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

Deliverable D4.1

Report on the High-level Architecture design including an interface control document

Due date of deliverable: 31/10/2020

Actual submission date: 12/03/2021

George Kolev[1], Garik Markarian[1], Nataly Polushkina[1]

Rinisoft Limited

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**uleranbl**E** civil society
Grant Agreement no.	832981
Call ID and Topic	H2020-SU-SEC-2018, Topic SU-FCT01-2018
Project Timeframe	01/05/2019 – 30/04/2022
Duration	36 Months
Coordinator	UIC – Grigore Havarneanu (havarneanu@uic.org)

Document details

Title	Report on the High-Level Architecture design including an interface control document
Work Package	WP4
Date of the document	12/03/2021
Version of the document	06
Responsible Partner	RINISOFT
Reviewing Partner	ETI, CBRNE, UIC
Status of the document	Final
Dissemination level	Public

Document history

Revision	Date	Description
01	03/09/2020	First Draft
02	02/10/2020	Technical Content Added
03	12/10/2020	Formatted for Submission to Reviewers
04	22/10/2020	Draft reviewed by ETICAS, CBRNE, UIC
05	30/10/2020	Final Submission incorporating reviewers' comments
06	12/03/2021	Update following mid-term periodic review

Consortium – List of partners

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

Executive summary

The architecture design specification is the main output of deliverable 4.1, the purpose of which is to ensure a modular, flexible, extensible, scalable, robust and secure system and to ensure consistency with the Mobile Application for Citizens, including those more vulnerable (D5.3). The design process focuses on facilitating Law Enforcement Agencies (LEAs) and Security Policy Makers ability to select, configure and adapt the system in line with their needs and preferences relative to the scenario they are facing. The system aims to improve the efficiency of the communication between LEAs, Policy Makers and Citizens, with a particular focus on information sharing (T5.1). The technology, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by mobile technologies, as well as modern data analytics capabilities to support users in overall decision-making processes. The provision of 'other applications' (3rd party) has also been addressed and refers to integration with third party applications, this covers any application outside of the PROACTIVE system, which may interact by pushing/pulling information to or from the PROACTIVE system.

Input from WP1, WP2, WP3, WP5 and WP8 has been reviewed to determine the needs and gaps of the users in terms of current public perceptions relating to Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) incidents. The research completed in WP1 will feed into the key engagement tasks in WP2 and WP3, and by default will provide key feedback for the Toolkits in WP4 and WP5. The work carried out in WP4 will then feed primarily into the exercises in WP6, whether they are in person or virtual and will create a feedback loop enabling an iterative approach to the toolkit development. In addition, WP8 and WP10 provided ethical and legal requirements which were built into the design of the App.

The initial end user requirements were derived from the Description of Action and the experience of Rinisoft, which provided a baseline for the minimal functionality of the system, including the web collaborative platform, and mobile applications. From this, the core requirements were agreed, and the initial designs were implemented, detailing the graphic user interface and the key functionalities in relation to the original proposed first exercise, scheduled for M18 in Rieti, Italy. However, due to the ongoing COVID-19 pandemic, and the proposed exercise being postponed, further feedback has been sought through network partners and planned webinars.

This deliverable documents the requirements captured prior to the 1st field exercise utilising the access we have to the end users within the consortium and the existing Practitioner Stakeholder Advisory Board (PSAB) network. Future iterations of the system development are expected to be customised in relation to the feedback from the planed exercises; initially focus will be placed on the Civil Society Advisory Board (CSAB) requirements, then the PSAB and the final exercise will amalgamate the two. To date, the development has focused on the core functionality, which will span across the exercises aiming to gather end user feedback to feed into the development loop. The next phase of the development will be to incorporate the current available content, effectively showcasing the usability and purpose of the system during and post the mid-term conference.

Due to the proposed iterative development of the PROACTIVE system, we realise further requirements will be identified, particularly in relation to customisation for the project exercises. Further requirements for the web collaborative platform and mobile application for LEAs and Security Policy Makers will be documented in D4.2, and D4.3 respectively, both of which are due in M36.

Table of Contents

1. Introduction 7

1.1. Project Summary 7

1.2. Objectives of WP4 7

1.3. Objectives of D4.1 8

2. Purpose of the Deliverable 8

3. Interaction with other Work Packages 9

3.1. Work Package 1 Input 9

3.2. Work Package 2 Input 15

3.3. Work Package 3 Input 25

3.4. Work Package 5 Input 31

3.5. Work Package 6 Input 33

3.6. Work Package 8 and 10 Input 35

3.7. Accessibility Functionality for Vulnerable Citizens 39

4. End User Requirements 40

4.1. Core Requirements 40

4.2. Functional Requirements – First Field Exercise 41

4.3. Functional Requirements - User Categories 42

5. System Requirements 44

5.1. System Functionality 44

5.2. System Security 45

5.3. System Interoperability 45

5.4. Graphic User Interface 46

6. Conclusion 50

7. Annex A – User Requirements Matrix 51

8. Annex B – Detailed Core Requirements 56

9. Annex C – Privacy Policy 60

List of Tables

Table 1 - Work Package 1 Input to the Technology Toolkit.....10
Table 2 - Work Package 2 Input to the Technology Toolkit.....15
Table 3 - Work Package 3 Input to the Technology Toolkit.....25
Table 4 - Work Package 5 Input to the Technology Toolkit.....31
Table 5 - Work Package 6 input to the Technology Toolkit.....33
Table 6 - Work Package 8 and 10 Input to the Technology Toolkit.....35
Table 7 - Core Requirements.....41
Table 8 - Functionality for the first field exercise.....42
Table 9 - Access Levels.....43

Table of Figures

Figure 1 Work Package Collaboration 9
Figure 2 Linux Based Server 45
Figure 3 Registration and About Us Pages.....47
Figure 4 Home Page and Key Contacts.....48
Figure 5 Information Sharing 49
Figure 6 Feedback Loop.....50

Table of Acronyms

AES – Advanced Encryption Standard
API – Application Programming Interface
AWS – Amazon Wen Server
CBRNe – Chemical Biological, Radiological, Nuclear, explosive
CSAB – Civil Society Advisory Board
GDPR – General Data Protection Regulation
GIS – Geographic Information System mapping
GUI – Graphic User Interface
HTTPS – Hypertext Transfer Protocol Secure
IP – Internet Protocol Address
LEAs – Law Enforcement Agencies
PSAB – Practitioner Stakeholder Advisory Board
REST – Representational State Transfer
SOP – Standard Operating Procedure
SQL – Structure Query Language
TLS – Transport Layer Security
WP – Work Package

1. INTRODUCTION

1.1. Project Summary

In line with the EU Action Plan to enhance preparedness against Chemical, Biological, Radiological Nuclear and explosive (CBRNe) security risks and the overall Security Union approach to fight crime and terrorism, PROACTIVE aims to enhance societal CBRNe preparedness by increasing Practitioner effectiveness in communicating and managing large, diverse groups of people in a CBRNe environment.

This will be achieved by testing common approaches between European Practitioners such as Law Enforcement Agencies (LEAs) and First Responders. These will be evaluated and validated against the requirements of civil society, including vulnerable groups of citizens reflected in the European Security Model. A Practitioner Stakeholder Advisory Board (PSAB) and a Civil Society Advisory Board (CSAB) will extend the representation of both sides in several surveys, focus-groups, workshops and field exercises. A benchmark study between LEAs will identify common approaches in assessing CBRNe threats and the protocols and tools used to help citizens. Liaising with the eNOTICE H2020 project, three joint exercises will include role play volunteers recruited by PROACTIVE. They will evaluate the acceptability and usability of existing procedures and test new tools developed within PROACTIVE to provide innovative recommendations for Policy Makers and Safety and Security Practitioners.

