensure that the PROACTIVE toolkit gains potential efficacy by going beyond legal compliance. The acceptability analysis and recommendations will focus on four relevant aspects identified in section 3:

a) **knowledge**, in terms of the characteristics of the information needed to be provided by PROACTIVE,

b) **transference**, concerning the optimal mechanisms for communicating this knowledge,

c) **perceived efficacy and ease of use**, regarding how PROACTIVE protocols should be conducted to ensure better preparedness and response to CBRNe events, and

d) the **contextual social factors** that should be taken into account so as to positively influence the implementation of the PROACTIVE toolkit.

5.1. Knowledge as an acceptability driver in PROACTIVE: context and recommendations

As we have seen above, increasing public knowledge about the characteristics of a CBRNe incident is essential for risk awareness and acceptability of security policies. Moreover, in order for the PROACTIVE tools to be positively received, **the public must be informed about the peculiarities and possible consequences of CBRNe incidents and crises**.

The **quality of the information provided to the public**, their comprehensiveness and clarity are also relevant for ensuring proposed policies' efficiency and acceptance. In this context, different limitations have been considered. On the one hand, the production and circulation of disinformation and fake news in CBRNe contexts are a barrier for the promotion of common protocols for tackling them. On the other hand, the information should be explicit while not revealing any confidential information or sensitive aspects that may harm individuals or public security.

Moreover, it has been revealed that **inequality in knowledge** related to socioeconomic status or cultural backgrounds has an impact on the capacity of social groups to respond to the guidelines proposed by the authorities and also to trust in provided instructions. Considering the vulnerability of each group is crucial for enhancing the PROACTIVE toolkit effectiveness but also for its social acceptability. Not properly addressing this factor could harm the legitimacy of the systems at stake. At the same time, a balance between specificity and harmonisation involves finding a mid-way point between adaptability and overall coverage of established guidelines.

Taking these elements into account, **the following acceptability recommendations** should be taken into account and translated into guidance or by design specifications within the PROACTIVE toolkit:

- **Language must be clear**, consistent and targeted to specific audiences.

- **Empathy, concern** -including those elements considered as uncertain-, **reliability** and **precision** should be the ground criteria.
- Instructions must distinguish between **clear actions to be taken** in each stage of the preparedness and response procedures.
- **Reputed and trustable sources** must be used and **reliable spokespersons** must be in charge of the communicative actions.
- **Guidelines must**:
    - openly inform about the risks at stake while seeking to avoid creating alarm;
    - adapt to values and cultural backgrounds of the target audience; and
    - address the vulnerable condition of the target audience by adapting communication methods.

5.2. Awareness and knowledge transference

Self-awareness and cultural-awareness are considered central factors for the efficient deployment of CBRNe policies. As mentioned in the previous section, degrees of knowledge about this topic greatly vary across social groups and correlate to socioeconomic status, cultural belonging and educational level. In this context, **public communication and formal education** democratise access to information and increase the capacity of having a proper attitude towards disinformation. Moreover, it has been considered that an approach to **community resilience**, built through community volunteers and previous experiences (recent events), should be taken. In this framework, the **following recommendations concerning knowledge transference** should be considered in the design and implementation of the PROACTIVE toolkit:

- Conduct and promote **risk-based training**, including incident simulations. Potential threats and options for tackling them should be provided. These exercises should take into account the specifics of CBRNe related risks in a specific context, such as the frequency and characteristics of the incidents. Decision-makers, including politicians in charge of tackling these events, should take part in these activities.
- Develop standards for the **communication of CBRNe events through the media**, taking into account the perception of targeted audiences as well as their responses.
- To have a **proper relationship with the media**, since they will play a central role both in the acceptability of the technologies implemented by PROACTIVE and for the communication of risks and uncertainties of a certain CBRNe incident to the public.
- **Multimedia strategies**, including TV campaigns, newspapers or the internet -with particular emphasis on social media- should be fostered.
    - Methodologies and instruments for reaching different audiences depending on their capabilities to access different sources and platforms must be developed (relevant

identified conditions include residence, age, vulnerability, socioeconomic status, educational level).

- Produce and disseminate hard copies of instructions, in particular for preventing scenarios when the internet is not available or limitations in reaching the elderly population.

- **Communication plans** concerning how to prepare and respond to different scenarios should be created.
  - It is recommended to produce and disseminate pre-incident information.
- Develop and promote the development of **specific strategies for counteracting disinformation and hybrid attac**ks, integrating the dissemination of fake news.
  - Use credible sources and local spokesman to disseminate official information.
  - Refute fake information by using multiple media platforms altogether (social media, news, TV, etc.).
  - Establish public-private governance strategies for ensuring rapid reacting of private corporate media and social media owners in the face of a CBRNe event.
  - Develop a protocol for human-machine interaction in the implementation of algorithmic analysis of collected information so disinformation can be rapidly identified and removed.
- Informative material on common threats, vulnerabilities and options to tackle them should also be circulated through **formal education**.
- It is also recommended to disseminate guidelines and information using visual media such as the **Internet of Things and games to produce simulations of scenarios or instructions** about how to proceed after the event.

5.2.1. Consent to CBRNe policies

Consent and acceptance can only be considered legitimate –and, depending on the case legal- if they are funded on the ethical grounds provided above when it comes to scientific and fact-based information. In this way, public spreading of fake news and the political manipulation of emergency scenarios is a threat to the legitimacy of CRBNe response policies**. PROACTIVE must, therefore, facilitate informed consent through its dissemination platforms and trough technological design.** Moreover, PROACTIVE guidelines must provide a specific strategy for the assent of those individuals who are not able to consent by themselves and harmonise this strategy so it can be applied across the EU.

5.3. Perceived efficiency and ease of use

The above dimensions of acceptability, including the information handled by users and their form of access to it, are quite dependent on their perception of proposed interventions. As we already

pointed out, this assessment conducted by individuals is not only carried out on the basis of a rational evaluation, but it also integrates sociocultural elements related to the dominant **perception of security policies and technologies** at hand. In order to ensure better adoption of the PROACTIVE toolkit, these perceptions must be considered. At the same time, proposed tools must ensure that users have to put the **less effort possible into their adoption in exchange for the highest efficiency possible**. The following recommendations take these two factors into consideration:

5.3.1. Managing perceived efficiency

Concerning the perceived efficiency of the PROACTIVE tools, it is proposed to:

- **Ensure adaptability of the PROACTIVE tools** to different cultural (nationality, religion) and emotional (fear, panic) status of users by:
    - Researching the cultural and social understanding of security and CBRNe related threats as part of the preparedness process;
    - Analysing social and social groups' resilience in this framework to ensure adaptability; and,
    - Using this information to adapt PROACTIVE toolkit to each scenario and each stage of the CBRNe security policy (preparedness, response).
- The above **communication tools must be inclusive** in terms of gender, disability and age. Methods that can support a balance in power relations among social groups should be taken into account.
- High quality in terms of harmonisation, clarity, guidance and adaptability to manage the implications of PROACTIVE in vulnerable citizens or groups.
- **Instructions about how to efficiently respond to a CBRNe event should connect the aim of the measure to be taken with its concrete outcome(s)** to influence the perceived efficacy of recommended behaviours.

5.3.2. Addressing effort expectancy

Reducing the effort to adopt PROACTIVE guidelines is highly dependent on the context of the application of a specific action, but the following are some basic recommendations to be followed:

- **Information shared in the guidelines and navigation in the three PROACTIVE technologies should be meaningful** with large, clear and intelligible sections for each function;
    - Multiple languages should be available in all produced materials;
    - Integrate manageable maps with the location of events to the PROACTIVE technologies;

- The information must be easily edited and uploaded/downloaded and shared within the three PROACTIVE technologies;

- Content must be **adapted to each user interests and capabilities**, including LEAs, policymakers and the targeted vulnerable populations.

