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

Deliverable D4.4

Policy-making toolkit to improve CBRNe preparedness in the European Security Model

Due date of deliverable: 31/05/2023

Actual submission date: 31/05/2023

Mariano Martín Zamorano[1], Virginia Bertelli[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 – 31/08/2023
Duration	52 Months
Coordinator	UIC – Grigore Havârneanu (havarneanu@uic.org)

Document details

Title	Policy-making toolkit to improve CBRNe preparedness in the European Security Model
Work Package	WP4
Date of the document	31/05/2023
Version of the document	07
Responsible Partner	ETICAS
Reviewing Partner	UKHSA, RINI, UIC, CBRNE
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	16/01/2023	Initial structure and index
02	22/02/2023	Deliverable and literature review and theoretical analysis reflected in sections 2 and 3
03	07/03/2023	Outcomes from data collection and systematization on updated versions of PROACTIVE systems
04	25/03/2023	Initial framework for problems and recommendations
05	10/04/2023	Guidelines integrating Rinisoft input, policy briefs analysis and fieldwork outcomes
06	22/05/2023	Final draft for review
07	31/05/2023	Final reviewed version integrating comments and suggestions

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
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
CSO	Civil Society Organisation
FR	First Responder
KPF	Key planning factors
EP	European Parliament
EC	European Commission
SDSP	Secure Design Support Platform
CST	Compliance Support Tool
IMP	Identity Management Platform
MS	Member States
ISO	International Standards Organization
CCS	Crisis Communication System
IT	Information technology

Executive summary

This Deliverable presents a policy-making toolkit for the secure, coordinated and efficient use of the PROACTIVE app and web platform, which also aims at facilitating these systems' scalability, modularity and interoperability mechanisms. It is described in the DoA in the following way:

> *"Each of the above-described PROACTIVE tools will be integrated into a system adapted to the needs of LEAs and other Practitioners. This system comprises therefore many functionalities and involves the management of citizens' data by different actors with different responsibilities, which makes necessary the establishment of clear protocols for its use. This task will be aimed to define a policy-making toolkit for the overall policy management of the system so its scalability, modularity, and interoperability mechanisms can be exploited at full while guaranteeing the respect to privacy and integrity of citizens and LEAs. This set of recommendations, reflected in D4.4, will be based on the analysis of D4.1, 4.2 and 4.3 and will take into consideration the results of the assessments conducted in Tasks 8.2 and 8.4. The policy making toolkit will be in line with the principles of the European Security Model and will include: (a) the results of the diagnosis of the system functionalities and usages, (b) a mapping of users' needs and the definition of policy problems to be considered, and (c) the recommendations translating users' needs into overall policy."*

Along these lines, the Deliverable supplements privacy by design achievements integrated into the PROACTIVE Crisis Communication System by guiding the system exploitation to LEAs and policymakers and aligning all the above outcomes and recommendations to the European Security Model principles. This was done by conducting the following activities:

- Diagnosis of the system functionalities and usages
- Mapping of users' needs and the definition of policy problems to be considered
- Translating users' needs and inputs into overall policy

The document is based on a methodology consisting of an in-depth review of all relevant project deliverables, together with scientific literature and interviews with technical partners in charge of technological development in WP4. Moreover, lessons learned from Dortmund and Rieti's exercises and preliminary elements from Campus Vesta fieldwork are reflected in the guidelines and recommendations described. The three Policy briefs and Guidelines annexed to this document have been developed since 2021 to facilitate the ongoing development of this toolkit. They put together lessons learned from PROACTIVE research in the form of recommendations adapted to the needs of relevant stakeholders, including LEAs, policy-makers and Civil Society Organizations, respectively.

Table of Contents

List of tables

List of figures

1. INTRODUCTION

PROACTIVE is an EU-funded project within the H2020 framework, addressing the topic SU-FCT01-2018-2019-2020: *Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism*. It began on the 1st of May 2019 and will finish on the 31st of August 2023. The project 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 better harmonising procedures between various categories of practitioners and better articulating the needs of vulnerable citizen groups.

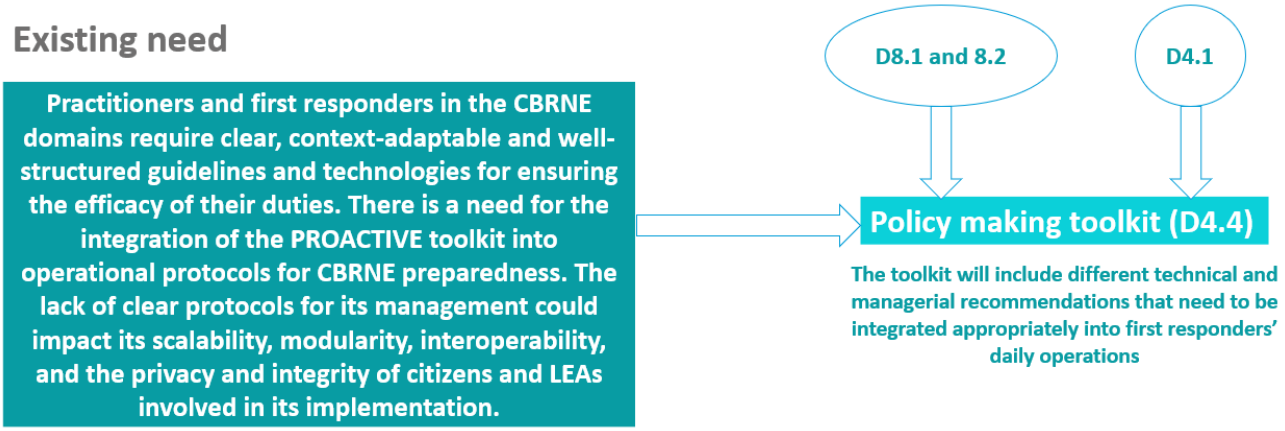
PROACTIVE will result in **toolkits for CBRNe Practitioners and civil society organisations**. The toolkit for Practitioners will include a collaborative web platform with tools for communication and exchange of best practices among Law Enforcement Agencies (LEAs), as well as an innovative response tool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

PROACTIVE is divided into ten Work Packages (WPs). This document is the fourth deliverable within Work Package 4, titled "*Toolkit for LEAs and security Policy-makers*". It is based on work carried out in Task 4.4. The aim of this Task 4.4, "***Policy-making toolkit based on recommendations of citizens and LEAs"*** (M24-35), is to:

*Each of the above-described PROACTIVE tools will be integrated into a system adapted to the needs of LEAs and other Practitioners. This system comprises therefore many **functionalities and involves the management of citizens' data** by different actors with different responsibilities, which makes necessary the establishment of clear protocols for its use. This task will be aimed to define a **policy-making toolkit for the overall policy management of the system** so its scalability, modularity, and interoperability mechanisms can be exploited in full while guaranteeing **respect for the privacy and integrity** of citizens and LEAs. This set of recommendations, reflected in D4.4, will be based on the analysis of D4.1, 4.2, and 4.3 and will take into consideration the results of the assessments conducted in Tasks 8.2 and 8.4. The policy-making toolkit will be in line with the principles of the European Security Model and will include:*

- ✓ *(a) the results of the diagnosis of the system functionalities and usages,*
- ✓ *(b) a mapping of users' needs and the definition of policy problems to be considered, and*
- ✓ *(c) the recommendations translating users' needs into overall policy.*

The methodology of this Deliverable is based on a literature review that included both **scientific papers and the examination of Deliverables 4.1, 8.2 and 8.4**. Results from these documents, including the technical specifications of PROACTIVE systems and their privacy impact assessment, provide comprehensive information about the system characteristics and deployment conditions. As shown in the Figure below, this Deliverable addresses gaps in the articulation between the stakeholders involved in CBRNe scenarios and PROACTIVE technologies by taking profit of work done in both WPs 4 and 8.



Source: own elaboration.

Figure 1. Policy making toolkit gap and main sources

To achieve the above goals, both technical specifications and perspectives on operational aspects were collected from different sources. Regarding the PROACTIVE systems, even though Deliverables 4.2 (Developed Web Collaborative platform) and 4.3 (Developed Modular App for Practitioners) have not been finalized yet, we integrated a set of questions regarding the deployment of the PROACTIVE solutions into qualitative interviews with practitioners and technical partners. Socio-technical data about the system operation was also collected in fieldwork conducted in 2022 and addressed during focus groups in the piloting process (Rieti and Campus Vesta). The present Deliverable integrates interview results to approach PROACTIVE system components from a **broad human-machine interaction perspective**. In this regard, going beyond technology assessment and using results from other PROACTIVE WPs, has allowed us to develop three Policy briefs and Guidelines (annexed[1]) since 2022. These documents focus on Policymakers, First Responders and Civil Society organizations, respectively, serving as the basis for this Deliverable. Still, it should be noted that Guidelines and Policy briefs annexed to this document comprised technological aspects but were **beyond the scope of the PROACTIVE Crisis Communication System** management to gather findings from all PROACTIVE WPs and tools. Therefore, for the purposes of the current Deliverable, elements associated with the PROACTIVE app and web platform have been extracted from them and reinterpreted in light of the operational perspective addressed in this Deliverable.

[1] It should be noted that this Deliverable includes a preliminary version of the Guidelines for First Responders (Annex 3) to be published in June 2023 according to the internal calendar developed by the PROACTIVE project partners. This final version will integrate results from Campus Vesta final exercise (May 2023).

1.1. Objectives

In terms of the general function and grounds of Deliverable 4.4 as part of the PROACTIVE project, the document is inscribed in WP4 objectives detailed in the GA as follows:

- *Develop the technological components supporting the Toolkit.*
- *Design the architecture toolkit (set of tools and supporting technologies), ensuring modularity, flexibility adaptability, scalability and robustness.*
- *Build technological tools facilitating communication and cooperation between LEAs and security-based policy makers in an efficient and effective way, exploiting the use of mobile technologies and bi-directional communication.*
- *Develop restricted access rich visualisation and reporting tools for LEAs and coordinating entities assisting security monitoring of communities; assessing risks, threats, vulnerabilities and incidents; allocation of resources and decision-making.*
- *Integrate and test the Toolkit.*
- *Outputs of this WP will be used in WP6, WP7 and WP8. WP1 and WP2 will give inputs to this WP.*

In this framework, this Deliverable seeks to provide **systematic guidelines for the implementation of the technological component of the PROACTIVE** toolkit without losing sight of overall project findings. The project guidelines and outcomes must be addressed holistically to gain efficiency and feasibility when integrated into end users' protocols and daily operations. While this will be considered, the focus of this document is to establish key **policy and governance aspects** leading to supporting human management of PROACTIVE technology (Crisis Communication System). In the process, these management guidelines will address both organizational aspects and the actual consideration of fundamental ethical principles and legal requirements, such as privacy protection and no harm.

The expected results must **align with the overall Security Union approach** to fighting crime and terrorism. Along these lines, PROACTIVE results are expected to provide valuable inputs to the EUROPOL and other supranational and national police agencies' initiatives to develop a knowledge hub for CBRNe activities and help consolidate the EU Action Plan to enhance preparedness for CBRN threats. In addition, PROACTIVE results will be explored by industrial partners of the project, aiming to generate significant revenues through the commercialization of the developed toolkits.

1.2. Description and structure

This deliverable is divided into the following sections:

1. Introduction: setting the context and goals of the Deliverable
2. Problem definition: summarising relevant CBRNe related issues shaping the management of the PROACTIVE system
3. The PROACTIVE web platform and app: describing the main system features, data management and organizational aspects
4. PROACTIVE acceptability and data protection principles: systematically organising WP8 knowledge to set the boundaries and orientation of the policy-making toolkit

5. EU CBRNe strategy framework: describing main elements of the EU security strategy for CBRNe to be considered in the management of the PROACTIVE system
6. Set of guidelines by system, phase and target group
7. Conclusions
8. References
9. Annexes: including the PROACTIVE policy briefs, guidelines for CSOs and LEAs

1.3 Translating PROACTIVE outcomes into a common policy making toolkit

As for this deliverable, we understand a **policy (making) toolkit** as a "*comprehensive set of recommendations for the setup or reform of policies that are based on insights gained from research*" (Duvvury et al., 2020: 70). Along these lines, we will frame and systematically organize outcomes of PROACTIVE in the form of **recommendations** for the management of its Crisis Communication System (app and web platform). Such recommendations will be adapted to each type of involved stakeholder and their most relevant interrelationships while considering relevant applicable data protection and ethical principles.

CBRNe preparedness and response strategies create the conditions for mitigating the impact of harmful situations concerning citizens' integrity and safety. Authorities are expected to **advance the knowledge of first responders and the public about CBRNe events** and expose the **need to strengthen coordination**, therefore supporting better decision-making by society as a whole. Along these lines, PROACTIVE builds specific but interrelated toolkits for CBRNe practitioners and for civil society organisations.

In PROACTIVE, we focus on three groups defined as follows. Firstly, Practitioners**,** who are defined as **Law Enforcement Agencies** (LEAs, typically Police organisations). Secondly, **First Responders** (e.g., civil protection agencies, fire brigades, ambulance) and related stakeholders comprising private and public bodies, transport and logistic operators, etc., who may be involved in the response in support of the official responders and international, national, and municipal authorities. Lastly, we target **Citizens (mainly represented by relevant Civil Society Organizations),** defined as members of the public. However, among citizens, we specifically address those with needs that differ from the average population, such as persons with disabilities, the ill (e.g., with chronic or acute health conditions), the elderly, or members of an ethnic minority or of a vulnerable group[2].

Moreover, this Deliverable aims to synthesize PROACTIVE conclusions, outcomes, and case studies to also **orient relevant local authorities and policy-makers** on including them in their agenda. In this way, Deliverable 4.4 will offer guidelines for the management of the PROACTIVE platform, its two apps and associated policies. In addition, this document provides tools for **first responders and Civil Society Organizations (CSOs)** to assess their

[2] Vulnerable groups may include children, pregnant women, persons with disabilities, chronic medical disorders or addiction, older persons with functional limitations and health restrictions, institutionalized individuals as well as their caregivers and companions. Vulnerable citizens also include persons with limited proficiency of the respective national languages or with restrictions regarding use of transportation.

current CBRNE frameworks and to understand how to advance towards a policy approach that considers better preventative tools and their complexity.

2. PROBLEM DEFINITION: CBRNE PREPAREDNESS AND RESPONSE

Chemical Biological Radiological Nuclear & Explosive (CBRNe) incidents[3] have been defined as: "*a wide scope of events, including naturally occurring disasters, accidental incidents at hazardous installations or during the transport of dangerous materials"* (European Parliament, 2019:8). Whether accidental or terrorist-based, these occurrences can have a **high impact on society**, including death, injury, and long-term health effects. In addition, CBRNe events can cause psychological trauma and disrupt social and economic systems.

Therefore, it is essential to have effective preparedness and response measures in place to minimize the impact of CBRNe events on public health and safety. Along these lines, PROACTIVE aims to **increase practitioner effectiveness** in managing large and diverse groups of people in a CBRNe environment. CBRNe preparedness and response is a critical public health and safety issue, particularly in the context of terrorism and other man-made disasters.

According to the literature and the PROACTIVE project results (D2.1, D2.5, D8.1 and D8.2), EU Member States **lack a unified approach** to enhance societal preparedness and response policies to CBRNe events and integrate vulnerable groups' needs. Effective preparedness and response to CBRNe events require a coordinated and comprehensive approach that involves a range of stakeholders, including first responders, healthcare professionals, and the public.

Furthermore, CBRNe preparedness and response are **multifaceted and complex**. Incidents widely vary in nature and scope, depending on their sources and social context (Rimpler-Schmid et al., 2021, p. 22). For instance, the emergence of new threats associated with the characteristics of **new technologies used for CBRNe attacks** creates a challenging and changing context for preparedness in terms of general public awareness (Koblentz, 2020). Moreover, besides the specifics of each threat source, one event often combines several forms of social impact, fostering disruptive social scenarios.

Following the National Risk Register for the UK[4], the types of risks and challenges posed by CBRNe events cover several sources and forms of social impact, as shown in the following Table.

[3] European Commission. CBRN Glossary: CBRN.
[4] See at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/952959/6.6920_CO_CCS_s_National_Risk_Register_2020_11-1-21-FINAL.pdf

Table 1. Types of incidents, sources and impacted groups/impact outcomes

Types of incidents	Possible causes	Forms of impact
• Biological • Chemical • Radiological • Nuclear • Explosive	• Warfare • Industrial incident • Rogue state • Terrorist attack • Fire and explosions	• Panic and disorder • Casualties • Toxin release • Fatalities • Environmental contamination • Infrastructure damage

Source: National Risk Register for the UK.

From first responders' and authorities' perspectives, two primary needs required to tackle these scenarios must be considered. On the one hand, **educating** and preparing **the public** to respond appropriately during a specific CBRNe incident is necessary, as detailed in D5.2. This requires the construction of meaningful and actionable messages and efficient communication tools. On the other hand, there is a need to improve the preparedness of **first responders and healthcare professionals** to identify, diagnose, and treat CBRNe **casualties effectively.** Each Member State counts with very different capabilities and coordination tools in this regard (Chatfield, 2018). Therefore, the ability to treat victims of chemical and biological attacks with the most appropriate countermeasures is conditioned by human and technological constraints, which include poor protection for first responders in many cases.

In this general framework, issues identified in the literature and by PROACTIVE (D1.3) project can be summarized and organized according to preparedness and response stages as follows:

CBRNe Preparedness issues:

To improve preparedness for CBRNe events, there is a need for a range of measures, including:

- **Training and education for first responders and healthcare professionals**: First responders and healthcare professionals must be trained and educated to effectively identify, diagnose, and treat CBRNe casualties. This requires specialized training and equipment, as well as ongoing updates and refreshers, to ensure that professionals remain current with the latest information and best practices. In this regard, base and clinical sciences, lessons learned, and continuous improvement have shown to be key in this (Coleman et al, 2019).
- **Development of effective communication and coordination protocols**: Effective communication and coordination between different stakeholders is essential for effective preparedness and response to CBRNe events. This requires the development of protocols for communication and coordination between first responders, healthcare professionals, and other stakeholders. Such coordination may be part of the legal obligations to which authorities and first responders are subjected (Frulli, 2022), which

increases the need for further solutions in this field. Special emphases need to be taken to ensure that the developed communications toolkits are suitable for use by vulnerable people within the stakeholders' groups.