PROACTIVE will result in toolkits for CBRNe Practitioners and for Civil Society Organisations. The toolkit for Practitioners will include a Web Collaborative platform with database scenarios for communication and exchange of best practice among LEAs as well as an innovative response tool in the form of a Mobile Application. The toolkit for the Civil Society will include a Mobile Application adapted to various vulnerable citizen categories and pre-incident public information material. These will provide valuable inputs to the EUROPOL initiative to develop a knowledge hub for CBRNe activities and help consolidate the EU Action Plan to enhance preparedness for CBRNe threats.

1.2. Objectives of WP4

The main objectives of WP4 can be summarised 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.

1.3. Objectives of D4.1

The key objective of D4.1 will be to document the architectural requirements of the web collaborative platform and mobile application for LEAs and Security Policy makers. The deliverable will highlight the key requirements identified to date and will be documented according to functionality, usability, security and interoperability.

2. PURPOSE OF THE DELIVERABLE

The architecture design specification is the main output of D4.1. The purpose of the architectural design specification is to ensure a modular, flexible, extensible, scalable, robust and secure system. The design process focuses on facilitating LEAs and Policy Makers to select, configure and adapt the system in line with their needs and preferences relative to the scenario they are facing. The system aims to improve the efficiency of the communication between LEAs, Policy Makers and Citizens, with a particular focus on information sharing (task T5.1). The technology, as an enabler, is an efficient and effective way to exploit bi-directional communication capabilities offered by mobile technologies, as well as modern data analytics capabilities to support the users in overall decision-making processes. The provision of 'other applications' (3rd party) has also been addressed and refers to integration with third party applications, this covers any application outside of the PROACTIVE system, which may interact by pushing/pulling information to or from the PROACTIVE system.

The architecture herein presented promotes customisation to fit the needs of each user group, while sharing common denominators expressed in this architectural design document. Although further information relevant to vulnerable citizens will be documented in D5.3, it is inevitable that the core structure of the system is the same across all stakeholder groups to enable consistency and bi-directional communication. Accessibility, in particular will be a key focus across the system as a whole, this is principally important for vulnerable communities or communities that are more difficult to reach; deaf, visually impaired, religious, children, elderly etc.

The architectural definition process focused on the following four principal objectives:

- To clearly present a description of the PROACTIVE system and how it addresses the stakeholder needs, (including LEAs, Policy Makers and vulnerable citizens);
- To provide a clear description of the critical aspects that need to be taken into consideration to ensure the system is modular, flexible, extensible, scalable, robust and secure;
- To provide enough details to allow technical teams to build instances of the system that share a common structure and consequently are interoperable by design;
- To ensure consistency for tasks 4.2, 4.3, 5.2 and 5.3 that will use this architecture design as a baseline input.

3. INTERACTION WITH OTHER WORK PACKAGES

Designing and developing the PROACTIVE Web Based platform and Mobile Applications for LEAs and security policy makers will predominantly be the responsibility of WP4. Input will be required from WP1, WP2, WP3 and WP8 to determine the needs and gaps of the users in terms of current public perceptions relating to CBRNe incidents. The research completed in WP1 will feed into the key engagement tasks in WP2, and by default will provide key feedback for the PROACTIVE Web Based platform and Mobile Applications in WP4. The work carried out in WP4 will then feed primarily into the exercises in WP6, whether they are in person or virtual and will create a feedback loop enabling an iterative approach to the toolkit development.

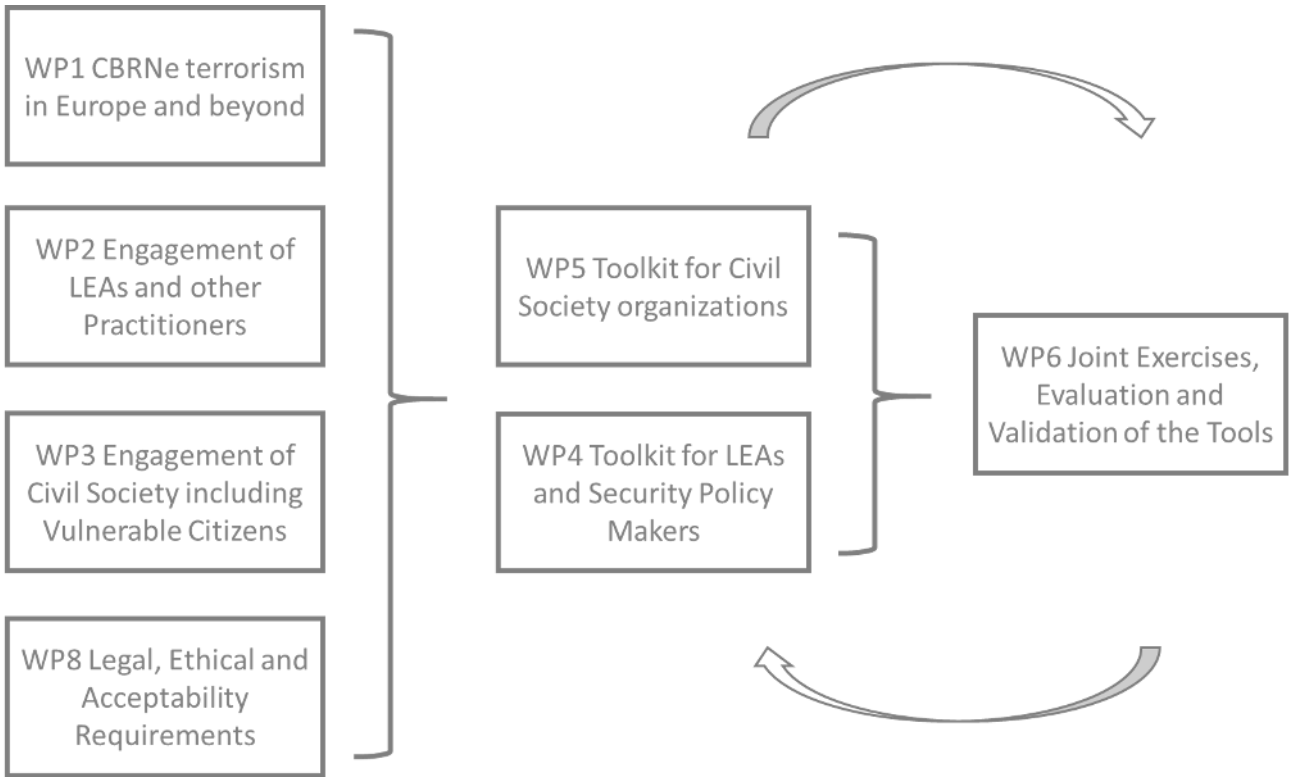


Figure 1 Work Package Collaboration

The research completed in each of the Work Packages highlighted in Figure 1, has been reviewed and analysed from the perspective of the Web Based Collaborative Platform and Mobile Applications. In each of the deliverables referenced in the following tables and sub-sectionsTable 1 - Work Package 1 Input to the Technology Toolkit, the key outcomes relevant to the development of the Web Based platform and Mobile Applications have been addressed. They have then been further evaluated to determine how the recommendations can be translated to either the system functionality and/ or content, as documented in Sections 4 and 5 in this deliverable.