5.4. Social influence and facilitating conditions

Acceptability of security policies depends on ethical grounds and public reputation. In this regard, the mechanisms mentioned above for integrating to overcome cultural barriers are essential. These include strategies to add**ress communication with cultural minorities for both preparedness and response** (languages and terminology) or **having multiple and adapted protocols** for decontamination, such as ensuring the presence of women during the process when interacting with populations belonging to some religions (e.g. clothing during the decontamination process).

Nevertheless, other operational aspects can limit the acceptability of the system by both citizens and end-users. This includes **the availability of resources needed to efficiently respond to CBRNe threats or events**, such as an open software system in the case of technological platforms, or the organisation of training. Adopting the toolkit should also fit current legal and political frameworks and address the technical capabilities needed for its implementation.

In this framework, and as part of the development of the toolkit, a set of materials should be produced and provided to end-users and, more broadly, citizens. These materials, which should be developed and shared with both end-users and citizens, include, on the one hand, **manuals explaining the functionalities and goals of the technologies implemented**, its characteristics, security conditions, as well as the restrictions to the processing of personal data. On the other hand, detai**led training** materials should be provided to all end-users managing the PROACTIVE technologies or deploying its proposed protocols. These documents should not only explain the actions to be conducted in the context of preparedness and response to CBRNe events but also properly address the legal, theoretical and ethical justification of such policies.

6. BEFORE, DURING AND AFTER THE EVENT RECOMMENDATIONS PER STAKEHOLDER GROUP

This section organises PROACTIVE project's recommendations on data protection and acceptability for each targeted stakeholder group. It outlines and justifies the proposed policies and protocols addressing their procedural dimension based on previous sections analyses and literature review. The recommendations' presentation considers the various stages of the PROACTIVE App and guidelines intervention, including preparedness, response and post event actions. The analysis's main focus is on data protection and acceptability requirements to be considered during the preparation, response, and post-emergency activities surrounding the adoption of PROACTIVE collaborative web and apps. In this way, this document contributes to the preliminary systematisation of managerial and conceptual aspects of PROACTIVE outcomes, including its guidelines and

technologies. This systematisation will be further developed in D8.4 on the basis of PROACTIVE validation activities.

Following the requirements reflected in the above-examined EU regulations and communications[14], **relations between stakeholders** involved in the first response to CBRNe events must be particularly considered. Along these lines, **citizens' protection and awareness through clear communication** are some of the key goals for technological developments for the PROACTIVE project. Since the analysis will focus on translating the above legal, data protection, and acceptability requirements into phase-by-phase technological use, it will particularly consider how technology mediates stakeholders' relations and contributes to end-users' preparedness and response (Sellström et al., 2011). Main concepts to be addressed for each stage and actor will be based on the adapted *resilience analysis model* for public health emergencies in Table 10.

Table 10 Resilience model for PROACTIVE actors' engagement

	Stages of CBRNe emergency		
Actors	**Preparedness**	**Response**	**Mitigation**
First responders (LEAs, firefighters, military, etc.)	• Training • Plans	• Personnel • Material supplies • Security • Needs assessments	• Return to normal activity • Design improvements • Technology advancements
Policymakers	• Training • Public awareness • Design of standards or regulatory frameworks	• Needs assessments • Material supplies • Security • Family reunification	• Design improvements • Technology advancements • Implementation of standards or regulations
Nongovernmental organisations (including civil society organisations)	• Training • Plans • Emergency contacts	• Personnel • First aid • Counselling	• Increased training

Source: adapted from Kapur and Smith (2011:8).

[14] The EU Internal security strategy (2010); Conclusions on preparedness and response in the event of a CBRN attack (2010); Council conclusions on the new CBRNE Agenda (2012); Communication from the Commission - An Open and Secure Europe: making it happen (2014); The renewed European Union Internal Security Strategy (2015); 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); and 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).

6.1. Preparedness protocols

Preparedness mechanisms will have to be established for efficient use of PROACTIVE tools by end-users, policymakers, and citizens' organisations gathering vulnerable groups who may require special support in the case of a CBRNe event. The "units of analysis" involved in implementing PROACTIVE tools for disasters preparedness are first responders -including LEAs' data controllers, civil society organisations for vulnerable groups and policymakers or public authorities. Among the preparedness measures identified by the literature in CBRNe contexts, **readiness plans and mechanisms for ensuring actors' skills and competences** are two requirements for PROACTIVE smooth implementation (Waugh, 2000; Haddow and Bullock 2006). Therefore, these mechanisms should address these three main groups' needs by design and starting at the implementation phase.

6.1.1. First responders (LEAs and other first responders)

First responders will act as data controllers and managers of the PROACTIVE technologies in most cases, which entails the need for ensuring a comprehensive set of technical and organisational protocols before the system is operational. Although PROACTIVE preparedness technologies requires dynamic collaboration between actors, the roles and responsibilities within this horizontal governance should be clearly demarcated. Tasks to be conducted by LEAs involve ensuring secure data management, establish protocols for implementation and ensure proper personnel training.

As part of these tasks, LEAs will also be responsible for establishing links in three directions:

- Firstly, with public authorities regarding awareness and coordinated strategies for using the PROACTIVE collaborative web platform and App during a CBRNe event;
- Secondly, collaboration with civil society organisations to ensure clear guidelines and skills in the use of the system;
- Thirdly, with the media to coordinate communication and response strategies.

6.1.1.1. Data governance organisation

During the preparation phase, first responders in charge of the system should ensure the establishment of the **legal basis for personal data processing and data governance** within the system management. This includes:

- The role of **controller, processors and assigned DPOs** and the framing of their responsibilities, ensuring that functionalities and the adoption of technology are entirely in line with the proposed governance.
- Boundaries **between GDPR and policing regulations** applicable to the system's management should be clearly defined, distinguishing each participant authority's legal competencies (LEAs and policymakers). In this regard, given the system's sensitive character and the potential management of criminal-related information, LEAs should always act as controllers of the system.

- First responders' organisations should **internally disseminate information about the PROACTIVE system data governance** and users' privacy rights among the first responders' units using the system.

Following the above data governance specifications, the controllers should promote the development of a **data management crisis plan**, with a focus on information sharing. During the entire CBRNe preparedness process, communication, cooperation, and the multi-agency approach need to be harmonised in order for the plan to remain consistent and coordinated. In the PROACTIVE collaborative web platform and App, information sharing takes place both horizontally and vertically, which may lead to possible errors. Data should be collected, analysed, disseminated and communicated to the right persons to circumvent these problems. In this way, all LEAs, civil society organisations and citizen get reliable and useful information and collaborate more efficiently, resulting in better decision-making during disaster response.

6.1.1.2. Data protection manual and training

The planning for the use of PROACTIVE should be reflected in a **PROACTIVE web platform and App management Manual (to be included in D8.4)**, which should integrate the above crisis data management plan. This document should be circulated among first responders and used to conduct training about the system. Such instruments should integrate thorough information about the technical and managerial protocols to be deployed by data controllers, including:

- How to provide **targeted information about data subjects' privacy rights** (both first responders and users) to involved groups and a detailed explanation of the personal data to be shared with the App for registration. This includes a valid email address in case of registered users; and organisation, name, position to use the system and geolocalisation, in the case of registered first responders.

- A template with the **minimum personal data needed** for achieving the PROACTIVE recommended protocols for prevention, preparedness, response and recovery activities together with a recommendation to ensure data minimisation.

- Instructions to **secure personal data integrity and confidentiality**, stressing the importance of protecting special categories of personal data. This includes encryption and (pseudo) anonymisation policies and access control systems.

- A **data breaches response methodology**, addressing relevant definitions on anonymised or properly pseudonymised record of personal data management. This should comprise information about how to track the source of the leak, make statements to counter the false information, communicate with the media to respond or release public information and provide protection to the people who may be falsely identified.