- **Management of essential supplies and equipment**: Stockpiling and administration of essential supplies and equipment, such as protective gear, decontamination supplies, and medical supplies, is essential for effectiveness. Different research has shown how supplies preparation and stockpiling are key in the capacity to respond to CBRNe situations (Taliaferro et al., 2021).
- **Lack of proper mechanisms and tools for the accurate and timely identification of threats**: literature shows that there is a need for further capacities in identifying the specifics of a CRBNe incident, which is determinant in setting proper tools for response (Havârneanu et al., 2022).

CBRNe Response Issues:

The following are some of the key CBRNe response issues that need to be addressed:

- **Lack of trained personnel**: One of the primary challenges in CBRNe response is the need for more trained personnel with the specialized skills and knowledge required to identify, diagnose, and treat CBRNe casualties. This is particularly true in low-resource settings, where access to specialized training and equipment may be limited, and in very specialized threatening scenarios such as agroterrorism (Moats, 2007: 31).
- **Limited access to specialized equipment and supplies**: Another challenge in CBRNe response is restricted access to technical equipment and supplies, such as protective gear, decontamination, and medical supplies. This can make responding to CBRNe events difficult, particularly in low-resource settings (World Health Organization, 2011).
- **Difficulty in identifying and diagnosing CBRNe casualties**: CBRNe-related substances or threats can be challenging to identify and diagnose, particularly in the case of chemical and biological agents (Wilkinson, 2009). This can make providing appropriate treatment and care to CBRNe casualties difficult, mainly if the causative agent is not immediately apparent.
- **Limited coordination among different first responders and LEAs**: In several cases across Europe, lack of coordination among the various agencies and authorities involved in responding, investigating and assessing the impact of CBRNe events has been found (Arrivillaga & Delaney, 2009; Kapucu, & Özerdem, 2011; Gavel et al. 2022), This has often deepened the negative long-term effects of attaches or disasters.

CBRNe Post-event Issues:

- **Psychological trauma**: among the several post-event aspects to be addressed by first responders, police and authorities, trauma has been underlined (Gouweloos et al., 2014). CBRNe events can cause significant psychological trauma, particularly in the

case of mass casualty incidents. This can make it difficult to effectively provide mental health support to those affected by CBRNe events.

The following table summarises the above issues identified by the literature review, which provides some elements of the primary sources of these issues. This suggests how PROACTIVE Crisis Communication System may contribute to filling such gaps.

Table 2. CBRNe scenarios management problems and sources summary

Phase	Problem definition	Related source or domain
Preparedness	Lack of systematic training for first responders	• Policy domain
	Lack of effective communication	• Scarce public resources and accessible technologies • Lack of clear guidelines and proper training
	Supplies and equipment availability and preparation	• Policy domain
	Accurate and timely identification of threats	• Police and first responders' technologies and protocols
Response	Lack of trained personnel	• Policy domain and first responders' governance
	Casualties' identification	• Police and first responders' technologies and protocols
	Lack of coordination among stakeholders	• Policy domain and first responders' governance • Communication and logistic technologies
Post events	Psychological management of those affected	• Policy domain and coordination with first responders and social services

Source: own elaboration.

In brief, CBRNe events pose a significant threat to public health and safety, both in terms of immediate impact and long-term consequences. Effective CBRNe response requires a **coordinated and comprehensive approach** that involves a range of stakeholders, including first responders, healthcare professionals, and the general public and tackles lack of trained personnel, limited access to specialized equipment and supplies, difficulty in identifying and diagnosing CBRNe casualties, and psychological trauma. Addressing these issues is essential to minimize the impact of CBRNe events on public health and safety.

2.1 Gaps in CBRNe preparedness and adapted response tools and strategies

The above issues have been addressed through **specific recommendations**, which will be used to understand PROACTIVE Crisis Communication System alignment with existing problems' solutions (Havârneanu et al., 2023). The document "*Key Planning Factors and Considerations for Response to and Recovery from a Biological Incident*" (Bio KPF; August 2022), provides first responders with a set of information, data sources and mechanisms to dynamize networks between relevant stakeholders. Given that one of the main goals of the PROACTIVE system is to increase coordinated action against CBRNe before and during the event, the document provides a complete, updated and valuable scheme of factors to address the scope of PROACTIVE technology in relation to such actions. The following table distinguishes those Key Planning Factors (KPFs) that are directly related to PROACTIVE technology from those for which PROACTIVE apps and web platform have indirect implications.

Table 3. Key planning factors for response and their alignment with PROACTIVE technologies

KPF	Definition	Alignment with PROACTIVE
Addressed KPF		
Communicate with External Partners and the Public	*Establishing and maintaining communications during a biological incident are important to: 1) enable coordination of efforts between response and recovery personnel and across multiple agencies, jurisdictions, and levels of authority; and 2) convey important messages to inform the public on key aspects of the incident, including the nature of the threat, what they can do to protect themselves, and what they can expect in terms of community mitigation*	PROACTIVE app and web platform core capabilities are designed in such a way to be more aligned with information provision purposes; it also includes communication tools to supplement first responders' work in case of an event. As to be shown in the following sections, accessibility has been considered when developing such tools.
Indirectly addressed KPFs		
Detect and Characterize the Threat	*Timely detection and accurate characterization of a biological incident are key components of an effective response. Early actions such as incident detection and characterization, resource mobilization, and disease containment can save lives. In the context of the malicious use of a biological agent, prompt detection and precise*	PROACTIVE web platform and apps will focus on providing information for CBRNe preparedness and ensuring smooth communication between first responders and those affected by these events. The developed proactive app and web platform incorporate a dedicated CBRNe library which provides easy access to the required information.

	characterization can also help prevent and/or mitigate a potential follow-on incident.	Through the Report an Incident feature, witness to a CBRNe incident can report to the admin (LEAs, first responders), which may help with detection. The information (witness statements, photographs, GPS data) provided in the reports may further help LEAs/first responders to character threats. However, neither detection nor identification of a CBRNe incident are the main goal of the PROACTVE App & web platform.
Control the Spread of Disease	*Disease control efforts limit the spread of disease by avoiding unnecessary exposure and preventing the onset of disease in those exposed.*	PROACTIVE can facilitate information sharing, educate individuals and set communication changes aimed at mitigating disease spread.
Augment Provision of Mass Care and Human Services to the Affected Population	*When mass care services are required during a biological incident, specific infection prevention procedures and protocols may need to be followed if the agent is transmissible from person-to-person. Most biological incidents will not require mass care services of the type and/or on the scale that may be needed in the context of other major disasters such as wildfires or hurricanes*	PROACTIVE management and educational aspects identified in the annexed policy briefs can help authorities and civil society organizations to foster the availability of mass care services and their proper strategic setting in such scenarios.
No addressed KPFs		
Augment Provision of Health and Medical Services to the Affected Population	*A wide range of public health and medical services – including clinical care, patient movement, medical supply chain logistics, and fatality management – may be needed during the response to and recovery from a biological incident.*	No relevant implications for PROACTIVE tools.
Augment Essential Services to Achieve Recovery Outcomes	*In the context of a biological incident, planning for recovery is as critical as planning for response. Resilient and sustainable recovery encompasses not only the restoration of a community's physical structures but also the maintaining continuity of essential services and meeting the enduring needs of the community members.*	No relevant implications for PROACTIVE tools.

Source: KPFs and definitions from Bio KPF 2022.

In brief, as will be detailed in the next section, the PROACTIVE app and web platform are mainly aimed at providing a **communicational and educational space** that will foster exchanges among relevant stakeholders (first responders, authorities and the public). This second preparedness KPFs communication is directly related to PROACTIVE, although response and evaluation phases associated with CBRNe will also serve from the system capabilities. Threat detection is limited to crowdsourcing of CBRNe incidents through the Report an Incident feature, as detailed below. As seen above, these represent two core gaps in the CBRNe domain. On the one hand, the lack of coordination between actors, which will benefit from PROACTIVE' interactive characteristics. On the other hand, actors' cultural capital and knowledge (namely their relevant identitarian, symbolic and educational backgrounds), which are also connected to knowledge transference from scientific to operational domains, will be addressed through the capacity of the system to gather data and information at the planning stage.

2.2 The issue of accessibility and management of vulnerable populations in CBRNe scenarios

The above issues associated with CRRNe management adopt specific implications regarding the way authorities and first responders consider and support vulnerable populations. The PROACTIVE literature review in WP1 confirms that there is little to no consideration of these groups in CBRNe response and preparedness protocols.

Among the identified gaps in PROACTIVE, D1.3 shows how **linguistic, cultural, religious and mobility barriers** need to be addressed when developing CBRNe strategies. In terms of language, communication challenges have been identified in these scenarios, particularly between patients and first responders or when offering aid to a group of people, including vulnerable individuals (Scottish Government, 2015; NHS, 2019). Besides multilanguage approaches, the literature suggests the need to further adapt messages to different ages and disabilities conditions (i.e., through sign language) (Becker, 2004; Marret et al., 2017; Yoshida et al., 2016; BESECU, 2011). Moreover, communication should be empowered by using a trusted spokesperson whose skills and knowledge should be adapted to specific groups at hand (for instance, residents or those with disabilities) (Carter, 2018).

When it comes to **diversity**, one of the main issues is the lack of consideration for different religious beliefs and practices, for instance, when conducting triage, decontamination or when communicating specific goals or protocols during an event (Department of Homeland Security, 2014; Rogers et al., 2013; Alshehri et al., 2016). Something similar has been shown in the case of **mobility and lack of guidance**, for instance, during the decontamination process (NHS, 2019), the use of adequate equipment for taking care of individuals with reduced mobility (Department of Homeland Security, 2014) or the management of service animals (Department of Homeland Security, 2014, 79; London, 2010).

The above has several implications for these groups' human rights (Hurst, 2010). Pre-existing conditions, ranging from disabilities to gender or class factors, work as **exclusionary variables** in CBRNe scenarios affecting rights such as the right to the projection of life. These social and economic conditions are also connected to basic needs such as shelter, or housing directly linked to how individuals are differentially affected by CBRNe events (Zack 2009; Brookings-Bern Project on Internal Displacement 2008).

The above unique challenges faced by vulnerable populations in CBRNe scenarios can also impact their physical and informational privacy (Chen et al., 2009; Hignett et al., 2019). Along these lines, **privacy-related challenges** and risks are frequently overlooked in data protection design and policy decisions. There is growing privacy literature outside privileged categories of young, white, and cisgender, seeking to understand knowledge associated with privacy practices and their implications for vulnerable communities (Guberek et al., 2018; McDonald and Forte, 2022).

3. THE PROACTIVE CRISIS COMMUNICATION SYSTEM (APP AND WEB PLATFORM)

PROACTIVE **collaborative web platform and a mobile app** (for iOS and ANDROID) are referred to as the **PROACTIVE Crisis Communication System (CCS).** The CCS is designed to support LEAs, policymakers, and citizens in the case of a CBRNe event, facilitating bi-directional communication between these stakeholders. Besides offering broad and precise information to enable pre, during, and post-incident information availability, these tools should enhance communication along these processes.

The PROACTIVE solutions provide **adaptability to users' needs and capabilities** to achieve the above purposes (Havârneanu et al., 2023:212). Some aspects concerning the integration of these factors, for instance, through enhancing privacy, accessibility and usability of the App have been addressed in WP8 (as part of the ongoing collaboration between Rinisoft and Eticas) and exercises[5]. However, other elements such as data protection, modularity, adaptability and scalability need to be supported in proper policy and organizational strategies. Along these lines, in this section, we will describe an updated version of PROACTIVE solutions from both technological and managerial perspectives to set the core of the Deliverable analysis in terms of policy making.

3.1 The Web Development Platform for LEAs and policymakers

Once in operation in real scenarios, LEAs will use the Web Platform to report incidents to the public (I.e., using visualisation methods), to monitor communities, assess risks, threats, vulnerabilities, and incidents and allot resources. In addition, the platform allows Bi-Directional

[5] These issues were also addressed to the gaps, needs and requirements definition (WP1), the planned workshops (WP2), as well as Ethics and Legal aspects (WP8).

Communication between LEAs and Security-based Policymakers via direct messaging and forums.
The collaborative platform includes:

- an Online Coordination Portal;
- text, images, videos, audio files and PDF documents

LEAs are able to upload and download these data. Furthermore, this platform includes GIS oriented data storage so LEAs can identify where an incident has occurred and track related information. The platform enables LEAs to create an FAQ page with useful advice about the website itself or about particular situations in their area. Moreover, in real operational scenarios, it will enable LEAs to provide/ signpost users to other relevant sites/ contacts for useful information, for example, accommodation, help lines, charities, etc.

Platform data governance
Given the aims and characteristics of the system, it is likely that **LEAs will be data controllers** of the system in most operational contexts and scenarios. In addition, the platform allows integration with the existing legacy platforms and systems currently used by LEAs.

However, members of **LEAs** managing the system have restricted access via a registration method. The levels of registration will have the necessary corresponding security levels, including:

1. Authorized admin: LEA responsible for the overall platform
2. A restricted user: policy maker
3. Low-level user: citizen

The LEAs are reliant on a map to record incidents, manage/ allocate resources and potentially record images and voice messages of the specific incidents on a map. Customization is available to all users according to the context of a particular scenario (location-map-based), the type of incident and the policies required for specific events.

Data management and security
The platform uses a GIS-based backend for the geo-located data gathered, enabling GIS-oriented data storage, management and analysis. Once in operation in real scenarios, the web platform will be available via the Police Secure networks. To this aim, the system will need to be certified and tested by Police IT (Information Technology) & Digital teams to meet stability and security standards in line with these specifications.

Personal data collected and shared by LEAs and practitioners will include:

- a valid email address,
- geolocalization will be applied.

Given the system architecture and functionalities, any information submitted by citizens

through the app (such as pictures, audios, etc.), including those datasets that may be from a vulnerable group, would also be processed by the LEA Admin before and after the event.

3.2 Mobile Application for Practitioners (LEAs)

The main features of the web platform -such as customization and the use of geolocated data- are replicated in the App used by LEAs and policymakers. In this way, users have remote access to the information they require in real time. Accordingly, LEA's are able to upload, download and remove data from the App, including personal information.

The App functionalities, including visualization methods, will allow LEA's to:

Table 4.End users' app goals, type of action and means

Goal	Action	How
engage with general public	direct	trough dynamic communication
assist in monitoring communities	direct	trough information provision
assessing risks	indirect	via the analysis of reported/gathered data
assessing threats, vulnerabilities, incidents	indirect	via the analysis of reported/gathered data
allocating resources	indirect	via the analysis of reported/gathered data

As for the platform, the language of the static App content is English (to reflect NATO standards). In addition, current version of the app also available in German and special emphases are implemented to ensure real time translation to any required European language.

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

App data governance

The Mobile Application is **administered by LEA**'s and used by policymakers. The App will have restricted access via a registration method, replicating the registration method of the web platform[6]. As for the platform, in order to enter into operation, the system will need to be certified and tested by the Police IT & Digital teams to meet stability and security standards.

It is likely that LEAs will be data controllers of the system in most cases. **The content and credibility of the information will be up to the LEAs and policymakers.** Depending on the

[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.

national legal context and framework and specifics of the political domain, first Responders, who will be provided with access to some information, will possibly act as data processors on behalf of the police.

The use of personal data

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

Stakeholders share this data to dispatch emergency-related information to First Responders, providing the capability to access and exchange personal data. To register for the App, users must share a valid email address, name and organization; geolocalization will be applied. It should be noted that the App will allow access to **sensitive information** about CBRNe incidents and communities in real-time facilitated by citizens. Such information can be shared between stakeholders under the rules defined by the data controller (LEAs).

The App 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. Two data sharing directions must be distinguished:

- To share the data with a citizen, LEAs can post an incident directly on the system and send it off for dissemination via the public App.
- Using multiple media options, pre-incident, real-time, and post-incident emergency-related information will be uploaded directly by citizens (push effect) and other LEAs. This data can be filtered by the data controller.

3.3 Mobile Application for citizens

This **App allows 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 are **able to download and -with manual filter- upload personal data** (PDF, videos, images, audio files).

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. They can also receive **automated early warnings** issued by authorities. Considering VoIP, web portals, softphones, and social media platforms, the vulnerable citizens' App places significant emphasis on delivering broad accessibility and the ability to review or report an incident at a specific location

using a map. However, once in operation and following best practices, 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 includes various settings for accessibility; Font Size & Type, Colour of Screen to support colour blindness, no flashing images are 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.

The App uses novelty, including **pictograms and symbols** to reduce the issue of language barriers. Moreover, it is available for cache data in areas where the internet is not available and, once in operation, should be uploaded automatically when it becomes available.

The App enables the user to select their preferred location when they log in. Moreover, it provides the citizens with useful advice about the app's functionalities and about particular CBRNe situations in their area via an FAQ page. This page has a section prompting the information to be provided during an incident, such as the route to the event or medical symptoms. Lastly, it signposts users to other relevant sites/ contacts for useful information, for example, accommodation, helplines, or charities.

App data governance

The App has two access levels: **Registered Users** (which enables citizens to report emergencies and view information) **and non-registered users, which enables citizens to view information but not reporting incidents**.

Data to be processed includes **personal data** shared by authorised users, including vulnerable groups using the application, such as images, video or audio. Users must share a valid email address only.

3.4 Summary of Apps and Platform functionalities by group

As shown above, PROACTIVE Crisis Communication System aims to connect different end users (these are first responders, including the police and firefighters, with authorities and partner entities) with technology target users, including vulnerable and non-vulnerable citizens. Means of the system to foster these links, co-developed with users and end users, are reporting mechanisms and communication tools, including text, audio, and video, and information repository facilitating education in CBRNe (Havârneanu et al., 2023). Two of these functionalities are crucial to framing the system governance and setting a policy toolkit for it. On the one hand, the location capabilities for end users so they can exploit response factors of this technology. On the other hand, accessibility features of the users' app should be broad communication in the case of those with vulnerabilities.