3.1. Work Package 1 Input

In each of the deliverables referenced in Table 1 - Work Package 1 Input to the Technology Toolkit*Table 1 - Work Package 1 Input to the Technology Toolkit*, the key outcomes relevant to the

development on the Web Based platform and Mobile Applications have been addressed in terms of content and functionality relevant to human factor analysis of preparedness and response.

Table 1 - Work Package 1 Input to the Technology Toolkit

CBRNe terrorism in Europe and beyond: Human Factors analysis of preparedness and response	WP4 Toolkit for LEA's and Security Policy Makers
D1.1 Findings from Systematic Review of Public Perceptions and Responses	
Recommended changes to informational texts and leaflets are relatively consistent across studies, with guidelines often consisting of rewording [30, 51] and the use of visual material [51] to assist in making the resource user friendly [30]. These recommendations have been showcased to be effective using multi-phase studies, in which participants are asked to review a currently existing leaflet, and feedback is subsequently used to aid in the creation of an adapted leaflet or informational text (e.g. [39, 46]. For example, Hellier et al. (2014), created a leaflet which: was highly approved by the participant group; was shorter in length; presented a lower reading age, and used definite and explicit language. Ability to recall information from the leaflet (i.e., recommended advisories to be taken in the case of an event) was also improved after reading the adapted leaflet in comparison to the original [39]. Additionally, successful pre-incident information has been novel in quality (e.g., featuring a cartoon character as a spokesperson), specific, easy to understand [55], and incorporated well versed analogies to allow information to be more applicable to the public [29].	**Content:** Recommendation on the structure, format, type and level of information. Specifically, the use of visual content.
A higher proportion of studies recommend having a credible spokesperson delivering information [14, 29, 37].	**Content:** Credibility of sources
The use of written communication (i.e., leaflets and informational texts) was perceived positively by members of the public, as they are tangible and therefore are harder for the government to retract [35]. Additionally, leaflets have been deemed by some to be successful in communicating pre-incident information, especially when developed following feedback from the public (e.g., shorter with less complex information [37]). However, within some literature, the effectiveness of written communication has been questioned as distribution needs are not always met when releasing information (i.e., with vast reports of non-receipt; [27, 39]). Furthermore, findings that demonstrate effectiveness of written communication are largely captured under controlled research settings [28, 37]; real life studies of such communications have yielded low percentages of participants claiming to have read and remembered various distributed pre-incident information, including a booklet [27], and a leaflet [39].	**Content:** Recommendation on the structure, format, type and level of information. Specifically, the use of written text.

In summary, review of the research revealed that in order to be effective, pre-incident information should: be easily understandable; delivered by a credible source; be disseminated via multiple platforms; and incorporate psychological constructs which reduce anxiety and provide emotional and rational appeal.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, multiple sources of delivery.
In summary, review of the research revealed that 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. Additionally, the more information made available to the public during an incident, regarding why and how they should comply, will increase the level of compliance shown. Anxiety can negatively affect the willingness to comply, whereas fear can motivate the public to comply with official instruction. Self-efficacy, response-efficacy and the ability to cope with the situation at hand were all associated with how much compliance would be shown by the public. Lastly, the desire to seek out loved ones during an incident and ensure their safety has a large effect on public willingness to comply with protective measures.	**Content:** Credibility of sources
Pre-incident information should be delivered to the public using multiple sources [33, 37]. It should be culturally appropriate [20], easy to understand, and noncomplex [37, 39, 51], allowing the information to be accessible for all [41]. Additionally, pre-incident information should meet the needs of the intended audience [37, 46], incorporate factual proof [37] and use a credible spokesperson (e.g., a specialist) [29] to account for the preference for information received via higher sources [47]. Furthermore, incorporation of novelty has been effective in dissemination of pre-incident information (e.g., using a cartoon character [47, 55]), which may provide an additional route for effective delivery of pre-incident information.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, multiple sources of delivery.
Furthermore, it may prove beneficial to implement more educational programs or to implement methods to raise awareness (i.e., interventions) as research indicates these are effective at: reducing anxiety [21], improving knowledge; [37, 51], and raising education, to allow members of the public to effectively attend to, and remember, information [36].	**Content:** Recommendation on the structure, format, type and level of information. Specifically, educational information.
Alongside the importance of pre-incident information and education, it is also necessary to consider that there is a possibility of provoking worry in members of the public that are not currently worried when circulating pre-incident information regarding CBRNe incidents [19, 34], so this should be done so mindfully. Additionally, it is important to remember that pre-incident information is not a substitute or replacement for real-time information for an ongoing incident [37].	**Content:** Recommendation on the structure, format, type and level of information. Specifically, educational information.
D1.2 Findings from systematic review of current policy for mitigation and management of CBRNe terrorism	

There seems to be a lack of detailed recognition for psychosocial aspects (psychological and social factors associated with human behaviour). Therefore, although it is important to provide practical and physical recommendations to responders to enable them to manage the incident, ensuring that they also consider psychosocial aspects and interactions with the public should not be overlooked.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, psychosocial impacts.
Additional modalities of communicating with people at the scene may not always be necessary depending on the size of the incident scene and the number of casualties, it is important that responders are aware that there might be a need to use additional modalities and are aware of what these are.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, multiple sources of delivery.
Recommendation 1: Incorporate up-do-date evidence-based advice in guidance and policy on how members of the public are likely to respond in a CBRNe incident.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.
Recommendation 2: Update guidance and policy to incorporate a detailed communication strategy for how emergency responders should communicate with casualties and members of the public during a CBRNe incident.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.
Recommendation 3: Ensure guidance and policy have a clear strategy on how to manage vulnerable groups in a CBRNe incident.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.
Recommendation 4: Review any discrepancies in documents both within and between countries to ensure consistency in recommendations on how emergency response organisations should respond to a CBRNe incident.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.
D1.3 Guidelines and Recommendations for mitigation and management of CBRNe terrorism	
How to communicate with members of the public (e.g., dissemination of information should be available in writing using non-complex language);	**Content:** Recommendation on the structure, format, type and level of information. Specifically, the use of written text.
Factors associated with compliance (e.g., information should seek to inform the public about family, friends and pets);	**Content:** Recommendation on the structure, format, type and level of information. Specifically addressing compliance.
Guidance on strategies for managing vulnerable populations during a CBRNe incident (e.g., more consideration must go into creation of policy and procedure for those with mobility issues).	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.