- Information about managing **users ARCO requests**. This includes systematisation of users' data, mechanisms for supporting rectification, portability or removal in applicable cases. The template annexed to this Deliverable and the protocol developed in D10.7-DPIA, together with the Privacy Policy already integrated into the PROACTIVE platform, are guiding instruments aimed at ensuring first responders and citizens data protection rights. Instructions about how to guarantee informed consent of non-registered users.

- In case **policymakers have restricted access to the PROACTIVE web platform**, the controller should monitor their access level. This information and the security systems to ensure access control should be disseminated by the controller among the corresponding institutions and data subjects with access credentials. **Information about Data Protection Impact Assessments (DPIA)** to be assessed or conducted before the adoption process.

6.1.1.3. LEAs policies and preparation activities

As part of the **planning and training process to be followed by LEAs** in charge of PROACTIVE collaborative web platform and App, a set of context-dependent actions will have to be defined before the technology adoption process. This includes establishing the social context for the system implementation, adapting its content to this environment, including targeted, clear and meaningful information about potential CBRNe scenarios, and develop internal protocols for adapting the PROACTIVE guidelines to these likely-to-occur contexts. In terms of these adapted internal and external communication protocols, it is important to consider PROACTIVE project preparedness guidelines and the all-hazard ICS 14 standardised features (Madigan, 2018:9):

- The LEA organisation acting as system controller should establish protocols to ensure that the PROACTIVE App allows all units to **quickly receive the right information** so that the information can be clearly understood. This should allow to easily identify actions, alternative actions and help to anticipate their impact (Sellström et al., 2011: 18). The protocol should also help decide what information collected through the system should be stored and communicated to competent authorities;

- First responders should develop **contingency plans regarding data filtering**, mechanisms for preventing biases and discrimination in this process. These plans should be in line with protocols for data filtering to be used by officers in charge of the system. The step-by-step process should call for triangulating sources to receive alerts from citizens and develop specific mechanisms for avoiding intentional disinformation before and after events;

- First responders should **establish contacts with potential users' organisations** to disseminate relevant information about using PROACTIVE toolkit, providing training, and coordinating its implementation. As part of this collaboration, LEAs should provide guidance about the app's use, **clarifying that the App is not to be used for reporting emergencies** and fostering the use of 112 with this purpose.

- A **credible spokesperson** from the end-user organisation should deliver pre-incident information. Language must be clear, consistent, and targeted to specific audiences.

- The PROACTIVE collaborative web platform and App implementing organisation should establish public-private governance strategies for ensuring rapid reacting of private **corporate media and social media** owners in the face of a CBRNe event.

- **Communication plans** concerning how to prepare and respond to different scenarios should be created. Mechanisms for producing and disseminating pre-incident materials should be defined in this context, also ensuring data privacy.

- LEAs must develop methodologies and instruments for reaching **specific audiences depending on their capabilities** to access different sources and platforms (relevant identified conditions include residence, age, vulnerability, socioeconomic status, educational level). Communication tools must also be inclusive in terms of gender and disability. Address communication with cultural minorities (languages and terminology). Ensure high quality in terms of harmonisation, clarity, guidance and adaptability to manage the implications of PROACTIVE collaborative web platform and App and guidelines in vulnerable citizens or groups.

- **Multimedia strategies**, including TV campaigns, newspapers, or the internet -with particular emphasis on social media- should be fostered to raise awareness about potential threats and inform about how PROACTIVE tools can be used in this context.

- Produce and disseminate **hard copies of instructions** for preventing scenarios when the internet is not available or limitations in reaching the elderly population. Methods that can support a balance in power relations among social groups should be considered.

6.1.2. NGOs and other civil society organisations

The PROACTIVE App smooth adoption and effectiveness greatly depend on the **collaboration between first responders and targeted social groups**. Organisations representing vulnerable populations or working in these domains should be considered a nexus between public authorities and registered users. NGOs have been identified as key **actors within the Common Ground Preparedness Framework** for public health emergency preparedness. They are particularly relevant concerning workforce, partners, and resources and the development and updating of all-hazards management plans (Gibson et al., 2012), and a key partner of public authorities in this domain (Madigan, 2018).

The PROACTIVE system managers should foster the intervention of these organisations within two domains:

- Pre-event targeted communication and awareness activities about PROACTIVE collaborative web platform and App to be conducted **with each represented group**.

- **Forums and collaboration activities with LEAs and policymakers** to ensure collaborative development of all-hazards management plans adapted to PROACTIVE apps and web.

Data protection and operational aspects detailed below follow this rationale.

6.1.2.1. Data protection protocols

NGOs can contribute to ensuring data protection rights of registered users and citizens by disseminating information about PROACTIVE mobile App adapted to each vulnerable population.

- Responsible for the PROACTIVE system should foster NGOs and other civil society organisations to provide **targeted information about the privacy rights of groups they represent** and a detailed explanation of the personal data to be shared with the App for registration (a valid email address) and use (i.e., CBRNe related pictures or videos). This

should include **all personal data managed by the systems**, their use and the data subjects' rights.

- In the above framework, NGOs and other civil society organisations may support **users of the PROACTIVE App to read and verify (tick a box) a Privacy Policy** regarding data protection measures and rights, access to personal data, consent form and disclaimer electronically before they can access the system.

6.1.2.2. Policies and preparation activities

NGOs play a key role in many crisis national response frameworks (Ozerdem and Kapucu, 2013), such as the US Federal Emergency Management Agency case. It has been suggested that NGOs working with a specific vulnerable group can contribute to **improving emergency preparedness and efficiency of response strategies** (Coppola, 2007). In this context, responsible for the PROACTIVE system should foster the support of NGOs in providing:

- **Informative material** on common threats, vulnerabilities, and options to tackle them should also be circulated through NGOs. Strategies should include non-formal and informal educational activities regarding CBRNe and the use of PROACTIVE App.

- **Clear information about the concrete use of the PROACTIVE App during a disaster event**. This should differentiate between PROACTIVE informative purposes from local emergency contacts to be used for reporting criminal activities regarding possible CBRNe attacks.

- **With the above purposes, public authorities and first responders in charge of PROACTIVE should provide specific human and materials recourses** so NGOs can support users during a CBRNe event by using PROACTIVE system.

6.1.3. Policy makers

The third group of stakeholders involved in PROACTIVE collaborative web platform, App and guidelines management are policymakers. This group's form of intervention is subjected to its role in defining data collection purposes. It includes the establishment of mechanisms for providing the technical and organisational means for PROACTIVE tools implementation. Besides these aspects, competent public institutions should inscribe PROACTIVE collaborative web platform and App within their security and social policies aimed at preparing populations for disastrous events. An important part of preparedness policies will focus on overcoming social and cultural constraints in engaging social actors and LEAs in analysing and preventing disaster scenarios (Perry and Lindell, 2006).

In this context, competent public authorities should establish external links in two main directions:

- Firstly, collaboration with LEAs in charge of the system to ensure the availability of material and technical resources and two-flows communication through the PROACTIVE system to integrate public interest content;

- Secondly, collaborate with NGOs to ensure efficient training of targeted groups and integrate targeted content, needs, and interest of target groups into public policies around PROACTIVE.

6.1.3.1. Data governance

Some data protection requirements should be considered by public authorities when adopting the PROACTIVE system, which will be detailed in the policy maker toolkit. In particular**, guidelines for policymakers** in charge of the system or accessing and managing the PROACTIVE App will also have to include instructions on the type of (personal) data allowed to be shared with LEAs and third parties through the platform. These instructions should detail the institutional **responsibilities as a data processor** within PROACTIVE following Art 28 GDPR. This includes designing and implementing IT processes and systems that would enable the data controller to gather personal data and implement security measures that would safeguard personal data or communicate to the controller possible data sharing with third parties.

6.1.3.2. Policies and preparation activities

Public authorities should establish the legal and recourses frameworks for ensuring the smooth adoption and implementation of PROACTIVE collaborative web platform and App, including:

- Establish guidelines for the **policymakers' web platform and App services administration**, including the FAQ page with useful advice about the website itself about particular situations in their area.