Table 5. PROACTIVE Systems, functionalities, goals and target groups

System	Functionalities	Main goals	Target groups
Web platform	• Pre and post- incident information • Reporting tools and Notification alerts • Data visualization • Bidirectional communication • GPS identification	• Monitor communities • Assess risks, threats and vulnerabilities • Communicate incidents • Allot resources	• Police • Firefighters • Policy makers
App for LEAs and policymakers	• Pre and post- incident information • Reporting tools and Notification alerts • Data visualization • Bidirectional communication • GPS	• Monitor communities • Assess risks, threats and vulnerabilities • Communicate incidents • Allot resources	• Police • Firefighters • Policy makers
App for citizens/ vulnerable population	• Pre and post- incident information • Reporting tools and Notification alerts • Communication tools • Selection, configuration and adapting of preferred tools (needs and preferences)	• Communicate with other citizens, LEAs and security policymakers • Obtain information and training	• Users (citizens/ vulnerable groups)

Source: own elaboration and Havârneanu et al. (2023).

4. PROACTIVE TECHNOLOGY AND POLICIES ALIGNMENT WITH LEGAL AND SOCIETAL REQUIREMENTS

This section will introduce two different sets of requirements shaping socio-technical aspects of the PROACTIVE Crisis Communication System that are relevant for designing its management policy. On the one hand, those associated with **data protection** and how it has been embedded into the system. On the other hand, **acceptability and usability dimensions**, which also determine how users may approach and interact with these technologies. This analysis is based on requirements and principles identified in D8.2, which are part of an ongoing process of integration into the systems as part of work done in WP4. In this regard, several legal requirements and societal issues presented in this section have also been reflected in D4.1, "*Report on the High-level Architecture design*", as requirements to be translated into technical specifications at the beginning of the project, including an interface control document and others obtained as part of the collaboration with the WP leader Rinisoft.

4.1 Privacy by design process in PROACTIVE Crisis Communication System: requirements and recommendations

In terms of privacy, a thorough examination of the regulatory framework on data protection led to the establishment of recommendations for the management of web-platform and the App to be reviewed in this Deliverable. Such analysis has focused on the role of both technologies and data controllers (those organizations setting the means and purpose for personal data processing, including LEAs and first responders). The outcomes of this study and the recommendations integration process can be summarized as follows:

Table 6. Summary of data protection recommendations in WP8

Variable	WP8 recommendations and definitions	Form of implementation
Data governance	• Identify the **data controller and processors** and frame their responsibilities**, ensuring that functiona**lities 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.	Recommendation for deployment (see guidelines below).
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 PROACTIVE toolkit. • Users of the system will be made **aware of the limitations of the system**, the extent of data to be collected (including their IP address), their right to remain anonymous and the purposes for which this information will be used. The Privacy Policy mechanism will allow users to consent for each category of personal data, detailing the specific purpose of data collection in each case. Users should not feel pressured to supply personal or sensitive information that they do not wish to share. Information on the Use of Cookies to be provided. Users shall be required to sign a consent form and disclaimer before accessing the data.	Recommendation for deployment. Still, the current privacy/cookies policy of the system and the data protection strategy followed during PROACTIVE exercises have been used to validate this approach.
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 into the technical requirements of the App. Minimal Data to be Collected/ Stored principle	This recommendation has been implemented as privacy by design. Data minimization has been enabled by limiting personal data needed for

	(Article 5,1, c, GDPR). When (if) registering, the users' profile shall not demand any personal data. All data requested must be volunteered by the user and is not compulsory. Only data which is absolutely necessary for the functioning of the system is to be collected. Maps must be designed in such a way that no particular home or address can be identified (granularity of event data) • 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.	registering into the app to an email, reducing from several identifiers (name, organization, etc.) to the one indispensable for the system purposes. Still, it is also included as a recommendation for deployment (see guidelines below).
Data security	• Produce protocols and tools for **securing the integrity and confidentiality** of personal data. All data collected through the system are only to be used for the stated purposes. 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. 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". Article 33.5 GDPR mandates to register personal data breaches properly. • Special care must be taken with PDF, audio, 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. Levels are provided according to 4 profiles: public user, LEA, Emergency Responder, and Military. This could be restricted and require permission by the parent organisation. • Users will be **notified of the parties** to whom the data may be transferred, the conditions for	Data security specifications have adequately been integrated into the system design, including a Secure Design Support Platform, a Compliance Support Tool and an Identity Management Platform (see below). Moreover, the access control framework restricts access to authorised individuals' personal data. The recommendations below have addressed procedural and organizational aspects regarding securing personal identifiers.

	transferring the data to third parties, and the rights of the individual (data subject) concerning further processing of their personal data. In case the App has inter-user functionality that allows federation with other App and systems security should be ensured by design (i.e. Encryption)	
Transparency and accountability	• The PROACTIVE toolkit, which will have a strong focus on communication, will have 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. • The evaluation of the need for a DPIA 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 **as mandated in Article 35.1 GDPR).** • Use specific tools and protocols for mapping and registering logs to the system to be integrated into the platform. Include a system to catalogue received information according to the source following Article 30 GDPR. • In this regard, mechanisms for avoiding the transmission of information leading to **false positives or the stigmatization** of protected groups must be considered (data filtering).	The PROACTIVE CCS allows for log tracking. Bias assessment, explicability and DPIA requirements are addressed in operational and organizational guidelines below.
Data subjects' rights	• 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. • Any personal Data collected is to be made available to the user upon Request and Users will have t**he right to access, modify, remove or oppose** processing concerning their personal data (Articles 15 to 22 GDPR). • **Ensure systematic management and 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. • **Ensure data quality and accuracy**	A model for privacy policy and cookies policy compliant with the GDPR has already been integrated into the web platform and App. Procedural and organizational aspects regarding securing personal identifiers have been addressed in the recommendations below.
Profiling and AI fairness	• **Monitor and prevent algorithmic bias and discrimination**, as well as possible false positives/negatives, in particular those	Included as a recommendation for

	related to protected attributes.	deployment.
Data removal	• Establish and communicate a proportional data retention period for all data collected as part of the PROACTIVE toolkit. • The data controllers 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. Article 5.1(e) • Develop tools and protocols for **removing personal data** once they are not needed for primary uses.	Data retention is properly communicated in the CCS privacy policy. Supplementary data removal is also provided as a recommendation for deployment below.

Source: own elaboration based on D8.1 and D8.2.

The above set of recommendations was conceived to guide the governance and protocols of technology **from a sociotechnical perspective** (see section 6). Still, it was also addressed by design following the technological development process as part of the collaboration established within WP4, as shown in the next section. The data protection requirements and their operationalization into potential features or components of the system were based on a taxonomy of issues derived from the system's legal and privacy impact assessment. Some of these requirements are key to be considered in managing PROACTIVE technology from a policy perspective. Beyond the work on privacy by design to be fully reflected in D8.4, the above Table summarises socio-technical requirements.

4.1.1 Data security scheme design

Privacy by design recommendations have also been translated into specific technical specifications and subsystems within the PROACTIVE app and web platform. In particular, to implement security and privacy by design (Data security in Table 5), Rinisoft has used the Security by design Framework and Methodology definition and implementation recommended by the RIA (Italy) as an integral part of the H2020 PANACEA project[7]. This toolkit includes:

- Quality Assurance Process for applications development
- Cyber security guidelines for certification development

Software tools used to enable both aspects are:

- SDSP – Secure Design Support Platform
- CST – Compliance Support Tool

Secure Design Support Platform (SDSP)

It will support the security of a medical device/information system in development, by providing

[7] Although PANACEA is dedicated to cybersecurity in HEALTHCARE, the developed tools are universal and applicable to other areas, including CBRNE

a **software platform for risk assessment** analysis over the system/software. Each risk assessment analysis may produce security controls that will lead to new requirements to be embedded in the system to improve its resulting security.

Compliance Support Tool (CST)

It will support the security of a medical device/information system in development, by providing a software platform for risk assessment analysis over the system/software in development. Each risk assessment analysis may produce security controls that will lead to new requirements embedded in the system to improve its resulting security. The **Compliance Support Tool** provides standardised software to assess the conformance of the target object in scope (i.e., medical device, information system, management systems, etc.) with the following standards:

- ISO 27001,
- EN ISO 13485,
- EN ISO 14971,
- ISO IEC 80001,
- ISO 27799,
- MDR/IVR,
- GDPR,
- ISO 62304

It supports the user in assessing the system development process during all the phases of its lifecycle to set up an effective internal control system focused on managing significant risks and verify the compliance of the whole process to the relevant standards.

The CST consists of a checklist reporting all the relevant risk analysis and standard compliance points. These points are translated into questions that are submitted to the user, who can check them step by step while conducting the internal audit. In addition, the CST allows us to match each standard point to one or more requirements of the developed application in order to verify the requirements coverage based on standards. This checklist is used by App Developers Quality expert, Auditors and support Technicians.

Overall, Rinisoft has implemented the following data security measures:

- Implemented improvements to risk management procedures to improve documentation around residual security risk acceptability;
- Established a sequestered area for user identifiable data for use in future if we start to participate in the management of this type of data;
- Conducted improvements to hazard analysis procedures to include consideration of sensitive data;
- Conducted improvements to the information classification and labelling process;
- Introduced independent review of information security systems to be considered in line with 27001.

Access to multiple standards in one place allowed a unified approach to assessment of conformity and:

- Faster identification of essential requirements;
- Easier identification of existing (and potential) issues due to streamlining audit processes;
- Key security gaps were identified and rectified during the software release review because of this comprehensive assessment;
- Confidence in product security was increased;
- Product quality management activities are planned in line with post-PROACTIVE project product releases.

4.2 Definition and integration of usability and acceptability requirements into PROACTIVE technologies

A second bloc of principles and requirements that should be embedded into the policy-making toolkit are those related to the **perception of end users and users** about the systems and CBRNe guidelines that may affect them during an event. These actors' perceptions and judgments of PROACTIVE technologies are relevant to facilitate their role as communication mechanisms between the stakeholders involved in the CBRNe domain. Based on the UTAUT approach (Venkatesh and Morris, 2003), the characteristics and functionalities of these technologies were discussed in D8.2 for each type of stakeholder. A summary of these examinations, together with elements extracted from the Dortmund and Rieti exercises in this regard, are presented in the following sections.

4.2.1 Platform and app’s acceptance and acceptability from LEAs, first responders and first responders' perspectives

Besides privacy requirements detailed above, acceptability analysis needs to be conducted to ensure an efficient and fair management of both the platform and the Apps for LEAs. This perspective means that acceptability must be assessed by considering the end-user's view about the system's effectiveness and efficiency. Furthermore, the analysis should also evaluate the position of this technological policy within the potential socio-political setting where it will be implemented by taking into consideration the so-called social influence and facilitating conditions.

As for the web platform and LEAs app management, the main acceptability challenges relate to its capacity to work as communication spaces able to organize and articulate relevant information among stakeholders. Other requirements are associated with the need for transparency when presenting the background administration of the platform and its purposes to citizens.

Table 7. Summary of acceptability variables, requirements and recommendations concerning the end users' work

Acceptability dimension	WP8 summary approach related to the platform and app management	Form of implementation
Performance expectancy	To respond to end users' performance demands, the systems should improve their understanding of the CBRNe incident at stake, increase their chances of achieving better preparedness and response coordination, and allow them to accomplish CBRNe tasks more quickly and more efficiently.	This has been partially achieved by the ongoing integration of accessibility and usability recommendations and requirements identified together with relevant stakeholders (CSOs, LEAs, etc.) into the technological design (Havârneanu et al., 2023).
Effort expectancy	To respond to end users' performance demands, the systems should provide a clear and intelligible overview of the crisis scenario and concrete and targeted functionalities for easily collecting and sharing information.	This has been partially achieved by the ongoing integration of accessibility and usability recommendations and requirements identified together with relevant stakeholders (CSOs, LEAs, etc.) into the technological design (Havârneanu et al., 2023).
Social influence	To ensure smooth adoption from LEAs and first responders, social and policy conditions include engaging with other first response agencies and authorities and facilitating to increase public acceptance and knowledge of LEAs task during CBRNe events.	Operational guidelines for deployment aligned with this requirement are provided in Section 6.
Facilitating conditions	To ensure smooth adoption from LEAs and first practitioners, social and policy conditions include that competent authorities would acquire the software, provide training and organizational aspects, ensure the platform fits existing legal and political frameworks, and that technical capabilities are available and fit the purpose of the systems.	Operational guidelines for deployment aligned with this requirement are provided in Section 6.

Source: own elaboration based on D8.2.

Concrete recommendations derived from this summary analysis are detailed in Section 6.

4.2.2 App acceptance and acceptability from users and vulnerable groups perspectives

The App's acceptability for vulnerable groups is vital for a safe and successful implementation of PROACTIVE. Accessibility and adaptability will be crucial to ensure that

it offers an answer to a core goal of the system, which is integrating those historically excluded from CBRNe technologies and protocols. This includes both disability and cultural-based forms of access barriers. Following PROACTIVE analysis in WP8 and a human-machine interaction approach to the App in (Torbjørnsen, 2019) main acceptability factors integrated into the system management policy are approached as follows:

Table 8. Summary of acceptability variables, requirements and recommendations concerning users

Acceptability dimension	WP8 summary approach related to the platform and app use	Form of implementation
Performance expectancy	To respond to users' and, particularly, vulnerable groups' performance demands, PROACTIVE CCS should allow them to better prepare and respond to a CBRNe incident. It should also facilitate their training and provide accurate/updated information on CBRNe issues and events while fostering their communication capabilities in case of a CBRNe event.	Usability requirements integrated into the PROACTIVE app foster the implementation of this requirement. Moreover, procedural recommendations regarding CBRNe awareness and knowledge sharing for CSOs reflected below in Section 6 further enable such performance expectancy factors.
Effort expectancy	To respond to users' and, particularly, vulnerable groups' performance demands, PROACTIVE should provide a clear and intelligible overview of the crisis scenario, as well as offer concrete and engaging functionalities for efficiently collecting and sharing information. Lastly, it should foster communication in the case of vulnerable groups, including the elderly and children and those with the following disabilities: deafness, blindness, intellectual disability, autism, epilepsy, post-traumatic stress disorder, and schizophrenia.	Usability requirements integrated into the PROACTIVE app foster the implementation of this requirement. Moreover, procedural recommendations regarding CBRNe awareness and knowledge sharing for CSOs working with vulnerable groups reflected below in Section 6 further enable such performance expectancy factors.
Social influence	Social organizations targeting vulnerable people should foster engagement with other citizens and support them before and after a CBRNe event to facilitate smooth technological adoption from citizens and vulnerable groups. They also visualise vulnerable groups' needs at the social level and better articulate support of non-vulnerable citizens to vulnerable citizens before and during CBRNe events.	Guidelines and policy recommendations for CSOs aligned with this requirement are provided in Section 6. In this regard, recommendations for policy-makers and regarding the governance/relationships between all stakeholders are vital for creating the social environment for the smooth implementation of the PROACTIVE CCS.
Facilitating conditions	Social organizations and authorities targeting vulnerable people should foster open-source software that could enable	Guidelines and policy recommendations for CSOs aligned with this requirement are provided in

	access, provide an open Manual for the app, provide public support for training vulnerable groups on how to use the app, public promotion of the app, its aims and functionalities.	Section 6. In this regard, recommendations for policy-makers and regarding the governance/relationships between all stakeholders are vital for creating the social environment for the smooth implementation of the PROACTIVE CCS.

Source: own elaboration based on D8.2.

Overall, as reflected in the published Guidelines for social organizations and policymakers (see Annexes 1 and 2), all acceptability requirements, in particular those concerning social influence and other facilitating conditions, require an active involvement of those organizations grouping those disabled, the elderly, children and individuals with other impairments. The issues summarized above are distilled in the form of recommendations for these organizations in Section 6.

5. PROACTIVE TECHNOLOGIES AND POLICIES AND THE EU CBRNE STRATEGY

Besides the above data protection and acceptability requirements, PROACTIVE technologies management should be aligned with the principles guiding the **EU security strategy**. This section summarises this policy framework to be considered in the PROACTIVE CCS implementation.

The **Lisbon Treaty** is the core legal text for the EU to set a framework of "shared internal competences" (Article 4 TFEU) regarding the area of freedom, security and justice, common safety concerns, and transport; civil protection measures (Article 196 TFEU)[8]. Moreover, according to the Treaty, in case of cross-border incidents of high magnitude, EU Member States may choose to employ EU (cooperation) instruments in their response. As such, the EU supports EU Member States through instruments such as judicial and policing coordination activities and cooperative efforts with actors outside the EU (e.g., via the CBRN Centres). The EU also contributes to knowledge building and awareness in this domain, including the

[8] Beyond the EU, the acknowledgement of the dangers related to CBRN weapons has led to the development of international regimes against these weapons. These international regimes can play an important role in reducing the risks of CBRN weapons being used. However, this depends on their actual effectiveness. The regimes seek to constrain state actors but, by tackling proliferation, also have an impact on non-state actors. Three key treaties underpin the international regimes against CBRN weapons – namely, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Chemical Weapons Convention (CWC) and the Biological and Toxin Weapons Convention (BTWC). However, it is also important to note that those key treaties have been supplemented by additional bilateral and multilateral treaties, some of which do not concern CBRN materials directly, but rather the means to deliver them, such as the Arms Trade Treaty (ATT). In addition, some United Nations Security Council Resolutions have introduced new relevant and binding obligations on states, which contribute to addressing the CBRN threat. In this regard, Resolution 1540 has to be mentioned in particular, as it aims at preventing non-state actors from acquiring nuclear, biological, and chemical weapons, their means of delivery, and related materials.

monitoring of incidents (e.g., through various Europol reports such as E-SAT, SOCTA, and Annual Activity report).

With regard to the detection of, response to, and mitigation of CBRNe threats, there is no single piece of overarching EU legislation. Instead, since CBRNe risk management is a cross-cutting, multisectoral, and multidisciplinary matter, there is a complex array of different policies across different policy domains wherein CBRN issues are dealt with specifically. For example, Decision 1082/2013/EU addresses the securing of the food chain against CBRN contamination and Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 offers a framework for combating terrorism.

Moreover, in 2010, the European Commission created the above-mentioned EU CBRN Centres of Excellence (CBRN CoE). The CBRN CoE are a **capacity building and cooperation mechanism** with third countries on CBRN issues, with a view to mitigating CBRN threats stemming from third countries and promoting best practices.