Information campaigns and education to build CBRNe public knowledge should be implemented.	**Dissemination and Exploitation:** Market awareness of CBRNe Information. Specifically, educational information.
Messages should be pitched at an appropriate level (in terms of language and complexity).	**Content:** Recommendation on the structure, format, type and level of information.
Official communication should be honest, empathic, assertive and reliable.	**Content:** Recommendation on the structure, format, type and level of information.
Information should be available in writing (i.e., print form), where possible, using non-complex language.	**Content:** Recommendation on the structure, format, type and level of information.
Multiple platforms should be used to communicate with the public, with consistent information being provided across platforms.	**Dissemination and Exploitation:** Market awareness of CBRNe Information.
Information provided by authorities should be pre-planned, where applicable, to ensure prioritisation and consistency, provide uniformity and advocate cohesion.	**Dissemination and Exploitation:** Market awareness of CBRNe Information.
Responders should communicate effectively and demonstrate respect for public needs.	**Content:** Recommendation on the structure, format, type and level of information
Communication should: 1) inform the public about loved ones' whereabouts in relation to family, friends and pets; 2) provide information about active police and security efforts to apprehend terrorists; 3) provide information on the importance of complying with instruction (including health specific information to address public health concerns; 4) and be delivered by a credible spokesperson (e.g., local resources, hazard groups and health departments).	**Functionality:** Missing Persons/ pets **Functionality:** Live Notification to registered members **Functionality:** Sharing pre-incident information
Communication should aim to reduce anxiety, by providing information to enhance self-efficacy.	**Content:** Recommendation on the structure, format, type and level of information.
Official sources should communicate honestly and accurately in detailing risks associated with an incident, as this will allow the public to make an informed decision as to whether they wish to comply with official instruction or recommended behaviour.	**Content:** Recommendation on the structure, format, type and level of information
Information should be provided in multiple languages, pictographic form, and sign language.	**Content:** Recommendation on the structure, format, type and level of information

More consideration should be given to developing policy and procedures to assist those with mobility issues (e.g., relating to service animals and essential mobility aids) during CBRNe incidents.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.

The research carried out in WP1 highlighted several key factors which then had to be considered during the development phase of the Web Based Platform and Mobile Applications as follows.

Method of information to be shared.

Extensive research was completed to show the varying methods, formats and structure of information that is currently or should be shared in relation to CBRNe events. A common theme identified is that multiple forms of communication should be utilised, not specific to an App. This includes, but is not limited to written text, visual content including danger signs/symbols, cartoon characters, multiple languages, pictographic form and sign language. The PROACTIVE Web Based platform and Mobile Applications have been designed to accommodate these needs by ensuring multiple file formats can be utilised to upload, download and provide information.

Content of information to be shared.

Some of the high-level findings from the research focused on reducing anxiety and enhancing self-efficacy of the public through the information shared. The research detailed that information should be factual, evidence based, cater for physical and psychosocial aspects, use non-complex language, be honest, empathic assertive and reliable, and be provided by a credible source. Other recommendations highlighted the type of guidance documents that should be made available, including communication strategies with the public, guidance documents on how the public is expected to react and strategies for managing vulnerable groups. The PROACTIVE Web Based platform and Mobile Applications cater for these needs by offering two key functionalities: 1). An area to share relevant information directly with the public, pre-incident and 2). An area for LEAs and Security Policy Makers to share information, e.g., guidance policies, confidentially.

The research also highlighted that pre-incident information is not a substitute or replacement for real-time information for an ongoing incident. With this in mind the PROACTIVE Web Based platform and Mobile Applications were developed to allow for pre-incident information to be shared but also updates on relevant live on-going incidents, for example health updates, security efforts, next steps etc in the form of updated alerts on the Mobile Applications and also push notifications/ alerts to registered users.

Additional Functionality

One of the key points of interest for the public when facing a CBRNe event is the whereabouts of family, friends and pets. This functionality is in the pipeline for the second phase of development to allow further research through engaging directly with the CSAB and PSAB networks to ensure all relevant requirements and purposes are captured accurately.

3.2. Work Package 2 Input

In each of the deliverables referenced in Table 1 - Work Package 1 Input to the Technology Toolkit*Table 2 - Work Package 2 Input to the Technology Toolkit*, the key outcomes relevant to the development of the PROACTIVE Web Based platform and Mobile Applications have been addressed in terms of content and functionality relevant to the Engagement of LEAs and other Practitioners.

Table 2 - Work Package 2 Input to the Technology Toolkit

WP2 Engagements of LEAs and other Practitioners	WP4 Toolkit for LEA's and Security Policy Makers
T2.2 – Engagement with Practitioners.	Workshop held on the 25th of February 2021. The outputs will be included in D4.3
D2.2 - Report on the pre-exercise workshop with practitioners	
In the case of a terrorist attack, procedures, such as evacuation may not start immediately (as Police will check if the terrorist is still near the victims first, for example) and procedures will be delayed (e.g., until decontamination is ready and available). Nothing can be ready immediately. They suggested that it may therefore make sense to educate the public to understand that procedures may be delayed and explain why this is the case.	**Content:** High level procedures in terms of evacuation to be shared with the public to further educate expectations during an event.
One attendee added that it would be helpful to provide information on how to distinguish fake news, i.e. which sources are correct, and which are not. Communication should be delivered by a credible spokesperson (e.g. local resources, hazard groups and health departments). It is necessary to establish whose duty it is to inform the public of CBRNe events, and who should be responsible in communicating during incident information. Risk communication cannot assume a scientifically ignorant public, and institutions should not exaggerate the superiority of their knowledge and judgment.	**Content:** Credibility of sources
Communication Should provide information on the importance of complying with instruction (including health specific information to address public health concerns);	**Content:** Health specific instructions and importance of complying
Three dimensions of disaster communication should be used when creating pre-incident information (strategic, contextual and personal).	**Content:** Recommendation on the structure, format, type and level of information. Specifically, pre-incident information.

Official communication should be honest, empathic, assertive and reliable.	**Content:** Recommendation on the structure, format, type and level of information
There was agreement that the public should be educated in how to handle a CBRNe incident (with reference to work being carried out to educate the public in relation to the COVID-19 pandemic). Indeed, one PSAB member reasoned that if the public are educated in CBRNe incidents they will be able to react in an appropriate way. However, there was also worry that over-education could have negative effects. For example: how much pre-incident information can be circulated, or how sensitive topics (including loss of life) could be explained, without creating unnecessary anxiety. From a policing perspective, concerns around the detrimental effects of revealing information regarding how attacks are handled for counter terrorism was discussed.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, education information.
"Official sources should communicate honestly and accurately in detailing risks associated with an incident, as this will allow the public to make an informed decision as to whether they wish to comply with official instruction or recommended behaviour."	**Content:** Recommendation on the structure, format, type and level of information
"Communication should aim to reduce anxiety, by providing information to enhance self-efficacy."	**Content:** Recommendation on the structure, format, type and level of information
Communication should Inform the public about loved ones' whereabouts in relation to family, friends and pets.	**Functionality:** Missing Persons/ pets
Communication should provide information about active police and security efforts to apprehend terrorists	**Functionality:** Active updates on police activities
The use of FAQs should be incorporated into communication efforts to reduce stress on authorities.	**Functionality:** Customisable FAQ section
Messages should be pitched at an appropriate level (in terms of language and complexity).	**Accessibility:** method of communication
Information should be provided in multiple languages, pictographic form, and sign language.	**Accessibility:** method of communication