- Guidelines should also include information about the most effective and acceptable (see above on LEAs communication) **communication mechanisms** to be considered by policymakers when providing/ signposting users to other relevant sites/ contacts for useful information, for example, accommodation or helplines during an event.

- Develop **public campaigns** (TV, newspapers and the Internet) about CBRNe response, addressing different scenarios to foster better adoption of preventative measures integrated into PROACTIVE. These dissemination activities should underline existing policies and regulations' efficiency, providing scientifically-based response strategies and specific examples of previous events in involved institutions competent territory.

- Develop **public-private alliances** with the media and governance protocols for exploiting PROACTIVE during CBRNe events as a tool for blocking and counteracting fake news during attacks.

- Informative material on common threats, vulnerabilities, and options to tackle them should also be circulated **through formal education**. Disseminate guidelines and information using visual media such as the Internet of Things and games to produce simulations of scenarios or instructions about how to proceed after the event.

- Training facilitated by public authorities should also involve social organisations working with vulnerable populations about how to use the app, types of personal data to be collected and shared, and safeguards to be taken in different scenarios and contexts.

- Facilitate **adaptability of the PROACTIVE tools to different cultural (nationality, religion) and emotional (fear, panic) status of users** by:
    - Researching the cultural and social understanding of security and CBRNe related threats as part of the preparedness process.
    - Analysing social and social groups' resilience in this framework to ensure adaptability; and,
    - Using this information to adapt the PROACTIVE toolkit to each scenario and each stage of the CBRNe security policy (preparedness, response).
- Ensure the **availability of resources needed to efficiently respond to CBRNe threats or events using PROACTIVE**, such as an open software system in the case of technological platforms, or the organisation of training. Adopting the toolkit should also fit current legal and political frameworks and address its implementation's technical capabilities.
- Conduct and promote **risk-based training, including incident simulations**. Potential threats and options for tackling them should be provided. These exercises should take into account the specifics of CBRNe related risks in a specific context, such as THE frequency and characteristics of the incidents. Decision-makers, including politicians in charge of tackling these events, should take part in these activities.
- Promote forums at the EU level to promote harmonisation of CBRNe protocols used to implement PROACTIVE in different contexts.

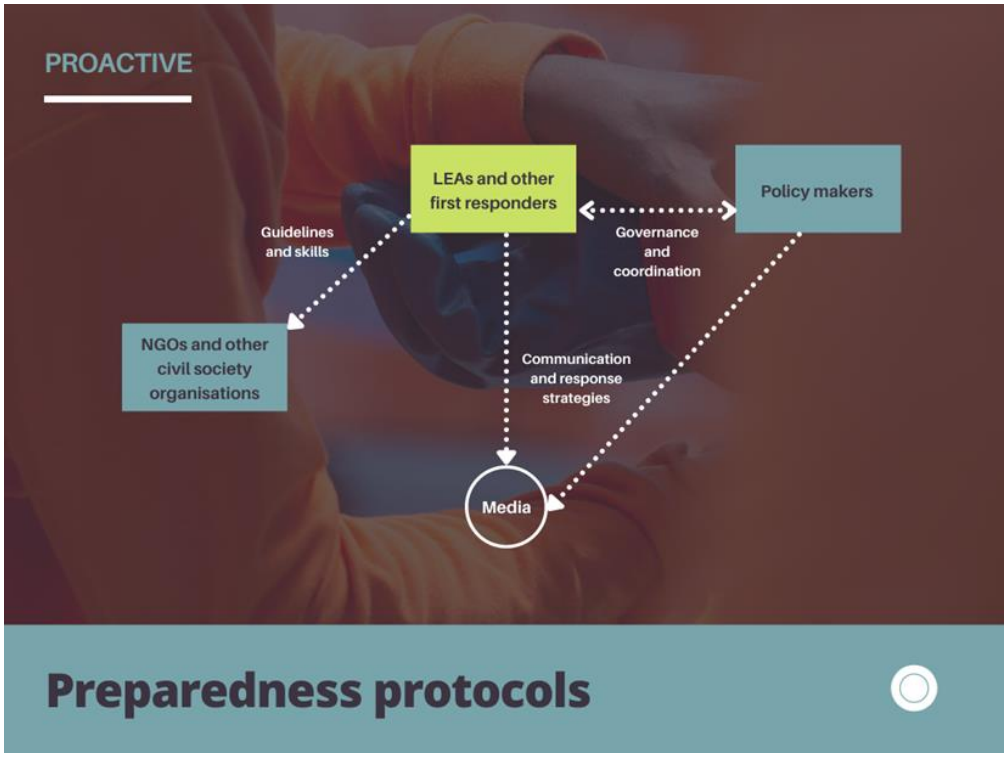

Figure 2 Overview of PROACTIVE preparedness protocols

6.2. Response protocols

As the literature has revealed (Carter et al., 2020), providing **adequate information about CBRNe events about undertaking actions rapidly** can reduce their impact. However, protocols to be deployed during the event are highly dependent on the type of incident at hand and its contextual factors. The PROACTIVE system managers will support the event's detection and foster the sharing of information about the event with those affected and Authorities, emphasising the needs and situation of vulnerable groups. Taking this into account, this section will translate the above data protection and acceptability analysis into targeted recommendations for end-users.

6.2.1. First responders (LEAs and other first responders)

First responders will be **key actors during the deployment of PROACTIVE** based protocols and the use of its technologies throughout a CBRNe event. **Two-way communication with PROACTIVE registered users** will ensure prompt reaction and the establishment of protocols adapted to vulnerable groups affected. Actions to be taken using PROACTIVE during the events include right control of the information, provision of counterinformation when applicable, credible and timely communication about hazards and casualties and support for affected individuals (Wilkinson et al., 2010). It is key for the system's correct functioning that LEAs acting as data controller **ensure prompt and secure communication** with corresponding authorities, including public institutions integrated into the system governance and data protection supervisory authorities. This will help to increase the **situational awareness of all actors involved**.

Three ways communication should be considered in this context:

- Firstly, with registered users following the guidelines below;
- Secondly, and depending on the context or issue at hand, with public authorities and the media;
- Thirdly, amongst units involved in the management of the emergence.

6.2.1.1. Data management

In terms of data management, LEAs effort should focus on **securing data exchanges during the event by applying the above contingency plans**. This includes implementing received guidelines and materials for filtering images and videos of individuals, particularly concerning vulnerable groups such as children.

6.2.1.2. Policies and response activities

In terms of response protocols, **PROACTIVE collaborative web platform and App should be seen as a communication environment** to mitigate damages derived from the event at hand. In this regard, implementing a resilience approach might involve **using PROACTIVE channelled data** about the event among units responding to the emergency, including logistic information about personnel, material supplies, and needs from the scene and security aspects. On this basis, PROACTIVE can support emergency response's key dimensions, including threat detection and classification and damage assessment and some incident management elements such as LEAs mobilisation and notification (Lindell et al., 2006).

Ongoing communication integrated into PROACTIVE tools during the event should be based on clear, consistent, inclusive and group targeted language. First responders should use credible sources and local spokesman to disseminate official information to openly inform about the risks at stake while seeking to avoid creating alarm, adapt to the target audience's values and cultural backgrounds, and address the target audience's vulnerable condition when using PROACTIVE communication tools

Empathy, concern – including those elements considered as uncertain – reliability and precision should be the ground criteria for these instructions. Commands must distinguish between clear actions to be taken in each stage of the preparedness and response procedures. Instructions about how to efficiently respond to a CBRNe event should connect the aim of the measure to be taken with its concrete outcome(s) to influence the perceived efficacy of recommended behaviours.