The EU further adopted two **Action Plans**. On the one hand, in 2009, the Strengthening Chemical, Biological, Radiological, and Nuclear Security in the European Union (EU CBRN Action Plan), which was adopted as a comprehensive roadmap in line with the 2005 European Union Counter-Terrorism Strategy and the 2003 EU Strategy against Proliferation of WMD and their Means of Delivery. It contained 124 different actions and took an all-hazards approach. On the other hand, in 2017, the Action Plan to enhance preparedness against chemical, biological, radiological, and nuclear security risk (2017 CBRN ACTION Plan). It focused on reducing the accessibility of CBRN materials, ensuring a more robust preparedness for and response to CBRN security incidents, building stronger internal-external links in CBRN security with key regional and international partners, and enhancing knowledge of CBRN risks.

Additionally, in May 2023, the EC issued recommendations from **Implementation of Recovery and Resilience Plans** - the latest European Commission's assessment of milestones and targets. Ensuring that the CBRN CoE Initiative becomes a genuine EU flagship programme, the document provides several recommendations, among which the followings are more connected to PROACTIVE policy contribution:

- **Recommendation 1**: The European Parliament (EP) may consider requesting the High Representative/Vice President of the European Commission to report to EP on the past achievements and current status of the CBRN CoE Initiative and the plans for its future development as a platform for cooperation and sharing best practices with the participating countries and regions.
- **Recommendation 7**: It is recommended that the EP supports international agreements that foster international collaboration, which contribute to increased security in the area of CBRN. In particular, the EP should continue monitoring the situation on the Korean Peninsula, working through its Delegation for Relations with the Korean Peninsula (DKOR). It may also consider asking the High Representative/Vice-President of the European Commission again to report back to

Parliament to ensure that the issue remains high on the EU's political agenda.

- **Recommendation 8**: The EP may wish to ask the President of the European Commission to report to the EP about the lessons learned from these recent crises, setting out concrete steps and measures to foster solidarity among EU Member States, ensure strategic guidance and close coordination among all relevant partners and EU bodies/agencies, and implement effective crisis management at EU level.
- **Recommendation 10**: The EP may consider monitoring how CBRN security measures are being implemented by different EU bodies/agencies within the scope of their respective mandate to benefit from synergies in programmes and actions.

Besides the above recommendations focusing on CBRNe scenarios, the EU has established a strategy to **improve MS cooperation on internal security challenges**[9] to tackle organized crime, including terrorist activity. This agenda from 2020 to 2025 maps out the primary efforts, tools, and actions to guarantee European security. Components of the strategy cover both the physical and digital world and sectors across all parts of society.

The agenda underlines that **cyber-attacks and cybercrime** continue to rise and security threats are also becoming more complex: they feed on the ability to work cross-border and on inter-connectivity; they exploit the blurring of the boundaries between the physical and digital world; they exploit vulnerable groups and social and economic divergences. In this framework, the European Commission has defined a set of protocols and tools to foster internal security associated with issues directly related to PROACTIVE goals, such as the prevention of violent radicalization. To this end, the EU strategy points to the importance of understanding an open strategic autonomy for supply chains in terms of critical products, services, infrastructure, and **technologies**. It is described as a genuine and effective Security Union that needs to combine a strong core of instruments and policies to deliver security in practice with a recognition that security has implications for all parts of society and all public policies.

In this sense, some of the core aspects of the EU security strategy are aligned with the PROACTIVE approach to CBRNe preparedness and response[10]. Awareness of the existence of "*dangerous chemicals that could be used to carry out attacks*", as well as the need for limiting their access, are just some of the gaps that could be indirectly filled by PROACTIVE tools. Another example is the need for the development of EU civil protection response (rescEU) capacities in the field of CBRN and the establishment "*of national and regional CBRN action plans, exchanges of good practices and CBRN capacity building activities*"[11]. Moreover, the EU Security framework seeks to **enhance security policies' inclusiveness** focusing on

[9] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

[10] The EU security strategy highlights the changing threat landscape: especially, how the world relies on digital infrastructures, technologies and online systems, which allow us to create business, consume products and enjoy services. There are ever-increasing ways in which digital technologies benefit our lives but that have also made the cybersecurity of technologies an issue of strategic importance. The threat analysis above points to four inter dependent strategic priorities to be taken forward at the EU level, in full respect of fundamental rights: (i) a future proof security environment, (ii) tackling evolving threats, (iii) protecting Europeans from terrorism and organised crime, (iv) a strong European security ecosystem. Considering that individuals rely on key infrastructures in their daily lives, the EU's existing framework for protection and resilience of critical infrastructures has not kept pace with evolving risks. In addition, Member States have exercised their margin of discretion by implementing existing legislation in different ways.

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN

"*racial or ethnic origin, religion, belief, gender, age or sexual orientation*"[12]. It is grounded in the common European values - respecting and upholding the rule of law, equality, and fundamental rights, and ensuring transparency, accountability, and democratic control - to give policies the right basis for trust. In particular, it stresses the need to ensure in all the security policies, the principles of necessity, proportionality, and legality, and with the right safeguards for accountability and judicial redress, while enabling an effective response to protect individuals, particularly the most vulnerable. Consequently, the framework is well aligned with PROACTIVE goals and methods.

6. GUIDELINES BY TARGET GROUP, SUBSYSTEM AND PHASE CONSIDERING THE EU SECURITY STRATEGY

Based on information and knowledge reflected in previous sections, this section provides a policy-making toolkit for the smooth implementation of PROACTIVE Crisis Communication System (CCS). As detailed above, CBRNe events pose a significant threat to public health and safety and require a coordinated and comprehensive approach to policymaking to effectively address this issue. The CBRNe policy-making toolkit should be framed to consider the issue's complexity and the range of stakeholders involved.

To tackle the above-summarized registers of the system implementation in one integral **policy-making approach, guidelines have been developed and distributed at different levels and for different actors**. This includes end users, users and their central relationships depending on the technology at hand and actors' roles. At the conceptual level, these relationships are seen according to governance and processes of governing the system (institutions, processes and practices through which issues of common concern are decided upon) and also considering interventions in each phase of CBRNe policies, pre, in and post-event, as follows:

Table 9. Guidelines categories: actors, systems, conceptual perspective, and phases

Actors	System	Level of intervention	Conceptual perspective	Phases
• End users and first responders • Local authorities	• Platform • App for end users	• Governance • Protocols and procedures	• Acceptability • Data management and protection	

[12] Introduction: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0605&from=EN

• Vulnerable groups organizations	• App for citizens	• Protocols and procedures	• Acceptability • Data management and privacy	Preparedness Response Post event
• Interactive approach	• Platform and apps	• Governance • Protocols and procedures	• Interoperability • Modularity • Security	

Source: own elaboration.

Below we describe the primary considerations for these actors to properly implement their tasks associated with **PROACTIVE from organizational and procedural standpoints**. It should be noted that these guidelines are designed to establish the management organigram and protocols best suited to ensure compliance with data protection and acceptability requirements outlined above when deploying the system in real scenarios. In this regard, they seek to reach a balance between standardization and actionability of recommendations while focusing on the most relevant findings.

6.1 Guidelines for end users (LEAs, military defence, firefighters)

PROACTIVE end-users include operators in Law Enforcement, military defense and first responders, which comprises firefighters and police forces. These groups, together with local authorities (see own section below), are expected to oversee both normative and logistic conditions for deploying PROACTIVE technology and managing its systems. The latter consists of its maintenance and data management protocols, among other tasks.

The following are some key considerations for framing the CBRNe policy making toolkit:

- **Coordination and collaboration:** CBRNe policy making should involve coordination and collaboration between different levels of government, as well as with international partners. This can help ensure that policies are comprehensive and consider the needs and perspectives of all stakeholders.
- **Risk assessment:** Risk assessment is a critical first step in the policy-making process. It involves identifying the potential risks associated with CBRNe events and prioritising the most likely and severe risks. This information can be used to inform policy development and decision-making.
- **Stakeholder engagement:** Effective CBRNe policy making requires engagement with a range of stakeholders, including first responders, healthcare professionals, policymakers, and the public. This engagement should be ongoing and involve opportunities for input and feedback at various stages of the policy making process.
- **Evidence-based decision making:** CBRNe policy making should be based on the best available evidence, including research, data, and expert opinion. This can help ensure that policies are effective, efficient, and based on the latest information and best practices.

- **Resource allocation:** CBRNe policy making should consider the allocation of resources, including funding, personnel, and equipment, to effectively address the risks associated with CBRNe events.

6.1.1 End users' CCS organizational and data governance policy

The administration of the ROACTIVE CCS from data controllers and legally responsible perspectives (LEAs and other first responders' units) involves several organizational aspects, including the organizational structure put in place by the implementation organization to support the system's goals, the governance mechanisms that are necessary to ensure the functioning and its evaluation tools. In addition, end users must define a set of main standard measures to implement before deploying the system.

Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **Establish the LEA lead for the system deployment**	The CCS lead organization, which is expected to be an LEA, should be defined and set the technical and organizational conditions for the management of the system. Together with local authorities, the team focal point for the system governance should be defined and informed in a clear manner for all parties involved. This unit is expected to provide training and clear guidelines for the system deployment to the rest of the organizations involved.	**# Preparedness**	• **LEAs** With the intervention of: • Local authorities
✓ **Set the PROACTIVE operations communication protocols**	Teams and an inter stakeholders' communication structure must be enabled, including the inter-agency contact points and agreed communication means (I.e., channels, periodicity, etc.). Moreover, vias used, such as social media or telephone, must be secured for the purposes of PROACTIVE CCS sensitive data management.	**# Preparedness**	• **LEAs** With the involvement of: • Local authorities • First responders

✓ **Define the legal basis for the processing of personal data**	Several aspects of the CCS implementation are determined by the legal basis for processing personal data facilitated by users and citizens that might be identified by the system before, during and after a CBRNe event. In this regard, the data controller must determine the legal basis for the processing (i.e., informed consent, exemptions defined in the LED, public or vital interest) and adopt measures to process data in accordance with such a basis.	**# Preparedness**	• **LEAs**
✓ **Data protection-based organizational conditions**	The identification of data controller(s), their corresponding DPO and technical structure involves ensuring the active role of LEAs in the definition and monitoring of technical and managerial protocols for data protection should be considered. It also involves that controllers and processors should document their corresponding processing activities concerning personal data. This includes a protocol for data breaches and to respond, in due time and form, cancellation, rectification, access and deletion requests. Finally, this protocol should include the DPIA assessment and implementation if required.	**# Preparedness**	• **LEAs**
✓ **Develop information-sharing protocols**	The PROACTIVE CCS team must establish a calendar for regular meetings and working groups to enable agencies to communicate relevant information about the system implementation, update and improvement. Moreover, its relative alignment with security and ethical principles must be discussed in this meeting together with its security implications (such as issues concerning intelligence and threat/risk assessment).	**# Preparedness/ Response**	• **LEAs** With the support of: • Local authorities • First responders

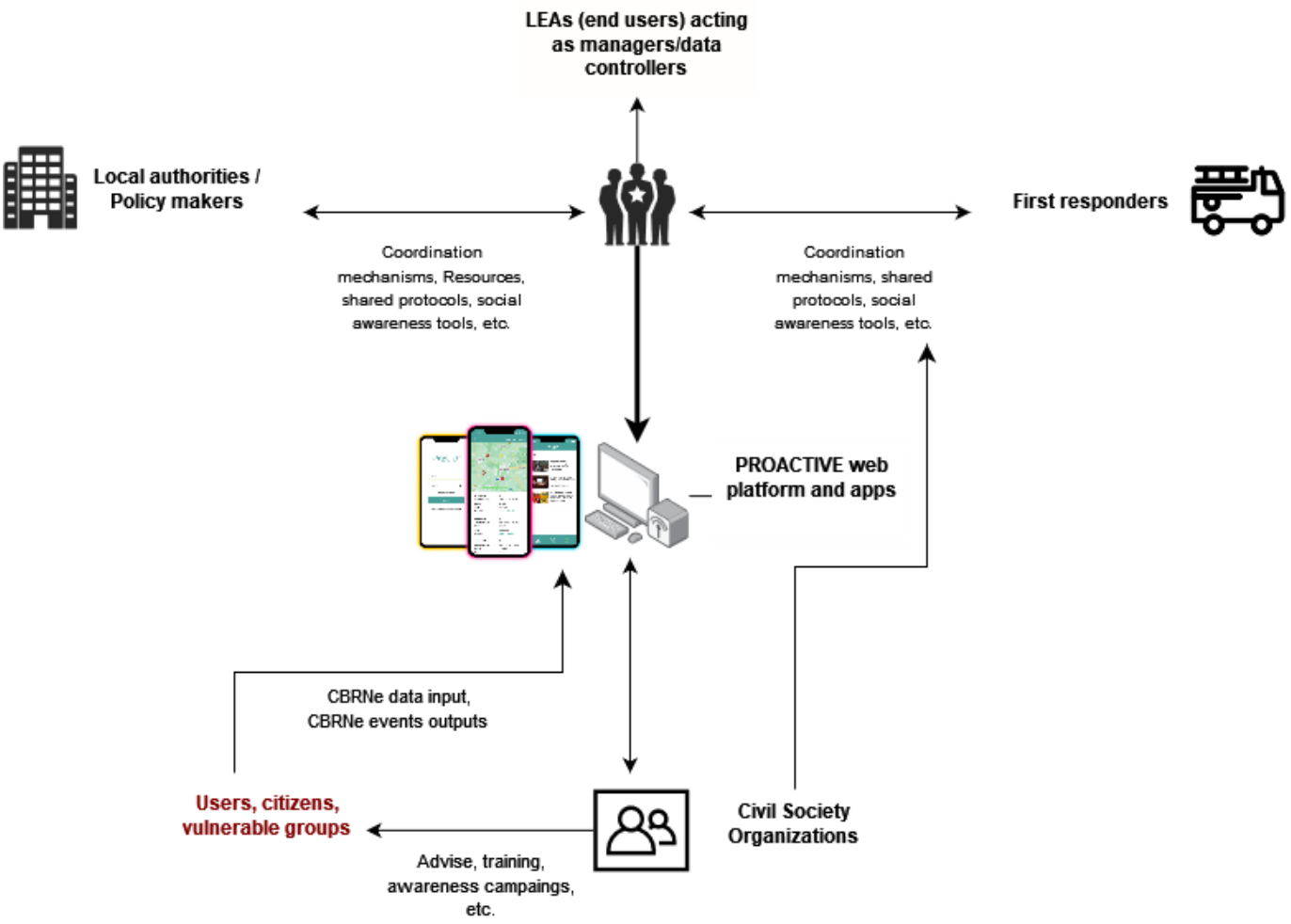
6.1.2 Procedural policy and protocols for end users' CCS management

The platform will not only be a space for the overall system management and end-user units' communication but to allow citizens easy access to CBRNe-related information. When implementing and using the system, the following recommendations and definitions in this regard must be considered.

Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **Manage content stored and provided by the system (acceptability driver I):**	The LEA manager of the CCS should ensure that its repository provides scientifically based guidance for each preparedness/response scenario at stake. Systematic and updated information and sources about CBRNe incidents must be offered, prioritising local sources. Overall, information should contain facts or proof to provide robustness. Pre-incident information materials PROACTIVE has designed should be considered in this regard. Moreover, the App should provide guidelines for users on when and how to report incidents, seeking to limit reporting to standard procedures such as phone calls (I.e. 112).	**#Response/ Post event**	• **LEAs** With the support of: • Local authorities • First responders • Scientists
✓ **Ensure and boost data minimization (already integrated by design)**	PROACTIVE CCS has been developed to ensure data minimization by design since it collects names, emails and IPs only and segments data access according to different end users' profiles, which allows for reducing the number of data entries even more. Still, end users should boost this approach: • They could provide recommendations to users regarding the specific data to be collected by the App. • End users can also select only relevant data to be uploaded to the platform based on their relevance and specificity, always considering avoiding sharing personal information if not needed. • They can implement data	**#Preparedness/ Response/ Post event**	• **LEAs** With the active contribution of • First responders In collaboration with ✓ CSOs

	deletion and retention policies able to ensure proper implementation of the principle of data minimization, which limits the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose.		
✓ **Filter out input personal data from CBRNe events collected by users**	Data filtering is a crucial task to be conducted by LEAs in charge of the CCS This includes assessing information provided by users (I.e., citizens sharing videos and images from CBRNe events that may include personal and sensitive information) from both data protection, accuracy, and security standpoints. The data controller must establish tools and protocols for examining the quality and veracity of personal data used in CBRNe incidents and confirm its veracity and fairness before releasing them and making it accessible to other users. In future versions of the CCS it is recommended to consider including a filtering algorithm to support this task while processing both images and text. If an algorithm for filtering misinformation supports the process and minimises false positive rates, therefore it should be audited to comply with the protection of personal data effectively.	**#Response/ Post event**	• **LEAs** With the potential contribution of: • Local authorities

The following Figure illustrates end users' main role in the **overall governance of the PROACTIVE technologies** and the multiple relationships with other stakeholders in the implementation process.



Source: own elaboration.

Figure 2. Systems governance diagram including main interconnections between actors

6.2 Guidelines for end users (firefighters, police) using the PROACTIVE CCS

6.2.1 Organizational and data governance policy for the end users' CCS management

End users (LEAs and First responders) must ensure proper maintenance and management of the App for both end users and users. This includes tasks such as configuring and updating the PROACTIVE App to ensure usability and enforce principles of veracity, transparency and accuracy. Based on previous research, the main aspects to be considered in this context are listed below.

Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **Prepare information-related conditions for users to adopt the PROACTIVE APP**	The system should be maintained to support the adaptation of content to each user, multiple languages and administration of uploaded and downloaded content. Information should be delivered to the public using multiple sources and explaining the functionalities and goals of the app. Such a process can be facilitated by providing and keeping up-to-date corresponding manuals, FAQ pages and training materials.	**#Preparedness**	• **LEAs** With the support of: • Local authorities
✓ **Tackle inclusiveness and accessibility (acceptability driver I)**	Further assessment of the App design should be conducted by integrating visualisation and communication methods, aiming to ensure that the system is inclusive in terms of gender, disability and age. Moreover, LEAs should assess quality in terms of harmonisation, clarity, guidance and adaptability concerning how to manage vulnerable citizens. Communication should focus on protecting the public's health and aim to influence the perceived efficacy of recommended behaviours. The PROACTIVE CCS has been designed in such a way as to allow for LEAs to communicate in an accessible and inclusive manner with the public at large, including vulnerable groups. It is therefore recommended that LEAs use these features and consider best practice in regards to the actual message sent out via the PROACTIVE CCS.	**# Preparedness**	• **LEAs** With the potential support of: • Local authorities • CSOs
✓ **Enable overall effort expectancy (acceptability driver II)**	End users can also advance efforts to foster the CCS's acceptability among users, making PROACTIVE information more digestible and accessible. Moreover, the platform should offer appropriate feedback from	**#Response/ Post event**	• **LEAs** With the potential support of: • Local authorities • CSOs

	web components and multiple languages the target population uses. Finally, information should be easily edited once uploaded and any edit of the platform should support easy access to it.		