PSAB members agreed with these recommendations and provided only limited comments, including it cannot be assumed that internet will be available during the incident and methods should be put in place to ensure that those who are not computer literate are still able to access the information, and that the current increase in smart technology could be used to provide safety instructions when necessary.	**Accessibility:** method of communication
Multiple platforms should be used to communicate with the public, with consistent information being provided across platforms.	**Accessibility:** method of communication
Information should be available in writing (i.e., print form), where possible, using non-complex language.	**Accessibility:** method of communication
It would be beneficial to prepare pro-active social media campaigns and get people to know where to go for good information during events.	**Dissemination and Exploitation**: Market awareness of CBRNe Information.
Information campaigns and education to build CBRNe public knowledge should be implemented.	**Dissemination and Exploitation**: Market awareness of CBRNe Information.
The use of displays, simulations, and online games should be used to engage the public and educate them in CBRNe matters.	**Dissemination and Exploitation**: Market awareness of CBRNe Information.
D2.3 Report on the survey and benchmarking study results	
Recommendation 1: In addition to a general increase in the consideration of vulnerable groups in CBRNe related SOPs, ethnic minorities, hearing impaired people and mentally ill people in particular should receive more attention.	**Accessibility:** method of communication
Recommendation 2: There is a need to raise awareness for the needs of vulnerable groups in CBRNe situations.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 3: An increase in regular CBRNe exercises is desirable for LEAs and healthcare professionals.	**Exploitation and Dissemination:** App to be used to influence exercises
Recommendation 4: Inter-institutional CBRNe exercises should be performed more regularly to enhance coordination between the emergency services during a CBRNe incident.	**Exploitation and Dissemination:** App to be used to influence exercises

Recommendation 5: Increased participation of vulnerable groups in CBRNe exercises is urgently needed.	**Exploitation and Dissemination:** App to be used to influence exercises
Recommendation 6: The needs of hearing-impaired people, visually impaired people, ethnic minorities, pregnant women, mentally ill people and people who do not understand the respective national language sufficiently or at all should be addressed more often in information resources that educate LEAs and First Responders.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, educational information.
Recommendation 7: The internal allocation of responsibilities should be more clearly emphasised, especially among LEAs and health care organisations.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 8: Where necessary, more extensive inter-institutional cooperation between the organisations involved in CBRNe incidents should be sought.	**Exploitation and Dissemination:** App to be used to influence inter-institutional cooperation
Recommendation 9: There is an urgent need for CBRNe practitioners to implement cooperation agreements with civil society organisations.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 10: Especially the topics of “containment”, “evacuation” and “decontamination” should be trained during CBRNe exercises.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 11: Unforeseen challenges in dealing with vulnerable civilians might be decreased by strengthening the exchange of knowledge between First Responder organisations and Civil Society Organisations.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 12: First Responder organisations might increase the number of the actual addressees of their information by acknowledging and understanding the diversity of their audience prior to a CBRNe incident.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 13: First Responder organisations should improve their awareness and consideration of their vulnerable audience prior to a CBRNe incident.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 14: There is an urgent need to include the needs of hearing-impaired people, visually impaired people, mentally ill people, pregnant women and ethnic minorities in communication strategies of CBRNe response.	**Content:** Recommendation on the structure, format, type and level of information
Recommendation 15: The amount of information material in additional linguistic formats should be increased and be stronger implemented, especially regarding hearing and visually impaired people.	**Accessibility:** method of communication

Recommendation 16: At the same time, restrictions on accessing information through additional linguistic formats should be reduced.	**Accessibility:** method of communication
Recommendation 17: Especially the availability of sign language should be increased so that in the future it will not only provide hearing impaired people with relevant information on CBRNe response, but also mentally disabled persons, autistic people, children and foreign people.	**Accessibility:** method of communication
Recommendation 18: LEAs and First Responders should include psychologists and psychiatrists into their networks.	**Exploitation and Dissemination:** App to be used to influence inter-institutional cooperation
Participants rarely indicated that those they represent use mobile apps to connect with them. They were even less likely to report using such apps themselves. Therefore, the proposal is to take this preference into account and develop strategies to change it. If we convince civil society organisations of the usefulness of such apps, the use and acceptance on the part of the vulnerable population will probably also increase.	**Dissemination and Exploitation**: Market awareness of CBRNe Information.
D2.4 Recommendations on how to adapt SOPs and tools	
Effective intervention is based on cooperation of the response agencies which require some form of agreement created in the preparedness phase.	**Content:** Recommendation on the structure, format, type and level of information
The main documents for managing a CBRN incident are Joint Standard Operating Procedures (JSOPs)	**Content:** Recommendation on the structure, format, type and level of information. Example Requested
The conclusion determined a necessity to create an integrated system of response, where all needful units will be involved. JESIP (Joint Emergency Services Interoperability Principles) tool	**Functionality:** Inter-agency communication (shared documents) and communication areas
Taking Evidence: Information gathering (it means scene assessment, threat assessment, place of leakage of dangerous substance)	**Functionality:** Incident Reporting (two-way between public and LEAs)
Agreed protocols should be in place to alert any commercial or industrial organisations whose premises, services or personnel could be affected, or required as part of the response and recovery effort.	**Content:** Recommendation on the structure, format, type and level of information **Functionality:** Live Notification to registered members
Prompt detection of the type of radioactive material used will greatly assist local authorities in advising the community on protective measures, such as sheltering in place, or quickly leaving the immediate area.	**Content:** Recommendation on the structure, format, type and level of information **Functionality:** Live Notification to registered members

Information gathering making prompt, accurate information available to the public may prevent the panic sought by terrorists.	**Content:** Recommendation on the structure, format, type and level of information
No principles for vulnerable groups were found in the main documents that are intended mainly for responding first responders	**Content:** Recommendation on the structure, format, type and level of information. Recommendations for LEAs requested
A simplified classification is used: persons showing signs of life – persons who do not show signs of life. The procedure is summarized in D2.4	**Content:** Recommendation on the structure, format, type and level of information
Firefighters provide first psychological assistance to the affected persons in order to stabilize the affected person, which mainly consists in meeting the need for the necessary information	**Content:** Recommendation on the structure, format, type and level of information **Functionality:** Live Notification to registered members
There is list of guidelines how to communicate a support affected people in order to calm down situation, reassuring people and gain their trust.	**Content:** Recommendation on the structure, format, type and level of information. Copy of guidelines requested
Decontamination procedures differ in procedures mainly in relation to two variables. Decontamination of responders against decontamination of victims against decontamination of equipment.	**Content:** Recommendation on the structure, format, type and level of information. Copy of procedures requested
The SOPs demonstrate that the media is informed following a summarisation and harmonisation exercise by the commander.	**Feature:** Further information gathered through the 'incident sharing' option in the PROACTIVE App.

There is list of some things to keep in mind when planning and executing decontamination of such group: • Make every effort to keep a child with a parent or trusted adult. • Unless contraindicated due to medical needs, families should undergo decontamination together. A method to hold or carry an infant through decontamination must be in place. • Patients with decreased mobility (e.g., in wheelchairs) may need to be transferred to a backboard or gurney and treated as a non-ambulatory patient. • Patients should retain, to the greatest extent possible, all materials required for "normal" functionality (e.g., prosthetics, hearing aids, eyeglasses). • Provide written and pictographic instructions for the decontamination process; translate to the most used languages within the population. • Integrate behavioural health professionals early in the response, as resources allow. • Take in consideration special needs of various religion or ethnic groups in population.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, an example of the decontamination process.
Information gathered and shared internally during the initial stages of an incident includes: M – Major incident declared. E – Exact Location T – Type of incident H – Hazards present or suspected. A – Access – rotes that are safe to use. N – Number. Type, Severity of casualties E – Emergency services present and those required	**Content:** Recommendation on the structure, format, type and level of information. Specifically, inter-agency communication.
Instruction provided by responders shall be unambiguous, clear and correct. Communication of instructions to the public could pose the risk of delay in operation and needs to be adapted to a situation. This doesn't mean that responders might give up the explanation, however, they might not delay operation for cooperating public because of individuals or groups who doesn't follow the operation instructions	**Content:** Recommendation on the structure, format, type and level of information. Specifically, instruction based
It is important that responders clearly communicate what they know about the incident, what is being done to help affected people and how they can help themselves. This will help foster public trust and confidence in responding organisations and help promote compliance with emergency interventions	**Content:** Recommendation on the structure, format, type and level of information. Specifically, public compliance