Moreover, first responders should establish ongoing **communication about the CBRNe event with the media**, considering the perception of targeted audiences as well as their responses. Ensure that the media channel risks and uncertainties of a particular CBRNe incident to the public. Address communication with cultural minorities (languages and terminology). Implement strategies for counteracting disinformation and hybrid attacks, integrating the dissemination of fake news. Refute fake information by using multiple media platforms altogether (social media, news, TV, etc.). Develop a protocol for human-machine interaction to implement the algorithmic analysis of collected information so disinformation can be rapidly identified and removed.

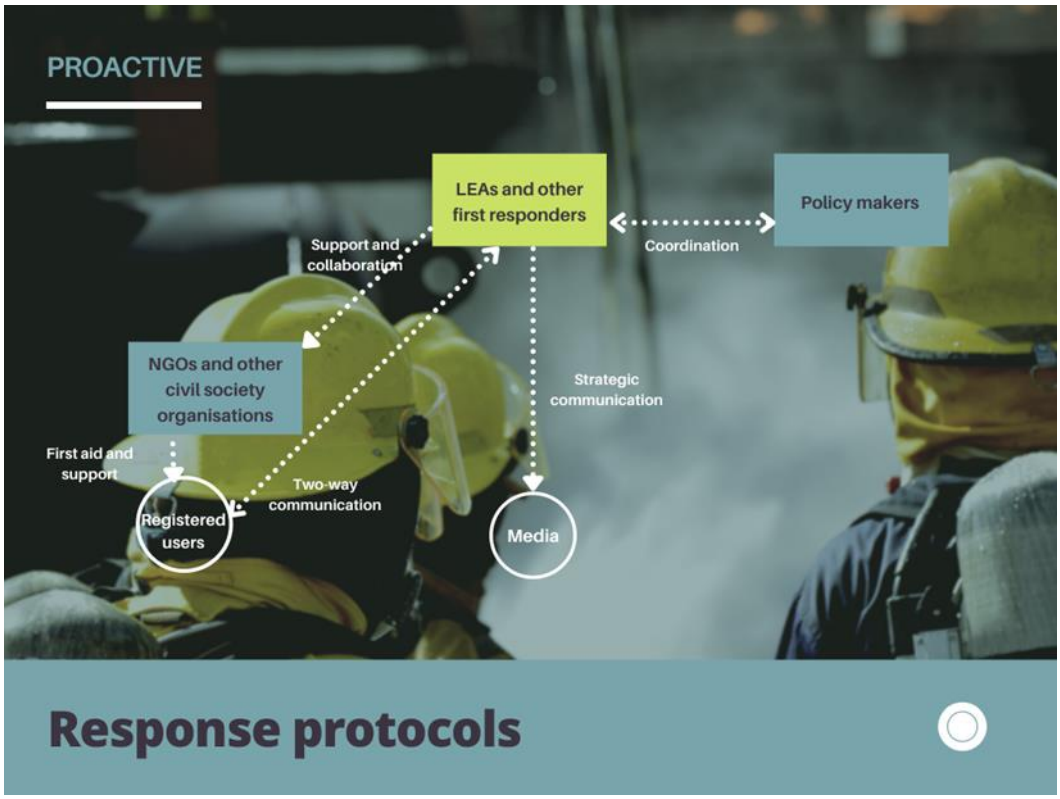

Figure 3 Overview of PROACTIVE preparedness protocols

6.2.2. NGOs and other civil society organisations

As pointed out above, as part of the resilience analysis model, first aid information and counselling tips would be available for user to view and/or download in the App during a CBRNe event. These guidelines will be enhanced during the preparedness and post events phases based on NGOs feedback and contributions.

6.2.3. Policy makers

Public institutions' role regarding PROACTIVE collaborative web platform and App during a CBRNe event will be limited to ensure the system's technical availability, monitoring its security and supporting PROACTIVE functionalities used for family reunification.

6.3. Post-event protocols

Even tough PROACTIVE technologies will mostly be applied to CBRNe events preparedness and response, certain **post-event actions will be required to ensure the non-stope**. With this aim in mind, specific recapping and engagement activities will have to be conducted by all actors involved.

6.3.1. First responders (LEAs and other first responders)

Recovery preparedness practices led by first responders should be improved based on PROACTIVE toolkit use. In particular, as part of the return to normal activity phase, **improvements should be made at both operational and technological levels**. In this way, the post-event processes should involve both mitigation and prevention actions with a particular focus on the utility and awareness of technology (Stanhope and Lancaster, 2018).

These protocols will require active teamwork between LEAs and:

- Firstly, with NGOs, to develop collaborative learning actions;
- Secondly, with public authorities to assess PROACTIVE performance and develop desirability analysis conducting to possible improvements.

6.3.1.1. Data protection

Data protection actions should ensure the mitigation of **any privacy risk derived from previous interventions in CBRNe events** while ensuring the integration of prevention measures based on these experiences. Actions must:

- Ensure that tools and **protocols for removing personal data** are applied once they are not needed for primary uses. Keep only anonymised metadata and records needed for criminal investigation under national and EU policing legal basis. Therefore, the controller organisation should distinguish between data to be used to prevent or tackle incidents and those data related to criminal offences in the context of CBRNe incidents.
- Establish protocols for **informing people and registered users** about data collected in public spaces within certain event scenarios, including data breaches. In this particular case,

protocols will include, depending on the scenario, notifications to data subjects and Supervising Authorities within 72hs after the event occurred.

- Communication **protocols for reaching the media** should be prepared for post-event data processing. In these cases, the policy could include specific counteracting mechanisms to revert misinformation online.

6.3.1.2. Policies and response activities

Actions to be conducted as part of the recovery and prevention process include performance **assessments and redesign of protocols in place**. They should also include developing knowledge materials on CBRNe response focused on vulnerable populations, which must be based on public and anonymous information shared trough PROACTIVE collaborative web platform and App:

- The PROACTIVE system managers should conduct a detailed assessment and modelling of CBRNe threats after a specific event. This should be oriented towards establishing an all-hazards plan to serve as a foundation for the PROACTIVE PROACTIVE collaborative web platform and App's future implementations. It should also be used to define future training developments.

- Accordingly, the examination should integrate recovery plans accounting for specific the PROACTIVE App effects related to its use during the CBRNe event. In this regard, the PROACTIVE system managers should commit to realistic and honest assessments of lessons learned both from previous incidents.

- Commitment to continuous improvement should be based on new knowledge from experience gained from exercises and actual incidents. For instance, adapted protocols for decontamination, such as ensuring women's presence during the process when interacting with populations belonging to some religions (e.g., clothing during the decontamination process).

6.3.2. NGOs and other civil society organisations

As already mentioned, the post-event phase will serve as **an instrument for remodelling PROACTIVE governance and enhance intervention/prevention information**. Specific actions to be promoted within NGOs supporting PROACTIVE should include:

- Conduct **training activities integrating lessons learned** about data management, exploiting the tool and other relevant information from previous PROACTIVE guidelines and technologies use scenarios;

- **Report to LEAs and public authorities on the performance of PROACTIVE** concerning its acceptability and usability for specific vulnerable groups. Limitations and mechanisms for improvement in the use of the App by vulnerable populations should be stressed.

6.3.3. Policy-makers

Public authorities dealing with PROACTIVE toolkits can also improve response to CBRNe disasters based on **continuous policy assessment**. This process is particularly relevant in the case of

PROACTIVE collaborative web platform and App, which could be used as an informative tool for policymaking, since “information about the disaster impact process can be used to identify specific segments of each community that will be affected disproportionately (e.g., low income households, ethnic minorities, or specific types of businesses).” (Lindell et al., 2006:153).

This process will require the active involvement of public institutions in collaborating with:

- Firstly, with LEAs involved in the PROACTIVE system management to conduct joint assessments;

- Secondly, NGOs and the media to examine and possible forms of differential impact of protocols in place.

Under these premises, specific actions may include:

- Produce **support strategies for first responders and civil society organisations** to address post-event mitigation strategies, including communication with the media.