6.2.2 Procedural policy and protocols for end users' CCS management

End users supervising the PROACTIVE app must regularly define how App processes across different sub-systems must function. They can also configure how these technologies run messages to each other. Lastly, end users must administer information stored and available to users is collected, shared and presented. Such protocols must be conducted according to precise main criterion as follows.

Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **Foster technological adoption and transparency concerning the social context (acceptability driver II)**	Information should incorporate factual proof and use a credible information to influence the perceived efficacy of behaviours recommended in cases of CBRNe events and ensure proper alignment of the app with social context. Finally, users must be informed about limitations to uploading and accessing pre-incident, real-time and post-incident.	**#Preparedness/ Response**	• **LEAs** With the support of: • Local authorities
✓ **Ongoing support of the App security (embedded by design)**	Integrate and update security mechanisms of avoiding unauthorized access to pre-incident, real- time and post-incident information and 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. LEAs should explain security conditions for ensuring the integrity of personal information stored in mobile phones.	**#Preparedness/ Response**	• **LEAs**

6.3 Guidelines and recommendations for policy-makers addressing the PROACTIVE system (CCS)

CBRN preparedness and response must be coordinated, with all stakeholders involved acting as an integrated unit. National and local authorities play a crucial role in ensuring CBRNe Governance associated with the effective operation of PROACTIVE while supporting LEAs and first responders. The following points must be considered by authorities when developing these tasks.

6.3.1 Governance policy for the PROACTIVE system

Public agencies in charge of CBRNe policy and security should integrate PROACTIVE CCS into the broad set of available resources to tackle CBRNe risks. The following specific organizational aspects must be considered in this regard.

Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **Enable the creation of a team for overseeing PROACTIVE system operation**	In line with UNICRI recommendations[13], a CBRN national team for the management of PROACTIVE system should be established. Policy makers and authorities should play a key role in facilitating resources for this task and enabling the setting up of a joint team led by LEAs concerning the CCS.	**#Preparedness**	• **Local authorities** With the collaboration of: • LEAs and other first responders
✓ **Document responsibilities in concrete terms**	Together with LEA leading the management of the system, local authorities must document responsibilities around the system following the national regulations and the principles of the above EU security agenda and recommendations. The team's unique responsibilities must be reflected in an organization chart and accountabilities must be precisely articulated.	**#Preparedness**	• **Local authorities** With the collaboration of: • LEAs

[13] Available at: https://unicri.it/topics/cbrn/security_governance

✓	**Foster standardization and scalability**	Policy makers must support LEAs in PROACTIVE system policies standardization. The unit overseeing the system should promote the creation of a list of areas demanding conformance to national, regional and international standards, including the potential use of the system in other regions of the MS. Action plans, including a timetable and responsibilities for this task, must be in place (see section 6.4).	**#Preparedness/ Post event**	• **Local authorities** With the collaboration of: • LEAs

6.3.2 Procedural policy for policy makers overseeing the PROACTIVE system

Public authorities must develop specific protocols for supporting LEAs, first responders and CSOs using and managing the CCS operations. The tasks listed below comprise a wide range of actions and strategies aimed at ensuring smooth operations covering material, technical and human resources.

Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **Promote coordination in the management of the PROACTIVE CCS**	Policy makers should facilitate pre-planning between agencies and organizations to ensure consistency. To this end, they must develop networked and coordinated procedures defining the roles and responsibilities of CBRNe practitioners. They can also improve overall response by sharing uniform instruction materials, plans and best practices (I.e., in the form of hypothetical scenarios) to achieve a consistently high level of preparedness when using PROACTIVE in their territory/power domain.	**#Preparedness**	• **Local authorities** In collaboration with: • LEAs • First responders
✓ **Promote and implement awareness and dissemination actions around**	Policy makers should put their effort into facilitating conditions for educating people on CBRNe events' impact and implications. Such educational programs	**#Preparedness**	• **Local authorities** In collaboration with: • LEAs • CSOs

	the PROACTIVE CCS	should raise awareness of their implications for vulnerable populations. Pre-incident information must be culturally appropriate, easy to understand and factual. Guidance and policy should be updated to incorporate a detailed communication strategy for how emergency responders should communicate with casualties and members of the public during a CBRNe incident.		
✓	**Set a communication protocol for CBRNe events aligned with PROACTIVE CCS**	Local authorities can support LEAs managing PROACTIVE in developing dissemination materials incorporating up-to-date evidence-based advice on how members of the public are likely to respond in a CBRNe incident, including psychosocial factors. It is recommended to adopt layman's terms in regard to language and complexity and integrate them into preparedness policy materials. Policy makers should monitor that, where possible, information communicated by the PROACTIVE App is available in writing using non-complex language. Guidance and policy should include a clear strategy on how to manage vulnerable groups in CBRNe incident. This includes both communication and response plans adapted to these groups.	**#Preparedness/ Response**	• **Local authorities** In collaboration with: • LEAs • CSOs

✓	**Ensure acceptability in CBRNe response communications**	Local authorities can support LEAs in monitoring that PROACTIVE technologies comply with the evidence-based crisis communication recommendations. Policy makers and LEAs must foster institutional action to ensure that CBRNe management adequately addresses cultural factors (I.e., language barriers).	**#Preparedness/ Response**	• **Local authorities** Supporting to: • LEAs
✓	**Assess PROACTIVE CCS governance**	Local authorities should set conditions for regularly assessing technology governance, including relations with all stakeholders involved, addressing LEAs, first responders, social organizations and the media. CCS performance should be analysed in these sessions to integrate stakeholders' perceptions into technological toolkits and protocols.	**#Post event**	• **Local authorities** Supporting to: • LEAs
✓	**Assess PROACTIVE CCS performance**	Local authorities should facilitate material and logistic conditions for the development of tabletop exercises, focus groups, and workshops with LEAs' and civil society organizations aimed at assessing the app's performance after a CBRNe event. Issues limiting the applicability of the CCS used in specific cultural contexts, such as linguistic barriers, should be discussed in these meetings.	**#Post event**	• **Local authorities** In collaboration with: • CSOs • LEAs

6.4 Guidelines and recommendations for civil social organizations to implement the PROACTIVE App

Civil Society Organizations (CSOs) acting in emergency protection should develop dynamic collaboration with First Responders (FR) and public authorities to facilitate the implementation of PROACTIVE technology. This coordination process can support coherent, evidenced-based emergency procedures before, during and after the CBRNe event.

6.4.1 Organizational framework for CSOs supporting PROACTIVE App implementation

CSOs have a secondary role in setting the organizational aspects shaping PROACTIVE technology performance and capacity to enable compliance with target populations' rights. Still, specific actions can be conducted by these organizations to develop a safe, inclusive and promoting scenario for the use of this technology.

Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **CSOs should foster agreements with end users to implement the CCS**	CSOs and FR (with the support of local authorities) should sign Memorandums of Understanding or Cooperation Agreements with respect to vulnerable groups' involvement in CBRNe prevention actions, joint education programmes, training exercises, etc.	**#Preparedness**	• **CSOs** gether with: • LEAs • Local authorities
✓ **Develop communication tools for promoting PROACTIVE CCS among potential users**	CSOs should consider e-mails, online newsletters, and their websites and social media channels for contacting members of civil society and providing them with CBRNe App-related material and updates.	**#Preparedness**	• **CSOs** In collaboration with: • LEAs

6.4.2 Procedural strategy and protocols for CSOs supporting PROACTIVE App implementation

CSOs can also promote the establishment of educational, communicational and lobbying tasks aimed at ensuring the proper adoption of technology by their members and target groups, focusing on vulnerable groups. The actions listed below cover these three main dimensions of potential vias of contribution to PROACTIVE use.

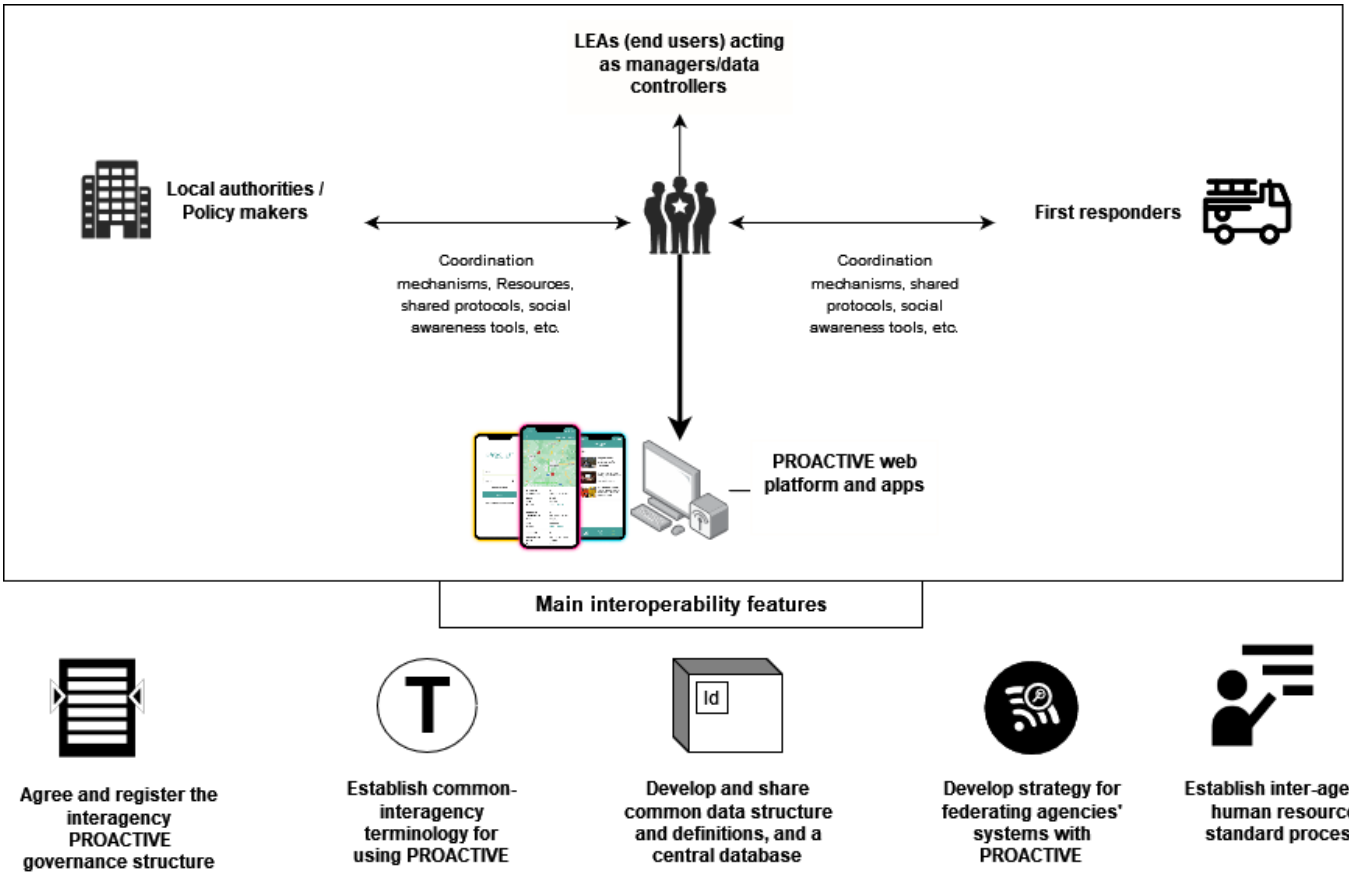
Recommendation	Definition	Corresponding phase(s)	Actors involved
✓ **CSOs should foster engagement of local first responders in adopting PROACTIVE CCS and managing it according to target population needs**	CSOs should lobby FR to designate one or multiple people to deal with PROACTIVE technology and supporting victims or potential victims in a CBRNe incident.	**#Preparedness**	• **CSOs** In collaboration with: • LEAs • First responders
✓ **Engage in public-private partnerships to implement PROACTIVE CCS**	CSOs should engage in public-private partnerships and dialogues that increase the consideration paid by FRs to vulnerable groups in PROACTIVE technology preparedness, training, and communication activities. CSOs should also advocate for developing common awareness and educational programs aimed implementing the app at the local and national levels and support the training efforts of FRs in field exercises testing this technology.	**#Preparedness**	• **CSOs** In collaboration with: • LEAs • Local authorities
✓ **CSOs should promote training supporting PROACTIVE App**	CSOs should boost formal and informal educational programs aimed at providing technological skills for vulnerable populations so they can use PROACTIVE in times of disaster. Moreover, developing the app management skills should be part of protocols promoted by CSOs, so they are implemented by both FRs and local authorities.	**#Preparedness**	• **CSOs** In collaboration with: • LEAs • Local authorities

✓ **CSOs should promote public use of the app as part of their CBRNe awareness campaigns**	CSOs should foster campaigns to push public authorities to finance the production and dissemination of the PROACTIVE app and its associated safety protocols. CSOs should lead their target audience into pedagogical and awareness activities using the app. This can facilitate the exchange of practices and procedures to protect vulnerable groups effectively in emergencies. CSOs should activate policies oriented towards fostering public authorities and FRs to use an evidence-informed and App based approach to assist vulnerable populations in reducing initial distress and facilitating short- and long-term adaptive functioning.	**# Preparedness** **# Post event**	• **CSOs** In collaboration with: • LEAs • Local authorities
✓ **Post event evaluation collected when using the PROACTIVE app should be used as pedagogical tools by CSOs**	CSOs should contribute to the spread of information provided by clinicians and other experts (including specialized first responders) on infection control and post-event disease transmission among the general public by using the PROACTIVE App. Communication should aim to influence the perceived efficacy of recommended behaviours. Information should be tailored to local communities and their respective relevant groups and contain facts or proof to provide robustness.	**# Preparedness** **# Post event**	• **CSOs** In collaboration with: • LEAs

6.5 Relational approach to the systems management policy

Besides the above efforts to be made by end users and policymakers to achieve proper coordination, standardization and interoperability of PROACTIVE, efforts must be made to ensure interagency implementation of such protocols. This includes:

- When using the PROACTIVE system in operational and emergency processes, LEAs, first responders and policy makers should clearly record and communicate the CCS inter agency governance. The system standard methodology led by the LEA in charge should be broken into stages and identifies specific objectives, metrics and control points showing converging goals for all stakeholders.
- The development of a national PROACTIVE CCS management glossary for ensuring the deployment under a common terminology, also consistent with EU standards.
- Common data definitions should be used, consistent with regional and international standards. Data composition stored in PROACTIVE datasets must be configured across agencies and in a manner aligned with EU standards. For instance, incidences recorded in each CBRN incident database or associated authorities' data should be reported in a common language.
- Moreover, depending on the scalability of the PROACTIVE CCS implementation process, a regional/national database may be structured to share critical data and foster interoperability with other national systems.
- LEAs must foster interoperability by federating the PROACTIVE CCS together with existing security and logistic software. These digital tools can also be used by national agencies conforming to national, regional and international standards.
- Specifications for procurement of the PROACTIVE CCS should be reviewed and approved by an inter-agency team. Moreover, the PROACTIVE interagency team should detect domains where existing software is not interoperable and develop a plan for addressing this limitation.
- A last inter-agency human resource standard process should be in place concerning PROACTIVE CCS training and inter-agency security standards. All personnel involved should be trained to meet national CBRN objectives.



Source: own elaboration.

Figure 3. Interagency main standardization and scalability factors

6.5.1 The alignment of PROACTIVE Crisis Communication System and the EU Security Agenda

In terms of the alignment of PROACTIVE with the EU Security agenda, the policy-making toolkit for the overall **management of the PROACTIVE platform and app** has been driven by scalability, modularity and interoperability mechanisms. Furthermore, its exploitation-oriented design for LEAs and policy makers reflects the work accomplished in terms of privacy.

The alignment between PROACTIVE CCS and the EU Security Agenda is embedded in the European legal and policy framework, starting with the Lisbon Treaty. In addition to focusing on the principles of "shared internal competences" (Article 4 TFEU), it should also focus on clearly defined **coordination activities and cooperative efforts** between European and external countries. In light of the late creation of a European crisis management framework in the 70's, and the lack of a unified approach to enhance societal preparedness and response policies to CBRNe events and integrate vulnerable group's need, it is required a coordinated and comprehensive approach to dealing CBRNe events.

In addition, security understandings are evolving and challenging. Hence, as the new Security Union strategy points out, the security ecosystem spans the entire breadth of European

society, whether in terms of CBRN events, terrorism, organised crime or corruption, or new digital challenges. To combat these challenges, it is necessary to assume that security is a shared responsibility. Thus, a plurality of actors, from governmental and commercial bodies, social organisations, institutions and citizens, must work together as in the PROACTIVE CCS development. Once the system is implemented, continuing this approach requires a range of **stakeholders working to the same standards**, albeit adapted to each state context, and having at their disposal a database with information on past events. Although experiences differ according to the type of CBRN and event and its context, the **knowledge generated in the recovery phase is of great value** and should be collected in good practices to promote societal preparedness and response policies in potential future events. Following the premise of the EU Security Agenda, according to which even a basic knowledge of security threats and how to combat them can have a real impact on society's resilience, PROACTIVE CCS is an fitting example.

Thus, the PROACTIVE CCS is a technology capable of being a **clearly defined role-based communication channel** to connect these actors further, to update information on the challenges posed by CBRNe events, and to provide a clear and concise overview and evolution of the CBRNe events. Indeed, following the EU Security agenda approach, **data protection principles** are being complied with both by design and by default.