Following points are recommended to responders to consider for communication to public: • What they know of the nature of the incident, even if it is just that more help is on its way. • What the emergency services are doing and that these actions will help. • That medical assistance is coming to them – they should not leave the scene. • That the advice and instructions from the emergency services should be followed. • That those who are capable should assist others who are injured or less able to carry out tasks – if they can.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, what messages should be provided to the public
Limited SOP's available specifically detailing the needs of vulnerable people. The solution is proper training of all aspects of communication among responders and to the public which involves specifics of CBRNe environment (communication impairment in PPE, influence of intoxication etc.) and public including groups with special needs.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, training requirements.
Czech law on FRS contains opportunity for people with special need to be listed in database at OPIC and they would be contacted in case of emergency. Registration of mobile number into warning systems maintained by local authorities is also common opportunity.	**Feature:** A similar functionality has been discussed for inclusion in the PROACTIVE App.
Methods of communication analysed. Sirens, SMS and Mobile Applications are currently in existence. Further details can be found in D2.4.	**Feature:** Signpost existing communication methods, specifically Mobile Apps.
Current SOPs are not considered as completely easy to read and understand by all participants. The ideas provided by participant on possible improvement could be summed up in these points: • Clear, structured, easy to understand, "big letter + easy text". • Using plain and common language • Call for common elements of threats in contrary to scenario based and specific. • Call for nationwide SOPs with individual agencies obligations. • Use of aide memoires, checklists, bullet points, charts and schemes.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, SOPs.

Information shared with the public must be specific to the situation and location to be relevant	**Content:** Recommendation on the structure, format, type and level of information.
There was identified element of response where almost all participants of the workshop declared deficiency in SOPs. Information on vulnerable groups needs are not covered enough. Common agreement on this was accompanied by sum suggestion for improvement which do not necessarily connect to all documents: • Information how to "reach" and engage different vulnerable groups. • Information how these people react. • Helpful words and positive communication strategy • How to identify person with special needs • Communication with larger groups and with visual impaired people • Vulnerable citizens life value is equal to the other (need of balance and robustness of overall operation)	**Content:** Recommendation on the structure, format, type and level of information. Specifically, how to communicate with vulnerable people.

The research carried out in WP2 highlighted several key factors which then had to be considered during the development phase of the Web Based Platform and Mobile Applications as follows. While analysing the deliverables, it became clear there are similar themes relating to WP1 tying the initial research into the ongoing engagement.

Content of information to be shared:

Three communication aspects are evidenced in the WP2 deliverables; LEAs to LEAs, LEAs to citizens and LEA's to other agencies, including citizen agencies, all of which have the concurrent theme of pre-education prior to an incident. This includes, but is not limited to, disaster communication (operational), containment, evacuation and decontamination procedures, health specific instructions, risk communication and guidance documents, specifically addressing the needs of vulnerable groups during a CBRNe incident. The reasoning behind is similar to that identified in WP1 in terms of reducing anxiety and encouraging self-efficacy, however an additional concern is raised around the level of information that should be shared so as not to incite unnecessary panic with the public community.

The research further suggests increased education around the needs and complexities of vulnerable citizens will ensure expectations are met on both sides. At present documentation in this area is limited. The PROACTIVE Web Based platform and Mobile Applications again addresses the concept of communication needs by offering 2 key functionalities: 1). An area to share relevant information directly with the public, pre-incident and 2). An area for LEAs and Security Policy Makers to share information, e.g., guidance policies and operational procedures, confidentially.

Operational Communication

Inter-agency communication relating to operational principles is raised several times in WP2. The general concept being there is a lack of consistency in the research to suggest efficient

communication is currently taking place. In addition, no principles for vulnerable groups were found in any of the main documents analysed. The PROACTIVE Web Based platform and Mobile Applications have been developed to accommodate the storage and sharing of such documents should they exist in the future.

The research also highlights agreed protocols between LEAs and commercial or industrial organisations should be in place to support the recovery effort. The PROACTIVE Web Based platform and Mobile Applications have been developed to accommodate such protocols for storage and sharing.

During the incident, the research notes that alerts around the status of the attack as it happens and what the public need to do is imperative in reducing panic. The PROACTIVE Web Based platform and Mobile Applications have been developed to accommodate the provision of live alerts by LEAs.

Evidence and information gathering is important during any CBRNe attack. The PROACTIVE Web Based platform and Mobile Applications have been developed with this in mind and support the public to share information about the incident directly through the Mobile Application.

Accessibility

Work Package 2 addresses accessibility in relation to the provision and receipt of information by the wider public but also vulnerable citizens. Aside from the method of communication referenced in WP1; appropriate language complexity, multiple languages, pictographic forms, and sign language, it was noted citizens may not have access to the internet or could be computer illiterate. On this basis it was recommended multiple platforms should be used to communicate consistent messages to the public and should if possible be available in print form. The PROACTIVE Web Based platform and Mobile Applications have taken these considerations into account and looked at options for improving accessibility and consistency, for example information will be available for multi-agencies to download and share internally or with the public, in addition the Mobile Applications have been developed with the intent of being interpreted effectively by a screen reader. Further information can be found in the accessibility section of this deliverable.

Additional Functionality

As referenced in WP1, there is a requirement for citizens to be informed about loved ones and pets during an incident, this will be addressed during the 2nd phase of development.

WP2 highlighted a fundamental issue during an attack is the inability to send out consistent and clear messages to general, non-specific queries. The PROACTIVE Web Based platform and Mobile Applications include an FAQ page to allow LEAs to address the key questions the public may ask during a CBRNE attack.

It was identified Emergency Apps do exist. These Apps will not be replaced by The PROACTIVE Web Based platform and Mobile Applications; however, we would like to further understand whether there is potential for collaboration and/or signposting the existing Apps.

Discussions are ongoing to understand the feasibility/ benefits of a database listing the contact details of vulnerable citizens to allow easy contact during an emergency. This already exists in

Czech; OPIC. Further research will be carried out to determine whether this would be beneficial to the PROACTIVE Web Based platform and Mobile Applications.

3.3. Work Package 3 Input

In each of the tasks/ deliverables referenced in *Table 3 - Work Package 3 Input to the Technology Toolkit*Table 1 - Work Package 1 Input to the Technology ToolkitTable 2 - Work Package 2 Input to the Technology Toolkit, the key outcomes relevant to the development of the PROACTIVE Web Based platform and Mobile Applications have been addressed in terms of content and functionality relevant to the Engagement of Civil Society, including Vulnerable Citizens.