- In line with the acceptability recommendations reflected above, **tabletop exercises, focus groups, and workshops with LEAs’ and civil society organisations'** participation should be coordinated by public institutions. System performance should be analysed in these sessions to integrate stakeholders’ perceptions into the PROACTIVE toolkit protocols. The quality and efficiency of communication tools should be evaluated in these contexts. Moreover, issues limiting the applicability of guidelines integrated into the PROACTIVE App in specific cultural contexts, such as linguistic barriers or the implementation of decontamination protocols for some religious groups, should be discussed in these meetings.

- Regularly **assess the PROACTIVE collaborative web platform and App governance**, including relations to all stakeholders involved, including LEAs, first responders, social organisations and the media.

Figure 4 Overview of PROACTIVE post-event protocols

7. CONCLUSION

This Deliverable analyses the legal requirements identified in D8.1 and examine the acceptability aspects to be considered in the development and implementation of the PROACTIVE toolkit. The methodology of the deliverable combines a thorough review of the literature with the examination of other PROACTIVE deliverables with the information provided by the first responders as part of the Workshop conducted on 19th March 2020. It also integrates the outcomes of a Tabletop exercise on data breaches held on 4th March 2021. This set of materials and activities provides a comprehensive understanding of the issues to be addressed by PROACTIVE toolkits. In this way, the project will ensure its legal compliance and its good reception by first responders and users.

The review of the legal texts shows that human/fundamental rights, data protection law and CBRNe related legislation and recommendations at the EU level are, for the most part, aligned with the goals of PROACTIVE. However, the analysis shows that many legal requirements need to be translated into new mechanisms in the CBRNe preparedness and response fields, mostly concerning how to ensure data protection. Concerning acceptability, the analysis reveals that both the literature and the first responders are on the same page concerning the most relevant elements framing and defining CBRNe policies' acceptability.

All the above normative aspects and proposals for improvement of existing CBRNe tools have been operationalised into a set of specific recommendations that further specify procedural and technical specifications proposed by the project. Having the legal and acceptability lines of development as two dimensions of the analysis also reveals that the PROACTIVE toolkits will have to combine harmonisation efforts oriented to ensuring better efficiency in CBRNe preparedness and response, with mechanisms for ensuring that specific perceptions, needs and interpretations of targeted users groups are taken into account. At the same time, technological standardisation will have to reflect a balance aimed at addressing this trade-off.

8. REFERENCES

Akpan, M. (2016). The Very Real Consequences of Fake News Stories and Why Your Brain Can't Ignore Them, *PBS NewsHour*.

Al-khateeb, S. and Agarwal, N. (2015). Examining botnet behaviors for propaganda dissemination: A case study of ISIL's beheading videos-based propaganda, *Proceedings of the ICDMW*.

Allcott, H., and M. Gentzkow. (2017). Social Media and Fake News in the 2016 Election, *Journal of Economic Perspectives 31*(2): 211–236.

Andrade-Rivas, F. and Rother, H. A. (2015). "Chemical exposure reduction: Factors impacting on South African herbicide sprayers' personal protective equipment compliance and high risk work practices", *Environmental research*,142: 34-45.

Ash, J. (1997). *Factors for Information Technology Innovation Diffusion and Infusion in Health Sciences Organizations: A Systems Approach*. PhD Thesis, Portland State University.

Bass, S.B., et al. (2015). Attitudes and perceptions of urban African Americans of a "dirty bomb" radiological terror event: results of a qualitative study and implications for effective risk communication, *Disaster medicine and public health preparedness, 9*(1): 9-18.

Barcenilla, J., Bastien, J.M.C. (2009). L'acceptabilité des nouvelles technologies: Quelles relations avec l'ergonomie, l'utilisabilité et l'expérience utilisateur? *Trav Humain* 72(4):311–331.

Beck, U. (2000), Risk Society Revisited: Theory, Politics, and Research Programmes, In: Adam, B., Beck, U. and Van Loon, J. (eds.). *The Risk Society and Beyond*. Sage: London.

Bell, P.A., Fisher, J.D., Baum, A., and Greene, T.C. (1990). *Environmental Psychology*. Harcourt Brace Jovanovich College Publishers.

BESECU Project (2011). *Final Report Summary. Human behaviour in crisis situations: A cross cultural investigation to tailor security-related communication*. Available at: https://cordis.europa.eu/project/id/218324/es.

Branson, C., Duffy, B., Perry, C. and Wellings, D. (2012). *Acceptable behaviour? Public opinion on behaviour change policy.* Report, Ipsos MORI Social Research Institute. Available at: https://www.ipsos.com/sites/default/files/publication/1970-01/sri-ipsos-mori-acceptable-behaviour-january-2012.pdf.

Brown, G.D., McMullan, C., and Largey, A. (2018). *A Study of Individual Risk Perception and Household Emergency Preparedness in Ireland*. Dublin, Ireland.

Bobillier-Chaumon, M.É., & Dubois, M. (2009). L'adoption des technologies en situation professionnelle: Quelles articulations possible entre acceptabilité et accceptation? *Trav Humain,* 72(4):355–382.

Busselle, R.W., and Greenberg B.S. (2000). The Nature of Television Realism Judgments: A Reevaluation of Their Conceptualization and Measurement, *Mass Communication & Society, 3*(2&3): 249–268.

Carter, H., Drury, J. & Amlôt, R. (2020). Recommendations for improving public engagement with pre-incident information materials for initial response to a chemical, biological, radiological or nuclear (CBRN) incident: A systematic review, *International Journal of Disaster Risk Reduction*, 51.

Caruana, M. M. (2017). The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement, *International Review of Law, Computers & Technology, 5*.

Cohn, S. (2016). Reconceptualising public acceptability: A study of the ways people respond to policies aimed to reduce alcohol consumption, *Health, 20*(3): 203–219. doi: 10.1177/1363459315574117.

Coppola, D. (2007). *Introduction to International Disaster Management*. Boston: Butterworth Heinemann.

Davidson, L., Weston, D., Amlôt, R, and Carter, H. (2019). *Findings from systematic review of current policy for mitigation and management of CBRNe terrorism*. PROACTIVE Project. Deliverable 1.2.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly, 13*(3): 319-340.

Del Rio Vilas VJ, et al. (2013). Prioritization of capacities for the elimination of dog-mediated human rabies in the Americas: building the framework, *Pathogens and Global Health, 107*: 340–345

Dorasamy, M. and Raman, M. (2011). Information systems to support disaster planning and response: problem diagnosis and research gap analysis, *Proceedings of International Conference on the 8th Information Systems for Crisis Response and Management*.

Douglas, M. (1985). *Risk Acceptability According to the Social Sciences* (Vol. 11). New York: Russell Sage Foundation Social Research Perspectives Occasional Report on Current Topics.

Dubey, Sunil (2018). *Cities, social media and preparedness for major threats*. T4GS Special Reports. Available at: http://www.tech4gs.org/sunil-dubey.html.

European Commission (March 2018). Final report of the High Level Expert Group on Fake News and Online Disinformation. Luxembourg: Publications Office of the European Union. Available at: https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation.

Février, F. (2011). Vers un modèle intégrateur “expérience-acceptation”: rôle des affects et de caractéristiques personnelles et contextuelles dans la détermination des intentions d’usage d’un environnement numérique de travail. Dissertation, Université Rennes 2.

Gibson, P.J., Theadore, F., Jellison, J.B. (2012). The common ground preparedness framework: a comprehensive description of public health emergency preparedness. *Am J Public Health*;102(4):633–42.

Government of Canada (2013). *Building resilience against terrorism Canada’s counter – terrorism strategy*. Available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/indexen.aspx.

Gupta, A., Lamba, H. and Kumaraguru, P. (2013). $1.00 per rt #bostonmarathon #prayforboston: Analyzing fake content on Twitter, *Proceedings of the APWG eCrime researchers summit*: 1–12.

Haddow, G.D. and Bullock, J.A. (2006). *Introduction to Emergency Management*. Boston: Elsevier.