In addition, the EU strategy points to the importance of understanding an **open strategic autonomy for supply chains** in terms of critical products, services, infrastructure, and technologies. Indeed, one of the priorities for protecting key EU and national digital assets is to offer critical infrastructures a channel for secure communications. While the Internet offers new potentials to elaborate, implement, and correct a common and up-to-date security strategy, it is also subject to cyber incidents and malicious activities online. The scale and diversity of hybrid threats today are also unprecedented. While a coordinated and cooperative approach is necessary also outside the European borders, because of the threats that cross physical and digital spaces, the development of PROACTIVE technologies against CBRNe events leads to a **decrease in their previous dependency.** To this end, more investment in research and innovation is required, as well as the deployment or reinforcement of basic internet infrastructure and resources. In line with the commitment set out in the European security agenda with the cooperation of the Intelligent Services, EU INTCEN and other security organisations, to maximise efforts to improve cyber security, combat terrorism, extremism, radicalisation and hybrid threats, PROACTIVE CCS can be a driver of change in the face of CBRNe events at the EU level.

In the framework of a solid European security ecosystem, where all parts of society should be engaged, equipped and connected for preparedness and resilience to security threats, thanks to technologies such as PROACTIVE, it is vital to highlight **the inclusiveness of the most vulnerable groups**. Thus, as an expression of European values, inclusivity must be at the heart of security responses, as well as of adjacent technologies. In the case of PROACTIVE

CCS, the focus is on the needs of vulnerable groups, without re-victimising their capabilities. After involving a wide range of actors during the development of the Toolkit for CBRNe Practitioners and civil society organisations, it has become clear that we need to not only commit to working on the inclusivity of security policies but also to continue to improve them in line with the changing needs of vulnerable groups and adapted to their respective contexts.

In this way, among goals and principles embedded in the EU Security strategy, PROACTIVE solutions contribution can be seen as:

- Better coordination between CBRNe stakeholders
- Risk awareness for social actors
- Enhanced training of first responders
- Contribution to CBRNe response technological resources
- Accessibility and inclusion of disadvantaged or vulnerable groups

These points coincide with the concrete work streams set out by the Security Union strategy to make progress around the following common objectives: building capabilities and capacities for early detection, prevention and rapid response to crises, focusing on results by a performance-driven strategy, and linking all players in the public and private sectors.

7. CONCLUSION

The present Deliverable presents a policy-making toolkit for the secure, coordinated and efficient use of the PROACTIVE app and web platform. It is based on a methodology consisting of an in-depth review of all relevant project deliverables, together with scientific literature and interviews with technical partners in charge of technological development in WP4. Moreover, lessons learned from Dortmund and Rieti's exercises and preliminary elements from Campus Vesta fieldwork are reflected in the guidelines and recommendations described. The three Policy briefs and Guidelines annexed to this document have been developed since 2021 to facilitate the ongoing development of this toolkit. They put together lessons learned from PROACTIVE research in the form of recommendations for relevant stakeholders, including LEAs, policy-makers and Civil Society Organizations, respectively.

As shown in the introductory sections, the PROACTIVE app and web platform fit within current gaps in CBRNe policies in Europe, primarily associated with the complexity of CBRNe events challenges in the current digital and globalized scenario and with the need for training, public awareness and interagency coordination before, during and after these events. After setting this scenario in Section 3, the Deliverable provides a summarised description of the PROACTIVE solutions aimed at offering information to citizens, focusing on vulnerable populations accessibility, and providing a platform for LEAs and other authorities to handle CBRNe scenarios in terms of knowledge spreading and intergovernmental action. The systems are analyzed in terms of their data governance process (compliant with the existing regulations), functionalities, expected goals, data management, data security by design and users' profiles. After to further framing the guidelines development from a legal and acceptability standpoint in Section 4, this document introduces the EU security policy and primary normative documents shortly in the CBRNe domain to examine the relative alignment of PROACTIVE technology with their philosophy and goals.

The above, together with the systematization of information collected through the above-detailed methodology, allowed us to put together a set of main recommendations for managing PROACTIVE technology in compliance with data protection, acceptability and ethical principles. Section 6 organizes these recommendations according to each phase of CBRNe events, each type of stakeholder involvement and taking into consideration the specific technology at stake (apps/platform). Lastly, under these coordinates, the relationships between first responders, policymakers and civil society organizations taking part in using PROACTIVE systems are synthesized, focusing on interoperability dimensions. In this way, although more elements extracted from Campus Vesta and ongoing analysis of the PROACTIVE CCS final prototype to be included in D4.2 and D4.3 (M52) will be reflected in D8.4, this document provides an overview of lessons learned and best practices concerning the deployment of the PROACTIVE app in real scenarios.

8. REFERENCES

Alshehri, S.A., Y. Rezgui, and H. Li. (2016). Public perceptions and attitudes to biological risks: Saudi Arabia and regional perspectives. Disasters. 40(4): p. 799-815.

Arrivillaga, M., & Delaney, P. (2009). The Subway Sarin Gas Attack—a Historical Perspective. *Joint Center for Operational Analysis Journal*, *11*, 8-9.

Becker, S.M. (2004). Emergency communication and information issues in terrorist events involving radioactive materials. Biosecurity and bioterrorism: biodefense strategy, practice, and science, 2(3): p. 195-207

BESECU (2011). Final Report Summary - BESECU (Human behaviour in crisis situations: A cross cultural investigation to tailor security-related communication).

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

Bunker D, Mirbabaie M, Stieglitz S. (2017).”Convergence Behaviour of Bystanders: An Analysis of 2016 Munich Shooting Twitter Crisis Communication”. In: *Proceedings of the Australasian Conference on Information Systems*.

Carter, H., et al. (2018). “Public perceptions of emergency decontamination: Effects of intervention type and responder management strategy during a focus group study”. *PLoS* One. 13(4): p. e0195922

Chatfield, S.N. (2018). *Member States’ Preparedness for CBRN Threats*. Brussels: European Parliament.

Chen, Jing; Diana Wilkinson, Richard B. Richardson, Barbara Waruszynski (2009). “Issues, considerations and recommendations on emergency preparedness for vulnerable population groups”, *Radiation Protection Dosimetry*, 134, 3-4,132–135, https://doi.org/10.1093/rpd/ncp083

Coleman, C. N., Bader, J. L., Koerner, J. F., Hrdina, C., Cliffer, K. D., Hick, J. L., ... & Hatchett, R. (2019). “Chemical, biological, radiological, nuclear, and explosive (CBRNE) science and the CBRNE science medical operations science support expert (CMOSSE)”. *Disaster medicine and public health preparedness*, *13*(5-6), 995-1010.

Department of Homeland Security (2014). *Patient decontamination in a mass chemical exposure incident: national planning guidance for communities*.

European Parliament (2019), ‘Workshop report: EU preparedness against CBRN weapons’ at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603875/EXPO_STU(2019)603875_EN.pdf.

Frulli, M. (2022). “The Challenge of Outlining the CBRN Definitional Framework”. In *International Law and Chemical, Biological, Radio-Nuclear (CBRN) Events* (pp. 3-14). Brill Nijhoff.

Gavel, A., Kroupa, T., Navrátilová, L., Setnička, M., Clutterbuck, L., Petersen, L., ... & Arnold, A. (2022). Deliverable D2. 4.

Gouweloos, J., Dückers, M., Te Brake, H., Kleber, R., & Drogendijk, A. (2014). Psychosocial

care to affected citizens and communities in case of CBRN incidents: a systematic review. *Environment international*, *72*, 46-65.

Guberek, T., A. McDonald, S. Simioni, A.H. Mhaidli, K. Toyama, and F. Schaub. (2018). Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 114:1–114:15. New York, NY: CHI.Borking J and Raab C (2001). 'Laws, PETs and Other Technologies for Privacy Protection', Refereed article, The Journal of Information, Law and Technology (JILT), (1).

Havârneanu, G. M., Petersen, L., Arnold, A., Carbon, D., & Görgen, T. (2022). Preparing railway stakeholders against CBRNe threats through better cooperation with security practitioners. *Applied Ergonomics*, *102*, 103752.

Havârneanu, Grigore M.; Laura Petersen; Natasha McCrone (2023). "Stakeholder Engagement Model to Facilitate the Uptake by End Users of Crisis Communication Systems," in Security Technologies and Social Implications, *IEEE*, 2023, pp.198-221, doi: 10.1002/9781119834175.ch8.

Hignett, S., Hancox, G. and Edmunds Otter, M. (2019), "Chemical, biological, radiological, nuclear and explosive (CBRNe) events: Systematic literature review of evacuation, triage and decontamination for vulnerable people", International Journal of Emergency Services, Vol. 8 No. 2, pp. 175-190.

Jean-Luc Marret, J.B., Helma van den Berg, Anke van Gorp, Dianne van Hemert, Liliana Leone, Rozetta Meijer, Richard Warnes, Ron Van Wonderen (2017). Final report providing background for using and further developing the validated toolkit IMPACT Europe. D6.2.

Kapucu, N., & Özerdem, A. (2011). *Managing emergencies and crises*. Jones & Bartlett Publishers.

Koblentz, G.D. (2020). 'Emerging Technologies and the Future of CBRN Terrorism', The Washington Quarterly, 43(2): 177-196.

London, N. (2010). *Exercise MILO report: Disability and Decontamination*. London: Health Protection Agency.

McDonald, N., Forte, A. (2022). Privacy and Vulnerable Populations. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (eds) Modern Socio-Technical Perspectives on Privacy. Springer, Cham.

Moats, J. B. (2007). *Agroterrorism: A guide for first responders* (No. 10). Texas A&M University Press.

Rimpler- Schmid, Alexandra; Ralf Trapp Sarah Leonard, Christian Kaunert, Yves Dubucq, Claude Lefebvre, Hanna Mohn (2021). EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats, Brussels: European Union.

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

Scottish Government., Nuclear emergency planning and response guidance. 2015.

Taliaferro, L. P., Cassatt, D. R., Horta, Z. P., & Satyamitra, M. M. (2021). A Poly-Pharmacy

Approach to Mitigate Acute Radiation Syndrome. *Radiation research*, *196*(4), 436-446.
TOXI-TRIAGE, Messages for clear and compelling communication during crises management, D8.5, 2019.
Venkatesh, V.; Morris, D. (2003). “User Acceptance of Information Technology: Toward a Unified View”, *MIS Quarterly*, 27(3): 425-478.
Wilkinson, D. (2009). Dealing with at-risk populations in radiological/nuclear emergencies. *Radiation protection dosimetry*, *134*(3-4), 136-142.
World Health Organization. (2011). Asia Pacific Emergency and Disaster Nursing Network Meeting and the Third International Conference on Disaster Nursing, Seoul and Daejeon, Republic of Korea, 21-24 October 2011: An All-Hazards Preparedness Approach to Disasters: report.
Yoshida, M., et al., 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, 2016. 155-156: p. 7-14.
Zack, N. (2009) Ethics for Disaster, Cambridge Scholar Publishing, Newcastle upon Tyne, UK.

9. ANNEX: POLICY BRIEF AND GUIDELINES

Annex 1. CBRNe toolkit for policy makers: integrating vulnerable groups in preparedness and response[14]

Summary

EU Member States lack a clear and coordinated approach to enhance societal preparedness and response to CBRNe (Chemical, Biological, Radiological, Nuclear and explosive) events that integrate the needs of vulnerable individuals. Based on preliminary results from the EU H2020 funded PROACTIVE project (Preparedness against CBRNe threats through cOmmon Approaches between security praCTItioners and the VuleranblE civil society), this policy brief recommends that EU policy makers should facilitate the development of coherent, evidenced-based guidance documents that include the needs of vulnerable citizens in three stages (before, during and after the event):

- **Before CBRNe events**, policy making should focus on enhancing preparedness by educating people and raising public awareness with culturally appropriate, accessible information using multiple modes of dissemination and languages (e.g., pictograms, sign language). Attention to protected groups should be paid. Policy makers should also ensure uniformity among guidance documents and integrate information on the needs of vulnerable groups.
- **During CBRNe events** policy makers should increase resilience toward misinformation and coordinate action of the practitioners involved in CBRNe response. Moreover, policy making should focus on ensuring that communication strategies implemented by first responders are effective, up to date, trustworthy, evidence-based, and consider vulnerable citizens' needs.
- Policy making in **post CBRNe events** should favour the undertaking of post-event evaluation taking differential impact on vulnerable populations into consideration. Communication and ICT technologies used in CBRNe events should undergo assessment in order to enhance existing tools and methods.

Problem

Many major cities across Europe have faced critical CBRNe related incidents over the past few decades[15]. Furthermore, with terrorism threat levels high across the continent, the use of chemical agents by terrorist organizations has shown to be a significant risk (EUROPOL, 2019). Vulnerable individuals, such as people with mental or physical disabilities, older adults or children, are particularly exposed in this scenario. Preparation and response to CBRNe incidents based on equal treatment require designing and implementing policies targeted to vulnerable populations. First responders and CBRNe practitioners need clear, context-adaptable and well-structured guidelines and technologies to ensure their duties' efficacy. However, the literature has underlined the need for intergovernmental coordination in Europe

[14] Eticas Research and Consulting. Authors: Mariano Martín Zamorano & Francesca Trevisan.

[15] Examples include the two explosions and a gas leak at a chemical plant south of Rotterdam or the chemical accident at a factory in Igualada (Spain) in 2015, which injured three people and cloaked large swathes in an orange chemical cloud, forcing over 60,000 people to stay indoors before it disappeared.

and harmonising response actions to ensure their efficiency (D1.1, D1.2). Moreover, policies and solutions are often limited in their capacity to integrate vulnerable groups behavioural and accessibility factors, which are relevant for ensuring fast and precise response.

Background study results

Current Situation

1. **Public understanding** of CBRNe prevention and management strategies is very low.
2. Emergency responders' guidance and training often continue to endorse outdated and discredited **assumptions about crowd behaviour** (e.g., mass panic, public disorder) that focus on controlling rather than communicating with people.
3. There are **discrepancies in CBRNe policies and guidance documents** within and between EU countries.
4. There is extremely limited focus placed on **managing the needs of vulnerable** groups.

Factors influencing public compliance

5. **Prior knowledge** has been identified as a factor in increasing public compliance with recommended preventative measures. Further, information available to the public **during an incident**, regarding why and how they should comply, increases the level of compliance shown.
6. **Trust in both spokesperson and source** are associated with increased compliance during an event, with an apparent preference for local sources over governmental or official communication. Trust, provision of information and emotional responses, can increase compliance with official instruction during incidents.
7. **Demographic characteristics** including gender, location and level of education affect the rate of compliance with preventative measures in relation to CBRNe incidents.
8. Public compliance with recommended preventative methods may be affected by the **emotions associated with CBRNe incidents**. Self-efficacy, response-efficacy and the ability to cope with the situation are all associated with how much agreement would be shown by the public.
9. The **desire to seek out loved ones** during an incident and ensure their safety significantly affects public willingness to comply with protective measures.

Issues and recommendations

The role of policymakers for CBRNe preparedness and response is to facilitate and boost practitioner's performance. This section identifies vital aspects to consider in this regard based on PROACTIVE preliminary results. Recommendations are organized according to the three critical stages of intervention, **preparedness, response and post-event recovery**. For each addressed issue we indicate the related PROACTIVE deliverables are linked to related issues and recommendations.

1. Policy making in CBRNe incidents preparedness

Institutions involved in CBRNe preparedness must provide the technical and organisational **means for the implementation of CBRNe policies and tools**.

Issue	How to tackle	Action point for Policy Makers
#1 A legal and policy framework that effectively defines roles and responsibilities of all CBRNe	*Policies and procedures should facilitate normative clarity and inter-agency collaboration in line with*	**#1** Policy makers must develop networked and coordinated procedures defining roles and responsibilities of CBRNe practitioners (D2.5).

practitioners is lacking (D8.1).	*DECISION (EU) 2018/199 and Rimpler-Schmid (2021).*	
#2 General public understanding of CBRNe prevention and management strategies is shallow (D1.1). Communication pre CBRNe event is vital for a successful outcome (D1.2, D5.1).	*Pre-incident public info campaigns for CBRNe terrorism should be characterized by being easy to understand with the use of non-complex language, disseminated across multiple platforms, delivered by a credible source. This is vital to ensure the public is aware of pre-incident information and campaigns.*	**#2** Policy makers should put their effort into educating people on CBRNe events and raising awareness of their implications for vulnerable populations. Pre-incident information must be culturally appropriate, easy to understand and factual (D1.1). Guidance and policy should be updated to incorporate a detailed communication strategy for how emergency responders should communicate with casualties and members of the public during a CBRNe incident (D1.2).
#3 Guidelines are based on traditional and not up to date crowd behaviour data (D1.1).	*Policy makers should facilitate ongoing and interdisciplinary analysis and research on crowds' management. They should also facilitate resources to integrate this information into CBRNe preparedness tools.*	**#3** Guidance and policy should benefit from incorporating up-to-date evidence-based advice on how members of the public are likely to respond in a CBRNe incident, including psychosocial factors (D1.2). In addition, communication must incorporate psychological constructs that aim to reduce threats and anxiety (Havârneanu et al, 2022) and provide emotional and rational appeal while clearly communicating threats and explaining to citizens how to proceed accordingly (D1.1).
#4 To maximize public engagement it is essential that these are pitched at an appropriate level to ensure the public can ensure maximum engagement with the material (D1.3).	*Messages should be pitched at an appropriate level in terms of language and complexity.*	**#4** It is recommended to adopt layman's terms in regards to language and complexity and integrate them into preparedness policy materials (D1.3).
#5 The public prefers written communication due to its concrete nature and the fact that it can't be retracted once provided (D1.3).	*Information should be available in writing (i.e., print form), where possible, using non-complex language.*	**#5** Policy makers should ensure that, where possible, information is available in writing using non-complex language (D1.3).
#6 Information should be pre-planned in order to ensure prioritization and consistency between organizations, provide uniformity and advocate cohesion between agencies and work practices (D1.3).	*Pre-planned information addressing all potential scenarios must be the strategic approach.*	**#6** Policy makers must facilitate pre-planning between agencies and organizations to ensure consistency (D1.3).
#7 Guidance and recommendations are not necessarily consistent, even within countries (e.g.,	*Guidance documents should seek to be uniform in instruction, particularly when released in the same country.*	**#7** Policymakers should improve overall response by sharing uniform instruction materials, plans and best practices (i.e. in the form of hypothetical scenarios) to

decontamination duration) (D1.2, D1.3)		achieve a consistently high level of preparedness in their territory/ power domain (D1.3, D2.4).
#8 There is a need for a greater focus placed on managing the needs of vulnerable groups in guidance documents to ensure that the needs of these individuals are met (D1.1, D1.2, D1.3, D2.5, D3.4).	*Producing new official materials and standards on preparation actions for preventing and managing harm on vulnerable populations in CBRNe events.*	**#8** Guidance and policy should include a clear strategy on how to manage vulnerable groups in a CBRNe incident. This includes both communication and response plans adapted to these groups (D1.2, D3.3). Policy and guidance should ensure that response strategies meet the needs of vulnerable groups without placing them at a disadvantage because of their vulnerability (D1.2, D3.3).
#9 There is a need to ensure equal treatment and maximum public engagement with information (D1.3) .	*Information should be provided in multiple languages, pictographic form, and sign language.*	**#9** Where possible, information should be fully accessible for all (e.g. in terms of language and format) (D1.3).