Table 3 - Work Package 3 Input to the Technology Toolkit

WP3 Engagements of the Civil Society including vulnerable citizens	**WP4 Toolkit for LEA's and Security Policy Makers**
T3.3 – Engagement vulnerable groups of citizens.	Workshop held on the 26th of February 2021. The outputs will be included in D5.3
D3.3 - Report on the workshop with vulnerable citizens	
Information needed during an incident: 1) what the public must do (i.e., instructions); 2) why compliance is important; 3) provide information and updates about ongoing security efforts; 4) provide details about loved one's whereabouts (e.g., be clear about which platform and which train was targeted).	**Content:** High level procedures in terms of evacuation to be shared with the public to further educate expectations during an event.
Additionally, it was also mentioned that the first on the platform are the first responders and they must inform the public quickly.	**Feature:** Live alerts/ notifications can be distributed via the Mobile Application prior to and as the First Responder arrives on site
A credible spokesperson should be used to speak to the media and public outside of the scene.	**Content:** Credibility of sources
Another CSAB member added that instructions on emergency decontamination, doffing, and the closest source of water are also very important factors that should be communicated to the public.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.

It may be beneficial to think of communication in terms of layers, or a matrix. For example, on-site communication should have clear instructions and provide information on why compliance is important (e.g., take off clothes, as they might be contaminated). For wider communication (i.e., individuals not directly involved in/ affected by the incident), it should be aimed to direct people away from the scene and close off the area. There should also be layers consisting of public announcements and social media response; a news and media level; and a political level.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.
Another CSAB member commented that the public, specifically the elderly, should be made aware that there can be a case of terrorism or a disaster (e.g., a fire) in railway stations and on platforms, and that "we are living in another world from 20 or 30 years ago". Additionally, in general, awareness regarding these incidents must be supported by information (e.g., how to manage such a situation).	**Content:** Recommendation on the structure, format, type and level of information
Official communication should be honest, empathic, assertive and reliable.	**Content:** Recommendation on the structure, format, type and level of information
Communication should aim to reduce anxiety, by providing information to enhance self-efficacy.	**Content:** Recommendation on the structure, format, type and level of information
The CSAB then discussed methods of communication that should be used in the event of a CBRNe incident. There was a suggestion of displaying a sign language interpreter on a digital screen to enhance accessibility to information for those who are hearing impaired.	**Accessibility:** method of communication
Another CSAB member stressed the importance of communicating information in different ways, particularly, for example, for those who are deaf; information that is made available to help protect the public should be accessible to everyone. Providing information in other languages, pictographic forms (with a preference for real photos in comparison to icons or diagrams), and using cartoon characters to appeal to children, were all additional methods of enhancing communication suggested by the CSAB.	**Accessibility:** method of communication

In terms of logistics, one CSAB member noted that "there is only so much first responders can have with them" as these resources would have to be in every vehicle used and therefore inexpensive. With this in mind, clear and easy to use pictorial aids, translators in case of emergency, and training in nonverbal communication could be preferable. One CSAB member stated that at least 5% of responders should know foreign languages, in this respect technology was also mentioned as having potential to aid communication.	**Accessibility:** method of communication
Information should be provided in multiple languages, pictographic form, and sign language.	**Accessibility:** method of communication
Multiple platforms should be used to communicate with the public, with consistent information being provided across platforms.	**Accessibility:** method of communication
Information should be available in writing (i.e., print form), where possible, using non-complex language	**Accessibility:** method of communication
Institutions should not exaggerate the superiority of their knowledge and judgement during risk communication and should not assume that the public will not understand important messages when they are communicated clearly and explicitly.	**Content:** Recommendation on the structure, format, type and level of information.
One CSAB member stated that people who live near a chemical facility should be educated on shelter in place, evacuation and wind direction as a matter of importance. It was also stated that people who live near nuclear power plants should have potassium iodide pills in their home first aid kits to counter radiation effects if there were to be an incident.	**Content:** Specific information around evacuation near a nuclear power plant
One CSAB member stated the importance of building resilience towards misinformation (i.e., fake news). This was agreed upon by the CSAB, and one member stated they have had first-hand experience trying to educate the public with social media and information sessions on CBRNe incidents; but the public are not retaining information or changing their behaviour as they do not perceive CBRNe incidents to be an apparent risk. Methods to educate the public were then discussed. Suggestions included: creation of a communication matrix (i.e., "1. on-site, 2. off-site incident related, 3. inform the public, 4. inform the media etc") to allow information to be pre-prepared and have guidelines on all communication levels;	**Content:** Recommendation on the structure, format, type and level of information. Specifically, educational information.

have easily accessible information available in community centres for the elderly; and to disseminate information about ongoing campaigns to community stakeholders as a way of reaching the community.	
Additionally, there was discussion around pre-incident information and CBRNe education having potential to induce anxiety and catastrophising thoughts, especially for children. However, there was preference from other CSAB members that teaching children in schools on how to react during CBRNe incidents and educating them on important factors (e.g., the CBRNe acronym and logos, the decontamination process through an exercise, and importance of stay in place), will be highly beneficial as they will hopefully also transfer the information to their family.	**Content:** Specific to education of school aged children
One CSAB member stated that general data protection regulation issues should be investigated, as during the COVID-19 pandemic some cities/communes were asked for addresses of disabled people in their area, to allow them reach out to provide aid; however, their company were not allowed to pass on these details. If this is wanted, special contracts are required to make this possible.	**Ethical Restrictions:** A feature to share information of different vulnerabilities has been discussed within the Technology Toolkit. Due to ethical restrictions, we are researching this further
Where there is increased risk (e.g., where a town or city is located where there is a chemical facility or nuclear reactor), people should receive in advance what to do in the case of a CBRNe incident, which will reduce anxiety and worry.	**Content:** Specific information around evacuation near a nuclear power plant
The public should be educated on how a CBRNe incident may play out, e.g., procedures may be delayed.	**Content:** Recommendation on the structure, format, type and level of information. Specific to education.
It would be beneficial to prepare pro-active social media campaigns and get people to know where to go for good information during events.	**Dissemination and Exploitation**: Market awareness of CBRNe Information.
Information should be available on how to distinguish fake news, i.e., which sources are correct, and which are not.	**Content:** Credibility of sources
The public should be educated on who to turn to for support and further information in the event of an incident.	**Content:** Recommendation on the structure, format, type and level of information. Specific to education.

More consideration should be given to developing policy and procedures to assist those with mobility issues (e.g., relating to service animals and essential mobility aids) during CBRNe incidents.	**Content:** Recommendation on the structure, format, type and level of information. Specifically, guidance and policies.
Information provided by authorities should be pre-planned, where applicable, to ensure prioritisation and consistency, provide uniformity and advocate cohesion.	**Content:** Recommendation on the structure, format, type and level of information
D3.4 - Report on the survey on common approaches of the civil society	
Some of the recommendations are about exchanges between civil society organizations and emergency responders. One of our findings in the study was that there are rarely exchanges between civil society organizations representing vulnerable groups and responders / authorities in the field of CBRNe. Here we definitely see a gap that needs to be closed (e.g., by promoting exchange formats between the mentioned groups).	Within the App a list of civil society organizations (possibly with contact details / web address) representing vulnerable groups that the emergency services can access would be conceivable. **Feature:** Contact list available in the Technology Toolkit.
If we promote the App to civil society organizations, it would also be conceivable to ask during the registration process whether one represents a civil society organization and, if so, whether one is willing to share the organization's contact details in the app. These contact details could then be added to the list of civil society organizations. Perhaps one could also ask during the registration process if organizations are interested in certain types of collaborations (CBRNe exercises, project participation, etc.).	**Feature:** Additional request for information during registration process. To be discussed further on the 26th of February.
Our study showed that the needs of vulnerable groups are rarely considered in CBRNe situations / CBRNe SOPs. Moreover, it has been shown that CBRNe information are often not provided in additional language formats (e.g., Braille and sign language).	To provide more CBRNe information for vulnerable groups, a library could be created in the App where info papers for vulnerable groups, books on CBRNe, etc. could be uploaded / linked. In this area a lot of information is already available. **Feature**: A section in the Technology Toolkit has been developed to accommodate 'Additional Resources'

The research carried out in WP3 highlights several key factors which then had to be considered during the development phase of the PROACTIVE Web Based Platform and Mobile Applications as follows. While analysing the deliverables, it became clear there are similar themes relating to WP1 and WP2, tying the initial research into the ongoing engagement with both the PSAB and CSAB networks.