Hales, D. and Race, P. (2010). *Public Security Technical Program Planning Scenario: Final Report*. Defence R&D Canada – Centre for Security Science.

Hall. C., et al., (2019). *Findings from Systematic Review of Public Perceptions and Responses*. PROACTIVE Project. Deliverable 1.1.

Hansis R. (1996). Social acceptability in anthropology and geography, In: Brunson MW, Kruger LE, Tyler CB, et al. (eds). *Defining Social Acceptability in Ecosystem Management: A Workshop Proceeding*. Portland, OR: U.S. Department of Agriculture, Forest Service, Pacific Northwest Research Station: 37–47.

Heath, R.L. and Lee, J. (2016). “Chemical manufacturing and refining industry legitimacy: Reflective management, trust, pre-crisis communication to achieve community efficacy”, *Risk Analysis, 36*(6): 1108-1124.

Heath, R.L., Lee, J.; Palenchar, M.; Lemon, L. (2017). “Risk communication emergency response preparedness: Contextual assessment of the protective action decision model”, *Risk Analysis, 38*(2): 333-344.

Heirston, B. (2010). “Firefighters and Information Sharing. Smart Practice or Bad Idea?”, *Homeland Security Affairs, 6*(2).

Hellier, E., et al. (2014). “*Evaluating the application of research-based guidance to the design of an emergency preparedness leaflet*”, *Appl Ergon, 45*(5): 1320-9.

Hémond, Y., and Robert, B. (2012). "Preparedness: the state of the art and future prospects", *Disaster Prevention and Management, 21*(49): 404 - 417

Hert (de), P. and Papakonstantinou, V. (2016). The New Police and Criminal Justice Data Protection Directive: A First Analysis, *New Journal of European Criminal Law 7*(1): 7-19.

Hughes, A. L. Palen, L. (2009). “Twitter Adoption and Use in Mass Convergence and Emergency Events.”, *Proceedings of the Information Systems for Crisis Response and Management, 6*. doi:10.1504/IJEM.2009.031564.

Huijts, N. M. A., Molin, E. J. E., Steg, L. (2012). “Psychological Factors Influencing sustainable energy technology acceptance: A review-based comprehensive framework”, *EnergyRev, 16*(1): 525–531.

Kanda, H., et al. (2014). “Internet usage and knowledge of radiation health effects and preventive behaviours among workers in Fukushima after the Fukushima Daiichi nuclear power plant accident”, *Emergency Medicine Journal, 31*(1): 60-65.

Kapur, B., & Smith, J. (2011). Public health security: protecting populations from emergencies, in Kapur, G. Bobby, & Smith, J. P. eds. *Emergency public health: preparedness and response*. Sudbury: Jones & Bartlett Learning.

Kaufhold, M-A., Rupp, N., Reuter, C. and Habdank, M. (2019). Mitigating information overload in social media during conflicts and crises: design and evaluation of a cross-platform alerting system, *Behaviour & Information Technology*.

Kingdon, J. (1984). *Agendas, Alternatives, and Public Policies*. Boston, MA: Little, Brown & Co.

Kolliarakis, G. (2017). ‘In quest of reflexivity. Towards an anticipatory governance regime for security’, In: Friedewald, M. Burgess, J. P., Čas, J., Bellanova R. and Peissl, W. (eds.). *Surveillance, Privacy and Security. Citizens’ Perspectives*. London: Routledge.

Kumar, K. P. K. and Geethakumari, G. (2014). “Detecting misinformation in online social networks using cognitive psychology”, *Human-centric Computing and Information Sciences, 4*(1): 14.

Lindell, Michael K.; Carla S. Prater and Ronald W. Perry (2006). *Fundamentals of Emergency Management*. Emmitsburg: FEMA.

Locke, S.; McDonald, M.; Reissman, D. (2004).*The Psychosocial Dimensions of Biodefense Preparedness and Response. A Call for Strategic Systems*. US: Centers for Disease Control and Prevention.

Lucini, B. (2017). *The Other Side of Resilience to Terrorism: A Portrait of a Resilient-Healthy City*. New York: Springer International Publishing.

Malich, G., Coupland, R., Donnelly, S. and Nehme, J. (2016). “Chemical, biological, radiological or nuclear events: The humanitarian response framework of the International Committee of the Red Cross”, *International Review of the Red Cross, 97*(89): 647-661. doi: 10.1017/S1816383116000266.

Marret, J. B., van den Berg, H., van Gorp, A., van Hemert, D. Leone, L., Meijer, R., Warnes, R. and Van Wonderen, R. (2017) *Final report providing background for using and further developing the validated toolkit IMPACT Europe*. D6.2.

Mathieson, K. (1991). "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior", *Information Systems Research, 2*(3): 173-191.

Matthiessen-Guyader, L. (2004). *Conference on Ethical implications of scientific research on bioweapons and prevention of bioterrorism. Report*. Brussels: European Commission.

Mendoza, M., Poblete, B. and Castillo, C. (2010). "Twitter under crisis: Can we trust what we RT?", *Proceedings of the SOMA-KDD*.

Minkyun, K., Raj, S., Cook-Cottone, C.P., Rao H.R., & Upadhyaya S.J. (2012). Assessing roles of people, technology and structure in emergency management systems: a public sector perspective, Behaviour & Information Technology, 31:12, 1147-1160, DOI: 10.1080/0144929X.2010.510209

Mora, A. (2019). 'The Current Legal Framework on Data Protection in CBRNE Crises: A General Exposition', In: O'Mathúna, D. P. and de Miguel Beriain, I. (eds.). *Ethics and Law for Chemical, Biological, Radiological, Nuclear & Explosive Crises*: 147-163. London: Springer.

Mordini, E. (2004). "Ethical Implications of Research into the Prevention of Bioterrorism: final remarks", *Conference on Ethical implications of scientific research on bioweapons and prevention of bioterrorism. Report*. Brussels: European Commission.

Mustonen R. (2018). *Preparedness and response to radiological emergencies*. Finland: Radiation and Nuclear Safety Authority.

Nadamoto, A. Miyabe, M. and Aramaki, E. (2013). Analysis of microblog rumors and correction texts for disaster situations, *Proceedings of the iiWAS*.

NATO (2010). *BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats*: 2. Available at: www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf.

Nyaku, M.K., et al. (2014). "Assessing radiation emergency preparedness planning by using community assessment for public health emergency response (CASPER) methodology", *Prehosp Disaster Med, 29*(3): 262-9.

Ozerdem, A., and Kapucu, N. (2013). *Managing Emergencies and Crises*. Burlington: Jones and Bartlett.

Pearce, J. M., et al. (2013). "Communicating with the public following radiological terrorism: results from a series of focus groups and national surveys in Britain and Germany", *Prehospital and disaster medicine, 28*(2): 110-119.

Perko, T., et al. (2013). "Communication in nuclear emergency preparedness: a closer look at information reception", *Risk Analysis, 33*(11): 1987-2001.

Perry, R.W., & Lindel, M.K. (2006). *Emergency Planning*. USA: John Wiley and Sons.

Pinel, W. (2009). *La résilience organisationnelle: concepts et activités de formation*. M.A.Sc. thesis. École Polytechnique de Montréal, Quebec, Canada.

Pont Sorribes, C. and Cortiñas Rovira, S. (2011). Journalistic practice in risk and crisis situations: Significant examples from Spain, *Journalism*, 12(8): 1052-1066. doi: 10.1177/1464884910388233.

Poortinga, W., Steg, L. and Vlek, C. (2004). Values, environmental concern and environmental behavior: a study into household energy use. *Environmental Behaviour, 36*(1): 70–93.

Public Safety Canada (2017). *An Emergency Management Framework for Canada*. Ottawa: Emergency Management Policy and Outreach Directorate Public Safety Canada.

Reilly, Paul, ; Atanasova, D. and Criel, X. (2016). *A strategy for communication between key agencies and members of the public during crisis situations*, CascEff. Available at: http://eprints.whiterose.ac.uk/93896/1/d3-3-a-strategy-for-communication_final.pdf.