2. Policy making in CBRNe incidents response

Public institutions' role regarding response protocols during a CBRNe event is to intervene in incident **communication, ensure technical availability, and often coordinate the practitioners** involved. Other relevant tasks include support for family reunification. Coordination between different stakeholders (first responders, LEAs, etc), including those related to vulnerable populations (e.g. social services and civil society organisations), is crucial for the effectiveness of the response strategy.

Issue	How to tackle	Action points for Policy Makers
#1 Communication employed does not take into account evidence-based recommendations for inclusive crisis communication (D1.1, D1.2, D2.2, D3.4).	*Apply existing recommendations such as the ones mentioned in the COVINFORM-PROACTIVE Whitepaper.*	**#1** Ensure CBRNe guidance documents comply with the evidence-based crisis communication recommendations.
#2 There is a need to ensure first responders can meet the needs of minority groups in the context of a CBRNe incident (D2.5).	*Policies and procedures for managing CBRNe incidents should remain culturally appropriate and be respectful of religious values.*	**#2** Policy makers must foster institutional action to ensure that CBRNe management adequately addresses cultural factors (i.e., language barriers) (D1.3).
#3 There is a need to ensure that first responders can meet vulnerable groups' needs, as both guidance and literature contain limited information about the management of members of vulnerable groups during CBRNe incidents (D1.1, D1.2, D2.2, D3.4).	*Guidance documents should inform responders about the needs of vulnerable groups and include plans for dealing with such groups in the case of a CBRNe incident.*	**#3** Policy makers must develop strategies to incorporate information and protocols relating to the needs of vulnerable groups and implement plans for dealing with such groups in the case of a CBRNe incident. This includes mechanisms to ensure safety for vulnerable populations (i.e. persons with physical disabilities) (D1.3, D2.2, D3.3).

#4 There is a lack of consideration in current policy and practices for supporting animals (D1.3, D2.2).	*Policies and procedures for managing CBRNe events should include plans on how to deal with support animals.*	**#4** Policy makers must implement procedures and coordination strategies with corresponding agencies for dealing with support animals in case of CBRNe events (D1.3, D2.2).

3. Post CBRNe incidents policies

The role of public institutions in the recovery from a CBRNe event is to perform continuous policy assessment and ensuring that the lessons learnt are actively applied in all guidance and policy documents.

Issue	How to tackle	Action points for Policy Makers
#1 There is a general lack of post-event evaluation and analysis by official institutions beyond LEAs and practitioners (D8.2).	*Evaluation of CBRNe policies must take from incident response experience to further enhance existing tools, policies and methods.*	**#1** Produce support strategies for first responders and civil society organizations to address post-event mitigation strategies, including communication with the media. Tabletop exercises, focus groups, and workshops with LEAs' and civil society organizations' participation should be coordinated by public institutions. Issues limiting the applicability of guidelines used in specific cultural contexts, such as linguistic barriers or the implementation of decontamination protocols for some religious groups, should be discussed in these meetings (D8.2).
#2 Performance of communication and ICT technologies used by public actors in CBRNe events is not assessed (D8.2).	*Technological systems used for coordinating response scenarios should also be evaluated.*	**#2** Regularly assess CCS governance, including relations to all stakeholders involved, addressing LEAs, first responders, social organizations and the media. The CCS performance should be analysed in these sessions to integrate stakeholders' perceptions into technological toolkits and protocols.
#3 Low standardization and scalability in the PROACTIVE system (D4.4).	*The governance policy for the PROACTIVE system should foster its standardisation and scalability.*	**#3** Policy makers should support LEAs in PROACTIVE CCS standardization. The unit overseeing the system should promote the creation of a list of areas demanding conformance to national, regional and international standards, including the potential use of the CCS in other regions of the MS. Action plans, including a timetable and responsibilities for this task, must be in place (D4.4).

Conclusion

We have found that public understanding of CBRNe events preparedness is low and that there are discrepancies on CBRNe guidelines between and within EU countries' policies. Furthermore, there is a lack of focus on vulnerable people. Building on our findings, we recommend that EU countries consider **adopting standard high-level policy documents**

and guidelines. These instruments should guide CBRNe stakeholders on how to effectively communicate, act, coordinate themselves and deal with the needs of vulnerable citizens pre, during and post CBRNe events. To achieve this, **we recommend that policymakers provide capacity to allow CBRNe public management** to be based on up-to-date evidence, integrate cultural and psycho-social factors, identify vulnerable citizens' needs, and build resilience toward the misinformation. Furthermore, **a post-event systematic assessment** would favour an iterative policy process that would, in turn, guarantee efficient and up to date practices. One of the outstanding challenges is the coordination of the action between different stakeholders involved in the management of CBRNe events. To address this, national governments could establish a forum where civil societies, LEAs, and other practitioners involved in CBRNe events regularly engage with each other on issues and practices.

Limitations

Since the PROACTIVE project is ongoing, these are preliminary results and are likely to be updated in the future.

Acknowledgements

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

References

EUROPOL (2019). European Union terrorism situation and trend report (TE-SAT). https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat

Havârneanu, G. M., Petersen, L., Arnold, A., Carbon, D., & Görgen, T. (2022). Preparing railway stakeholders against CBRNe threats through better cooperation with security practitioners. Applied Ergonomics, 102. https://doi.org/10.1016/J.APERGO.2022.103752

Rimpler-Schmid, Ralf et al. (2021). EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats. European Parliament.

Note: to know more about the PROACTIVE referenced deliverables please visit https://proactive-h2020.eu/ .

Disclaimer: The views expressed in this publication are those of the author/s and should not be attributed to all PROACTIVE project partners or the European Commission.

Annex 2. Protecting Children in CBRNe Incidents: Guidelines for Civil Society organizations

Summary

EU Member States lack an approach to enhance **societal preparedness and response policies to CBRNe** (Chemical, Biological, Radiological, Nuclear, and explosive) events that integrate the **needs of children**. Based on preliminary results from the EU H2020 funded PROACTIVE project (Preparedness against CBRNe threats through cOmmon Approaches between security praCTItioners and the VulnerablE civil society), these **Guidelines for Civil Society Organisations (CSOs) working with children** recommend developing solid and long-term collaboration between First Responders (FR) and CSOs and facilitating the advance of coherent, evidenced-based emergency procedures that address the management of children in three stages: before, during and after the event. With this aim in mind, the document provides critical recommendations for CSOs working with minors[16] to promote their safety in these situations.

Problem

Many major cities worldwide have faced critical CBRNe-related incidents over the past few decades[17]. Furthermore, with terrorism threat levels high across the EU, using chemical agents by terrorist organisations has shown to be a significant risk also in European soil (EUROPOL, 2019)[18]. In this scenario, children[19] are a vulnerable group that could be at higher risk in CBRNe events, as was determined in cases such as the chemical weapons attack in Douma, held by the Syrian Regime in 2018, which left at last 90 people dead, 30 of them children[20].

Systematic information about children's needs, behaviour and forms of interaction in some of these situations is lacking. All involved stakeholders, including FR -such as public health officials, emergency management personnel, or even clinicians-, public authorities and CSOs may need to better comprehend children's unique characteristics and requirements in such situations.

Children are different from adults physically, developmentally, and socially and it can be challenging to abide by the existing regulations, offer caregivers the information they need to grant informed consent, and attempt to optimise medical countermeasures coverage in a pediatric population during a major incident.

[16] The main scope of CSOs within this domain is to keep kids safe, healthy, and educated concerning disaster scenarios. For example, Save the Children Emergency response programs focusing on assisting children in crises (https://www.savethechildren.org/us/what-we-do/emergency-response)

[17] Examples include the explosion of a large amount of ammonium nitrate stored at the Port of Beirut (2020) which killed 220 people, instantly injured over 6,500 more, and severely damaged the densely populated residential and business districts nearby (Al-Hajj et al., 2021) or the ongoing Covid-19 pandemic (2019 - 2023). One well- known case in Europe is a Tunisian couple's attempt to attack with ricin in Cologne, Germany, using an improvised explosive device.

[18] It should be noted that no major CBRNe attack involving children has occurred in the EU and attacks in the West have dramatically decreased since their peak in 2018, falling by 68% in 2021 (OCHA, 2022).

[19] For the European Union, as laid down in the UN Convention on the Rights of the Child (UNCRC), a child is any human being below the age of 18, but regulations have different declinations in every country. Ethics requirements for exercises carried out under the PROACTIVE project followed the regulations of the specific countries in which the exercises took place.

[20] See: https://www.reuters.com/world/middle-east/syria-gas-attack-victim-awaiting- justice-say-impunity-fuels-war-crimes-2022-04-10/

A pathway for a protecting children

To properly account for children, professionals in the disciplines of public health, disaster preparedness, and clinical treatment must have a thorough understanding of their vulnerabilities. These Guidelines for CSOs are linked to the PROACTIVE Policy Brief (action point 1/section 3) and offer a systematic account of the type of contribution CSOs can make in three phases of children protection, CBRNe preparedness, response, and recovery management.

All CBRNe authorities must identify their relevant stakeholders to make them part of policy design and implementation. These Guidelines are expected to be disseminated among CSOs that are relevant to CBRNe situations so that decision-makers can encourage them to engage in CBRNe preparedness, training and communication activities. These Guidelines represent the other side of the stakeholder management approach in this process since they offer tools to prepare CSOs for the CBRNe contexts.

Issues and recommendations

One role CSOs could play in CBRNe scenarios would be to foster and improve communication between FRs and the public. Based on PROACTIVE preliminary results and the literature, this

section identifies vital aspects to consider when dealing with children. Recommendations are organized according to the three critical stages of intervention, preparedness, response, and recovery. For each point we indicate the related PROACTIVE deliverables and recommendations.

Children's management in CBRNe incidents preparedness

Issue	How to tackle by CSOs	Action point for CSOs
#1 Children are often invisible in CBRNe policies and protocols: The need to include children's conditions in civil protection planning has been identified (Save the Children Italy, 2020).	CSOs should aim to develop a culture of prevention and response and dissemination of knowledge concerning emergencies that promotes an active role for children and adolescents. This will be highly beneficial as they will hopefully also transfer the information to their family.	**#1** CSOs should engage in public-private partnerships and dialogues that increase the consideration paid by FRs to children in CBRNe preparedness, training, and communication activities. To achieve this, CSOs could engage in the lobby for inclusiveness and children's welfare in first responders' SOPs. CSOs should also advocate for developing common awareness and educational programs aimed at children to be implemented at the local and national levels and support the training efforts of FRs in field exercises (Save the Children Italy, 2020; D1.3).
#2 Pre-incident information and CBRNe education **could potentially increase worry**, especially for children, but this effect can be mitigated by helping citizens to understand why information is being shared (D1.3).	CSOs should partner with authorities and develop CBRNe awareness materials and curricula based on modern teaching methods (interactive, engaging etc.) to build children's resilience and skills for real life.	**#2** CSOs should foster campaigns to push public authorities to finance the production and dissemination of modern and engaging educational materials about CBRNe scenarios and safety protocols adapted to children's needs (D3.4).
#3 Communication materials for children **should be prepared in advance** (D3.4).	CSOs should implement specific and diversified communication strategies for reaching children.	**#3** CSOs should consider e-mails, online newsletters, and their websites and social media channels for contacting members of civil society and providing them with CBRNe-related material to be shared with children. In general, Instagram, Facebook, YouTube, and WhatsApp seem to be particularly suitable for them (D3.4).
#4 Close cooperation agreements should be established between CSOs and FRs' organisations (D6.4).	CSOs should approach and lobby first responders, central and local authorities, and community representatives and establish cooperation platforms with them.	**#4** CSOs and FR should sign Memorandums of Understanding or Cooperation Agreements with respect to children's involvement in CBRNe prevention actions, joint education programmes, training exercises, etc. (D6.4).

Children's management in CBRNe incidents response

Issue	How to tackle by CSOs	Action point for CSOs
#5 Protection issues in evacuation centres and camps: children exhibit that can exacerbate their risk of adverse health effects during CBRNe disasters. These behaviours may all contribute to an **increased risk of physical exposure** to agents, toxins, and other hazards (Bartenfeld et al., 2014).	CSOs should cooperate with FRs to promote practices and procedures which FRs can develop and implement to effectively protect children in emergencies (Save the Children Italy, 2020).	**#5** CSOs should lead their target audience into training and collaboration with FRs so that they can assume these pedagogical and awareness activities. This can facilitate the exchange of practices and procedures to protect children effectively in emergencies. Moreover, as part of this collaboration with authorities and FRs, CSOs should promote that children have a delimited area, dedicated services (WC, mother, and baby areas), and a strategic position in the reception areas of event sites (Save the Children Italy, 2020).
#6 Limited communication: depending on age and development, children may not have the communication skills, motor skills, or judgement to effectively move toward safety in a dangerous situation (Bartenfeld et al., 2014).	CSOs should collaborate with FRs to encourage them to assume communication that is effective and immediate.	**#6** CSOs should lobby FR to designate one or multiple people to deal with children that are victims or potential victims in a CBRNe incident. They should also promote that FR avoids using acronyms, familiarise themselves with the technical language children understand and keep the language simple and clear (Havârneanu et al, 2022), prepare a glossary of critical terms for children, and make use of audible material, pictorial language, and colours (Mor & Waisman, 2002). CSOs should also promote that the information is emphasised through body language. This may take the form of age or disability-adapted language and messages (for example, if the child has some hearing impairment)[6]. Accordingly, CSOs must lobby FR so that all information within the hot zone is presented in a large format and positioned in easily visible locations, preferably in the waiting area before the decontamination tent. The positioned height should also be taken into account (D3.4).

Children's management in CBRNe incidents response

Issue	How to tackle by CSOs	Action point for CSOs
#7 Children may react with rigidity or escape tendencies in the event of an evacuation and may not follow perfectly the instructions of FRs (D3.4).	CSOs should help teachers in preparing children for the basic elements of an evacuation process, for example through regularly trained fire alarms at school and informal educational methods focused on awareness and independence in critical situations.	**#7** CSOs should boost formal and informal educational programs aimed at providing a safe environment in which children can play, socialise, learn and express themselves in times of disaster (Save the Children Italy. 2020). Moreover, developing basic skills such as correctly evacuating, giving first aid, etc., should be part of protocols promoted by CSOs, so they are implemented by both FRs and local authorities.

#8 Children are dependent on caregivers, whether parents or others. Their dependence on caregivers to make **informed healthcare decisions** on their behalf creates challenges. Providing the necessary information to receive informed consent from caregivers and maximising Medical Counter Measures (MCM) coverage in a paediatric population during a large-scale event is difficult (Bartenfeld et al., 2014).	CSOs should cooperate with FRs to undertake measures that mitigate separation anxiety and its negative effects.	**#8** CSOs collaborate with FRs and authorities to develop policies and training programs to improve stakeholders' knowledge and ensure that children should be accompanied by a caregiver or supported by one designated caregiver when carrying out the undressing and decontaminating process if possible. In this context, CSOs should promote the availability of transitional objects (e.g., blankets, stuffed animals, etc.) for individual children. The "buddy system", consisting of children-pair operating together as a single unit, is also indicated in regard to unaccompanied children. This may make it easier for the caregiver to give informed assent (D3.4).
#9 Undressing and decontamination process: tensions have been identified concerning standard measures and their capacity to ensure children's privacy (D3.4).	CSOs should collaborate with FRs to encourage them to guarantee children's privacy at all times and minimise the shame as well as cultural/religious restrictions factors during the undressing and decontamination processes.	**#9** CSOs' contribution to training and CBRNe awareness should promote the availability of shielded areas where the undressed can wait. Those areas should be divided into male and female if possible. Another measure to be embedded into CSOs' awareness activities in their collaboration with public authorities is the need to guarantee physical privacy. For instance, shower boxes should be separated by gender, and emergency personnel who control the process being also of the same gender. Additional considerations for children after a chemical attack include their requirement for sized and adequate clothing after decontamination (D3.4).

Children's management in CBRNe incidents recovery

Issue	How to tackle by CSOs	Action point for CSOs
#10 Mental health and psychosocial support for children in CBRNe incidents recovery are **lacking** (Save the Children Italy, 2020).	CSOs should work towards ensuring mental health and psychosocial support for children in the immediate aftermath of CBRNe events. CSOs should also enhance their expertise to ensure that, when allowed by law, they can provide mental health and psychosocial support in a post-incident situation.	**#10** CSOs should activate policies oriented towards fostering public authorities and FRs to use an evidence- informed approach to assist children in reducing initial distress and facilitating short- and long-term adaptive functioning. This approach should not necessarily involve a discussion of the traumatic event but identify specific needs. In this framework, related workshops, meetings, or activities should also be designed and partnerships and activities with the professional associations of psychologists and psychiatrists, who have the necessary experience with trauma, can be used.

#11 Screening children for infection after they are exposed to biological pathogens is another challenge: young children may have **unusual presentations of diseases**. Young children may also have **difficulty describing symptoms**, particularly symptoms such as difficulty breathing, chest discomfort, muscle pain, nausea, and headache (Bartenfeld et al., 2014).	CSOs should cooperate with FRs and clinicians to spread basic knowledge about the importance of balancing an understanding of children's unusual presentations of diseases with a need to consider biological threat agents in the diagnosis.	**#11** CSOs should push the authorities to develop solid long-term strategies to support child victims of CBRNe incidents and their consequences. In this context, CSOs should contribute to the spread of information provided by clinicians and other experts (including specialized first responders) on infection control and post-event disease transmission among the general public (Bartenfeld et al., 2014).
#12 Potential lack of postevent evaluation collected when using the PROACTIVE app (D4.4).	CSOs should contribute to the spread of information provided by clinicians and other experts (including specialized FR, with the collaboration of LEAs'), on infection control and post-event disease transmission among the general public, and especially the children, by using the PROACTIVE App.	#12 CSO's contribution to communication should aim to influence the perceived efficacy of recommended behaviours. In this sense, PROACTIVE app should be used as pedagogical tools by CSOs should be tailored to local communities and their respective relevant groups, such as the children, and contain facts or proof to provide robustness (D4.4).