Reuter, C., Stieglitz, S. and Imran, M. (2019). "Social media in conflicts and crises", *Behaviour & Information Technology, 39*, doi: 10.1080/0144929X.2019.1629025.

Reynolds, J. P., Archer, S., Pilling, M., Kenny, M., Hollands, G. J., & Marteau, T. M. (2019). Public acceptability of nudging and taxing to reduce consumption of alcohol, tobacco, and food: A population-based survey experiment. Social Science & Medicine, 236, 112395. https://doi.org/10.1016/j.socscimed.2019.112395

Ringel Morris, M., Counts, S., Roseway, A. Hoff, A. and Schwarz, J. (2012). "Tweeting is believing?: Understanding microblog credibility perceptions", *Proceedings of the CSCW*.

Rolf, W., Wolsink, M., & Burer, M.J. (2007). Social acceptance of renewable energy innovation: an introduction to the concept. *Energy Policy*; 35:2683–91.

Rogers, M. B., Amlôt, R. and Rubin, G. J. (2013). "The impact of communication materials on public responses to a radiological dispersal device (RDD) attack", *Biosecurity and bioterrorism: biodefense strategy, practice, and science, 11*(1): 49-58.

Rubin, J., et al. (2010). *Public Information and Responses to Terrorist Events: Short summary*. PIRATE.

Sellström, Å., Plamboeck, A., Sigsworth, A., Deegan, A., Brinek, J., Kralik, L., … Menning, D. (2011). Final Report of CBRNE map: A better preparedness and response for European citizens facing CBRNE Threats. Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-68666

Spicer, A. (2005). The political process of inscribing a new technology, *Human Relations*, 58(7): 867-890. doi: https://doi.org/10.1177/0018726705057809.

Starbird, K., Maddock, J., Orand, M., Achterman, P. and Mason, R. M. (2014). "Rumors, false flags, and digital vigilantes: Misinformation on Twitter after the 2013 Boston Marathon bombing", *iConference 2014 Proceedings*.

Starbird, K., Spiro, E., Edwards, I., Zhou, K., Maddock, J. and Narasimhan, S.. (2016). "Could this be true?: I think so! Expressed uncertainty in online rumoring", *Proceedings of the* CHI.

Stanhope, M., & Lancaster, J. (2018). *Foundations for population health in community/public health Nursing*. Canada: Elsevier.

Stieglitz, S., Bunker, D., Mirbabaie, M., and Ehnis, C. (2017). Sense-Making in Social Media During Extreme Events", *Journal of Contingencies and Crisis Management, 26*(1): 4-15.

The Guardian (Agencies in Tokio). (1st August 2016). "False Smartphone Alert of Huge Earthquake Triggers Panic in Japan", *The Guardian*. Available at: https://www.theguardian.com/world/2016/aug/01/false-alert-of-huge-earthquake-triggers-panic-in-japan.

Thompson, C. (2017). "Fake News 101: The New Civics Course in US Schools?", *Associated Press, CBSN Boston*. Available at: https://boston.cbslocal.com/2017/02/13/fake-news-school-teaching-trump-facebook/.

Thomson, R., Ito, N., Suda, H. Lin, F., Liu, Y., Hayasaka, R., Isochi, R. and Wang, Z. (2012). "Trusting tweets: The Fukushima disaster and information source credibility on Twitter", *Proceedings of the ISCRAM*.

Torbjørnsen, A., Ribu, L., Rønnevig, M. et al. (2019). “Users’ acceptability of a mobile application for persons with type 2 diabetes: a qualitative study”, *BMC Health Services* Research 19. doi: 10.1186/s12913-019-4486-2.

Tricot, A,, Plégat-Soutjis, F., Camps, J.F., Amiel, A., Lutz, G., & Morcillo, A. (2003). Utilité, utilisabilité, acceptabilité: interpréter les relations entre trois dimensions de l’évaluation des EIAH. In: Desmoulins C, Marquet P, Bouhineau D (ed.) *Environnements informatiques pour l’apprentissage humain*, pp 391–402.

Venkatesh V.; Thong J. Y. L. and Xu, X. (2012). “Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology”, *MIS Quarterly, 36*(1): 157-178.

Venkatesh, V.; Morris, D. (2003). “User Acceptance of Information Technology: Toward a Unified View”, *MIS Quarterly, 27*(3): 425-478.

Vosoughi, S., Roy, D. and Aral, S. (2018). “The spread of true and false news online”, *Science, 359*(6380), 1146-1151. doi: 10.1126/science.aap9559.

Wallner, J. (2008). Legitimacy and public policy: Seeing beyond effectiveness, efficiency, and performance. *Policy Studies Journal*. https://doi.org/10.1111/j.1541-0072.2008.00275.x

Waugh, William L. Jr. (2000). *Living with Hazards Dealing with Disasters: An Introduction to Emergency Management.* New York: M.E. Sharpe.

West, J. (2013). “Bowling with terrorist: Resilience, social capital and hybrid security in the effort to prevent terrorism”, *Paper presented at the CPSA Annual Conference*.

Wilkinson, D., Waruszynski, B., Mazurik, L., Szymczak, A.M., Redmond, E., & Lichacz, F. (2010). Medical preparedness for chemical, biological, radiological, nuclear, and explosives (CBRNE) events: gaps and recommendations. Radiat Prot Dosimetry, 142(1):8-11. doi: 10.1093/rpd/ncq206. PMID: 21041238.

Working Party (2014). Opinion 05/2014 on Anonymisation Techniques. Brussels: European Commission.

Wray, R. J., et al. (2008). “Communicating with the public about emerging health threats: lessons from the Pre-Event Message Development Project, *Am J Public Health, 92*(12): 2214-22.

Wrightson, P. S. (2004). *The Science and Security Dilemma”Conference on Ethical implications of scientific research on bioweapons and prevention of bioterrorism. Report*. Brussels: European Commission.

Yoshida, M., et al. (2016). “Availability of Japanese Government's supplemental texts on radiation reflecting the Fukushima Daiichi Nuclear Power Plant accident for elementary and secondary education from dental students' understanding”, *Journal of Environmental Radioactivity, 155-156*: 7-14.

Zannettou, S., Sirivianos, M., Blackburn, J. and Kourtellis, N. (2019). “The Web of False Information: Rumors, Fake News, Hoaxes, Clickbait, and Various Other Shenanigans”, *Data and Information Quality, 11*(3).

Zubiaga, A., and Ji, H. (2014). “Tweet, but verify: epistemic study of information verification on Twitter”, *Social Network Analysis and Mining, 4*(1): 1–12.

9. ANNEXES

9.1. Annex 1 – Model of ARCO rights request Form

As a data subject under the protection of the GDPR, you are entitled to a set of rights that are generally known as ''ARCO rights''. This form will allow you to exercise those rights as a user of PROACTIVE. If you want to find out more about your rights, you can access the PROACTIVE Privacy Policy and its Manuals, in which there is detailed information on this matter.

a) Identifying information.

In order for us to know who you are and assess your case, we need the following information[15]

- **Data Subject's Name:**
- **Email:**
- **Any other information that may help us to locate your personal data:**

b) **Representatives (only complete if you are acting as the representative for a data subject)**
Representative's Name:
Email:

c) The right you want to exercise:

Now we know who you are. It is time for you to tell us which right you wish to exercise from among the different rights recognised by GDPR, including:

- Right to access
- Right to rectification
- Right to the restriction of processing
- Right to object
- Right to data portability
- Right to erasure

d) Reason or ground on which you base your request:

This section should include a menu with the list of grounds under which the above rights can be exercised. This will change according to the specific right that the user wants to exercise.

e) Data affected:

Here the user would have to specify which data she/he wants to have affected by his or her request. That could be all the data in the hands of PROACTIVE or just a part of it.

[15] *Important note*: the information collected must be the minimum necessary to carry out the processing.