Closing remarks

These Guidelines integrated into PROACTIVE Policy Brief aim to provide CSOs, FRs, and CBNRe authorities tools for enhancing their coordinated action and governance in protecting children before, during, and after disaster events. The best practices to be considered in their contribution to children's safety are summarized as follows:

1. Before CBRNe events, CSOs working with children should focus on developing partnerships, communication/educational campaigns, and Memorandums of understanding with FR and CBRNe-related authorities. Efforts must focus on promoting a culture of prevention of emergencies that supports an active role for children.

2. Pre-event efforts made by CSOs should ensure smooth collaboration with authorities and FR during the disaster phase. This includes pedagogical, non-discrimination, and trauma mitigation measures (for example, through regularly trained fire alarms at school). Moreover, CSOs could cooperate with FRs to promote practices and procedures that FRs can implement to protect children in emergencies effectively, encourage them to assume effective and immediate communication, undertake measures that mitigate separation anxiety, and guarantee children's privacy at all times.

3. Finally, CSOs should engage in activities aimed at lobbying authorities to promote an evidence-informed approach to assist children's mental health as well as raise awareness about post- event treatment for children and contributing to the spread of

information through the Proactive App.

Limitations

The recommendations included herein may be updated without prior notice if the PROACTIVE consortium and other entities develop new standards and guidance.

As PROACTIVE is an ongoing project, more empirical work involving children is still expected to be produced.

References

Al-Hajj, S., Dhaini, H. R., Mondello, S., Kaafarani, H., Kobeissy, F., & DePalma, R. G. (2021). Beirut ammonium nitrate blast: Analysis, review, and recommendations. Frontiers in Public Health, 9. https://doi.org/10.3389/fpubh.2021.657996

Bartenfeld, M., Peacock, G., & Griese, S. (2014). Public Health Emergency Planning for Children in Chemical, Biological, Radiological, and Nuclear (CBRN) Disasters. Biosecurity And Bioterrorism: Biodefense Strategy, Practice, And Science, 12(4) 201-207. https://doi.org/10.1089/bsp.2014.0036

Carbon, D., Arnold, A., Siemens, M., & Görgen, T. (2021). Common approaches between the vulnerable members of the civil society. Deliverable D3.4 of the PROACTIVE project.

Davidson, L., Weston, D., Dennis A., Amlot, R., Carter H. (2021). Findings from systematic review of current policy for mitigation and management of CBRNe events. Deliverable D1.2 of the PROACTIVE project.

EUROPOL (2019). European Union terrorism situation and trend report (TE-SAT). https://www.europol.europa.eu/activities-services/main- reports/terrorism-situation-and-trend-report-2019-te-sat

Godwin T. et al. (2023). Report on the second field exercise and evaluation workshop. Deliverable D6.4 of the PROACTIVE project.

Hall C., Weston, D., Long, F., O'Sullivan, F., Amlôt, R., & Carter, H. (2020). Guidelines and recommendations for mitigation and management of CBRNe terrorism. Deliverable D1.3 of the PROACTIVE project.

Institute for Economics & Peace. Global Terrorism Index 2022: Measuring the Impact of Terrorism, Sydney, March 2022. Available from: http://visionofhumanity.org/resources (accessed 10 January 2023).

Havârneanu, G. M., Petersen, L., Arnold, A., Carbon, D., & Görgen, T. (2022). Preparing railway stakeholders against CBRNe threats through better cooperation with security practitioners. Applied Ergonomics, 102. https://doi.org/10.1016/J.APERGO.2022.103752https://doi.org/10.1016/J.APERGO.2022.103752

Mor, Meirav, and Yehezkel Waisman (2002). "Triage principles in multiple casualty situations involving children: the Israeli experience." Pediatric Emergency Medicine Database (serial online).

Nicholson, W., Hall C., Weston, D., Burlin, A., Marsh, I., Zamorano, M., Amlot, R., Carter, H., (2021). Report on the Workshop with Vulnerable Citizens. Deliverable D3.3 of the PROACTIVE project.

Nicholson, W., Hall C., Weston, D., Burlin, A., Amlot, R., Carter, H., (2021). Initial Pre-Incident Public Information Materials for CBRNe terrorism. Deliverable D5.1 of the PROACTIVE

project.
Save the Children Italy (2020). Save the Children Italy: Emergency response and prevention. PROACTIVE Field Exercise Progress Meeting. London, 15 January 2020.
Strand, E., Johansson, P., (2021). Formation of the Civil Society Advisory Board. Deliverable D3.1 of the PROACTIVE project.
Zamorano, M., Suarez Gonzalo, S., Clavell Galdon, G., (2021). Legal and acceptability recommendations for PROACTIVE toolkit. Deliverable D8.2 of the PROACTIVE project.

Annex 3. Mitigation and Management of First Responders in CBRNe incidents: Guidelines for Policymakers

Summary

EU Member States lack an approach to enhance societal preparedness and response policies to CBRNe (Chemical, Biological, Radiological, Nuclear, and explosive) events that integrate mitigation and management needs of First Responders (FR). Based on preliminary results from the EU H2020 funded PROACTIVE project (Preparedness against CBRNe threats through cOmmon Approaches between security praCTItioners and the VulnerablE civil society), these Guidelines for Policy Makers recommend developing solid and long-term collaboration with First Responders and Civil Society Organisations (CSOs) and facilitating the advance of coherent, evidenced-based emergency procedures that address the mitigation and management policies in three stages: before, during and after the event. With this aim in mind, the document provides critical recommendations for Policy Makers on how to address FR's mitigation and management needs.

Problem

Many major cities worldwide have faced critical CBRNe-related incidents over the past few decades[21]. Furthermore, with terrorism threat levels high across the EU, using chemical agents by terrorist organisations has shown to be a significant risk also in European soil (EUROPOL, 2019). All involved stakeholders, including FR -such as public health officials, emergency management personnel, or even clinicians-, public authorities and CSOs may need clear, context-adaptable and well-structured guidelines and technologies to ensure their duties' efficacy. However, the literature has underlined the need for intergovernmental coordination in Europe and harmonising responses and actions to ensure their efficiency (D1.1, D1.2).

Issues and recommendations

FRs are key actors in the deployment of protocols and the use of technologies throughout a CBRNe event. Based on PROACTIVE preliminary results and the literature, this section identifies vital aspects to consider. Recommendations are organised according to the three critical stages of intervention: preparedness, response, and recovery. For each point we indicate the related PROACTIVE deliverables and recommendations.

[21] Examples include the explosion of a large amount of ammonium nitrate stored at the Port of Beirut (2020) which killed 220 people, instantly injured over 6,500 more, and severely damaged the densely populated residential and business districts nearby (Al-Hajj et al., 2021) or the ongoing Covid-19 pandemic (2019 - 2023). One well-known case in Europe is a Tunisian couple's attempt to attack with ricin in Cologne, Germany, using an improvised explosive device.

Management of CBRNe incidents preparedness

Issue	How to tackle by FRs	Action point for FRs
#1 The special needs of vulnerable persons are not always sufficiently taken into account in pre-incident information material. This concerns both the content and the format of the communication (D3.4, D6.4)	In cooperation with FRs and CSOs, policymakers could aim to develop a culture of prevention, response, and dissemination of knowledge concerning emergencies that promote an active role for civilians, including vulnerable groups, facilitating FRs' interaction with the public.	**#1** Pre-incident information should be provided to FRs to be delivered to the public based on the diversity and inclusion of all people. This means multiple sources (D1.1) and language formats (audio language, Braille, sign language, simple language and pictorial language), (D1.3). In addition, information materials should be offered in languages other than the local language (D3.4) or translated and trained in nonverbal communication (D3.3).
#2 Pre-incident information and CBRNe education can have the **potential to induce anxiety and catastrophising thoughts** (D1.3) that need to be overcome.	Policymakers could elaborate and disseminate, in collaboration with FRs and CSOs, pro-active social media campaigns and get people to know where to go for good information during events, facilitating FRs' interaction with the public.	**#2** To reduce the potential for anxiety and catastrophic thoughts, civilians could be trained on where to go for support and further information in the event of an incident (D2.2). To this end, pre-incident information should be culturally appropriate and respectful of religion and religious values (D1.3), be easy to understand, and be noncomplex, thereby allowing the information to be accessible to all (D1.1).
#3 Poor or outdated information leads to a lack of public commitment to follow FR instructions (D1.3).	Policymakers could request for detailed explanations to FRs, primarily, and to CSOs, secondly, about their responsibilities and strategies on crowd management and include this information in CBRNe preparedness tools.	**#3** Pre-incident information should meet the needs of the intended audience, incorporate factual proof and use a credible spokesperson (e.g. a specialist) to account for the preference for information received via higher sources (D1.1). Positive perception of pre-incident information and its effectiveness at influencing knowledge, understanding and confidence in undertaking recommended behaviours (D5.2).
#4 There is a need to harmonise the communication, cooperation and multi-agency approach regarding the preparedness protocols (D8.2).	Policymakers could co-responsabilise FRs to act as data controllers and managers of the PROACTIVE technologies in most cases.	**#4** FRs need to ensure a comprehensive set of technical and organisational protocols before the CCS is operational and 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 to maintain a consistent and coordinated plan (D8.2). Thus, teams and an inter stakeholders' communication

		structure must be enabled, including the inter-agency contact points and agreed communication means (I.e., channels, periodicity, etc.). Moreover, vias used, such as social media or telephone, must be secured for the purposes of PROACTIVE CCS sensitive data management (D4.4).
#5 Potential weak governance policy for the PROACTIVE system **(D4.4).**	Local authorities, with the collaboration of LEAs and FRs could set the PROACTIVE operations communication protocol.	#5 FR could be part of a CBRN national team established for the management of PROACTIVE system. Policy makers and authorities could play a key role in facilitating resources for this task and enabling the setting up of a joint team led by LEAs concerning the system management.

Mitigation and management of CBRNe incidents response

Issue	How to tackle by FRs	Action point for FRs
#6 Lack of public compliance and cooperation due to the limited public perception of trust and legitimacy during CBRNe events. These behaviours may all contribute to an **increased risk of physical exposure** to agents, toxins, and other hazards (Bartenfeld et al., 2014).	Policymakers could cooperate with FRs and CSOs need in order to design strategies to enhance public compliance and cooperation. It is essential to carry effective communication strategy among these actors and be aware that the way in which FRs manage an incident will impact the way the public behaves	**#6** FRs could focus on ensuring the protection of the public's health and could aim to influence the perceived efficacy of recommended behaviours (D1.1). To this end, FRs could maximise information sharing. The more information made available to the public during an incident (e.g. how and why official instruction should be followed), the higher the rate of compliance (D1.1). FRs could communicate openly and honestly about the nature of the incident and provide regular updates about actions being taken. A key emphasis is on giving clear, precise, and true information that is conveyed to people at the incident site, those who have evacuated, and the general public, in a practical, empathetic, and sensitive way. Factors associated with compliance (e.g., information should seek to inform the public about family, friends, and pets) (D1.2).
#7 Missing or insufficient outlining of clear responsibilities in the Standard Operating Procedure (SOP)'S and cooperation agreements between Law Enforcement Agencies (LEA)s and FRs organisations which need to be continuously adapted based on the learning outcomes of the exercises (D2.3).	Policy makers could ensure that FRs meet the needs of the public, especially those of vulnerable groups.	**#7** Communication is essential for transmitting responsibilities. Communication during an incident could be delivered by a trustworthy spokesperson, present useful and needed information, and incorporate facts or proof to provide robustness (D1.1). The use of FAQSs could be incorporated into communication efforts to reduce stress on authorities (D2.2). The compilation of all group needs should be reflected in an up-to-date way in the guidance documents and SOPs (D1.3).

#8 Assumptions outdated in the CBRNe incident response **regarding the psychosocial aspects** of crowd management strategies have prefixed ideas of controlling the public, rather than communicating with it (Carter et al, 2013).	The Proactive app can be a channel to facilitate communication between policy makers, FRs CSOs and LEAs with members of the public (and vice versa) during CBRNe emergencies.	**#8** Policy makers could convey the importance of FR management on the effects of public behaviour, the effective communication with members of the public, and the understanding and preparation of the needs of vulnerable groups. Providing adequate information about CBRNe events about undertaking actions rapidly can reduce their impact (Carter et al., 2020). The scope is to maximise public compliance with official communication in order to provide information to enhance self-efficacy to avoid the likelihood of maladaptive behaviour (D1.3).
#9 Need to review **discrepancies in guidance documents** to ensure consistency both within and between countries (D1.3).	Policymakers could facilitate FRs' contribution to the incorporation of up-to-date evidence-based advice in guidance and policy across Europe to reflect the importance of recognising psychosocial aspects of CBRNe response.	**#9** Although guidance on the overall response strategy during a CBRNe incident has the same management strategies (evacuation, disrobing, wet decontamination, dry decontamination, re-robing, commencing life-saving treatment prior to decontamination, shelter in place), the guidance and recommendations were not necessarily consistent, even within a country (e.g. decontamination duration (D1.3). Countries compare their CBRNe procedures with one another to enable a 'best practice' blanket approach to CBRNe incidents (D2.2). This guidance and policy must have a clear strategy on how to manage vulnerable groups and must be uniform in instruction, particularly when released in the same country (D1.3).
#10 Need to handle immediate practical training as awareness-raising measure to demonstrate practicalities associated with CBRNe incidents during the undressing and decontaminated processes (D1.3).	Policymakers could provide FRs and CSOs with the necessary means to offer training programmes to build CBRNe public awareness and knowledge.	**#10** Policy makers could allow FRs lead practical training and let them identify and delegate urgent tasks to CSOs', which contribution to training and CBRNe awareness should promote the availability of shielded areas where the undressed can wait and physical privacy is guaranteed. For instance, the Involvement of female CBRNe responders to address ethical needs during decontamination (e.g. disrobing) in Lebanon (D2.5). In sum, FRs could emphasize why disrobing is imperative (health hazard due to contaminated clothing, etc.) (D3.4).

Mitigation and management of CBRNe incidents recovery

Issue	How to tackle by FRs	Action point for FRs
#11 Low reporting of CBRNe-related information materials available to the public. There is a need to provide and spread information on infection control and post-event disease transmission among the general public (Bartenfeld et al., 2014).	Policy makers could provide FRs with all the necessary means to ensure that they can ensure physical, mental health and psychosocial support in the immediate aftermath of CBRNe events.	**#11** There could be a stronger development of systems of joint cooperation: joint-threat assessment and joint-coordination centres (D2.5) with PSAB, CSO, discussions/consultations with the CSAB members (D3.3). In Addition, Aide Memoire can be useful to identify and handle the ever-changing needs, expectations and challenges of vulnerable groups (D3.4).

#12 In the return to normal activity, there is a need to **assess the design improvements and technology advancements** (Kapur and Smith, 2011:8) (D8.2) as well as the ethics of the response operations (D6.4).	Policymakers could enhance the recovery preparedness practices in charge of the FRs could be improved by using the PROACTIVE toolkit.	**#12** FRs and LEAs could exchange knowledge about communication procedures with other national relevant practitioners, including private companies (Havârneanu et al, 2022), to create joint communication strategies, as well as with practitioners from other countries. In addition, they could use networks with other practitioners and interested/relevant CSOs to exchange "lessons learned" and "best practices" (D2.3). These should become 'lessons implemented' as part of a dynamic process to constantly update SOPs (D2.4). Later, they need to be further adapted by the respective practitioners in their respective countries according to their needs (D2.5).

Conclusion

These Guidelines integrated into the PROACTIVE Policy Brief are intended to provide policymakers with tools to improve their coordinated action and governance with FRs in mitigating and managing CBRNe incidents. Building on our findings, we outline the following recommendations in each phase.

- During the **preparedness**, to deliver pre-incident information based on diversity and inclusion, in an accessible manner and considering the needs of the audience, especially the vulnerable groups. These values need to be translated when setting for the PROACTIVE operations communication protocol.
- During the **response**, by protecting public health by maximising information sharing, transmitting responsibilities with adequate information, clear strategy and practical training.
- Finally, during the **recovery**, developing systems of cooperation to identify the ever-changing needs and expectations of the civilians, and transforming these lessons learned into lessons implemented in the return to normal activity.

Limitations

The recommendations included herein may be updated without prior notice if the PROACTIVE consortium and other entities develop new standards and guidance. As PROACTIVE is an ongoing project, empirical work conducted in Campus Vesta (May 2023) is expected to be used to review and disseminate the project results.

References

Bartenfeld, M., Peacock, G., & Griese, S. (2014). "Public Health Emergency Planning for Children in Chemical, Biological, Radiological, and Nuclear (CBRN) Disasters". *Biosecurity And Bioterrorism: Biodefense Strategy, Practice, And Science*, 12(4), 201-207. https://doi.org/10.1089/bsp.2014.0036

Becker, S.M. (2004). "Emergency communication and information issues in terrorist events involving radioactive materials". *Biosecurity and bioterrorism : biodefense strategy, practice, and science*, 2(3): p. 195-207.

BESECU (2011). Final Report Summary - BESECU (Human behaviour in crisis situations: A cross cultural investigation to tailor security-related communication).

Carter, H., et al. (2013). Perceived responder legitimacy and group identification predict cooperation and compliance in a mass decontamination field exercise. Basic and Applied

Social Psychology. 35(6), 575-585.
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.
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.
Havârneanu, G. M., Petersen, L., Arnold, A., Carbon, D., & Görgen, T. (2022). Preparing railway stakeholders against CBRNe threats through better cooperation with security practitioners. Applied Ergonomics, 102. https://doi.org/10.1016/J.APERGO.2022.103752
NHS (2015). NHS England Emergency Preparedness, Resilience and Response (EPRR). Chemical incidents: planning for the management of self-presenting patients in healthcare settings.
NHS (2019). Guidance for the initial management of self-presenters from incidents involving hazardous materials - HazMat/CBRNe.
Pearce, J.M., et al. (2013). Communicating public health advice after a chemical spill: results from national surveys in the United Kingdom and Poland. Disaster medicine and public health preparedness. 7(1): p. 65-74.
Witte, K. (1992)- Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs.* 59(4): p. 329-349.