Content of information to be shared:

The research completed in Deliverable 3.3 looks at the content requirements from the perspective of the citizens, including those more vulnerable. As a result, more detail is available on the expected structure and delivery method of the content. It was stated multiple times the level of information shared should be relevant to the audience receiving it, to accomplish this, a matrix structure was proposed, onsite instructions, social media responses and political information. The onsite information is key during the initial response to the incident, it needs to be delivered quickly, be concise, instruction based and reiterate why compliance is important. The PROACTIVE Web Based platform and Mobile Applications were built with this in mind and include a live notification section, in an attempt to support first responders in delivering information from a credible source.

Other content requirements include information that can be shared with the public prior to an incident, this includes decontamination processes, evacuation processes, and general educational information relating to CBRNe incidents. To accommodate this, the PROACTIVE Web Based platform and Mobile Applications have 2 key features, 1) a pre-incident information section and 2) an additional resources section. Combined, these sections allow users to find existing information directly in the PROACTIVE Web Based platform and Mobile Applications and gain access to other sources of information, such as, websites, other Mobile Applications or Leaflets.

Accessibility

Several methods to improve accessibility were identified in the research, sign language interpreters for live updates, multiple languages, pictographic formats with a preference to real photos and cartoon characters to name a few. In addition, it was noted that first responders should be more prepared in the art of non-verbal communication, however this is resource dependant. The PROACTIVE Web Based platform and Mobile Applications can support multiple formats for information sharing at the discretion of the LEA. When resources are limited the Proactive Web Based platform and Mobile Applications would be able to reach a mass audience in a very short time.

The CSAB members also noted in the research the information should be available in multiple platforms. To ensure consistency the PROACTIVE Web Based platform and Mobile Applications can advise the agreed process for communication as well as host the information to be shared.

Additional Features

Exchanges between Civil Society organisations representing vulnerable groups and first responders is rare. To aid this, a contacts section is available in the PROACTIVE Web Based platform and Mobile Applications enabling key organisations to be listed for reference during an incident. This is available to LEAs and the general public. To further encourage organisations to be added to the list, there has been some initial discussions around adding a section in the registration section for organisations to list their details. This will be discussed further before adding it as a development task for the next iteration.

3.4. Work Package 5 Input

Work Package 5, in particular Task 5.1 and the corresponding D5.1 aimed to understand the perceptions of members of the public on draft pre-incident public information materials, with a specific focus on the needs of members of vulnerable groups. The following conclusions were drawn and have been analysed against the PROACTIVE Web Based platform and Mobile Applications to determine whether any future adaptations are required.

Table 4 - Work Package 5 Input to the Technology Toolkit

WP5 Toolkit for Civil Society Organisations	WP4 Toolkit for LEA's and Security Policy Makers
D5.1 Initial pre-incident public information materials for CBRNe terrorism	
Participants reported that the instructions were unclear and too long. The use of colour and graphics might help to reduce information overload and increase engagement with the materials.	Content can be uploaded in multiple formats, allowing the use of images, graphics, videos etc. Accessibility in terms of non-sighted citizens will be reviewed in this instance.
Participants were generally negative about the use of an app, with issues of phone memory space being frequently mentioned. A multipronged approach was suggested for communication and dissemination of the materials, with traditional forms (e.g., leaflets, or billboards in public spaces) being widely supported, especially in public places. Based on the discussions reported herein, it is recommended that: a) adverts for the PROACTIVE App are clear on the amount of memory that the App will require, and b) the PROACTIVE App include downloadable PDF versions of the pre-incident information that could be downloaded and disseminated using more traditional methods by relevant groups (e.g., community groups, responders, etc).	A similar recommendation is identified in WP3. The Technology Toolkit has been developed to allow for documents to be downloaded. During the exercises further questions will be asked to address this issue and to determine if there were any features that would encourage the uptake usage of an App during an incident.
Participants were mostly confident and willing to take the actions in the materials. However, some participants suggested that they might wait for others to take the actions or wait for the emergency services. It is suggested that including phrasing in the materials which suggests others will also be taking the actions may aid in increasing compliance.	The Technology Toolkit can be used here to ensure the information is shared quickly and efficiently. Live notifications issued by LEAs may to some extent provide the confidence sought. This theory can be tested during the exercises.

Finally, many participants reported being reassured to receive pre-incident public information materials, yet some participants commented that without any context the information may scare them. A brief introduction to the materials on why they are important might help people contextualise the information and reduce anxiety.	The relevant level of information can be uploaded and shared through the portal.
Throughout the discussions, several important points were raised regarding the importance of ensuring any materials are accessible by, and relevant for, all members of society, including members of the vulnerable civil society. The following recommendations are proposed to address these points and ensure that pre-incident information materials are appropriate for vulnerable groups: Firstly, the instructions need to be of a reading age which is appropriate for wider society. There may be scope to send the final materials to an expert in this field to check the reading age. Secondly, concern around how vulnerable groups (e.g., individuals with visual impairments) would access these materials could be countered by ensuring that the PROACTIVE App has the ability to read aloud any instructions or text displayed on the screen. In terms of undertaking the recommended actions, participants suggested that the materials also provide advice on how to help people with additional needs and vulnerabilities; such modifications could be developed in conjunction with representatives from the CSAB.	The Accessibility of the Technology Toolkit has been a consideration throughout the initial development phase. Further details on how we are currently addressing this issue is detailed in Section 3.7. During the exercises further testing and input will be required to ensure as many different vulnerabilities have been addressed as possible.

As a result of the research carried out in Task 5.1, it is clear the features and content of the PROACTIVE Web Based platform and Mobile Applications are key in supporting any changes to the public perception of using Mobile Applications during a CBRNe incident. The flexibility of the content is also key to enable the correct information is sent out addressing the needs of the public, including those more vulnerable. Finally, the concept of accessibility also plays a role in the usefulness of any Mobile Application. Section 3.7 addresses this further, however future tabletop exercises will verify the existing approach and propose new ways in which the project can work with CSAB members to support accessibility.

In preparation for D5.2 - final pre-incident public information materials for CBRNe terrorism, the work completed in D5.1 enabled the following pre-incident information sheet to be produced. This will be included as the first piece of content in the PROACTIVE Web Based platform and Mobile Applications:

- If you think you have been exposed to a harmful substance, you should move away from the hazard as soon as possible to prevent further exposure. You should remain at the scene as emergency responders will soon arrive to help you.
- Get fresh air if possible – this can help with any symptoms you may be experiencing. Do not eat, drink, smoke or touch your face to avoid swallowing any of the harmful substance.
- Remove your outer clothing. Your outer clothing may have some of the harmful substance on it, and so removing this will help to reduce your exposure to the harmful substance. Try to remove clothing without pulling any clothes over your head, if possible. If this is not possible, try to avoid clothing coming into contact with your face whilst removing over your head.
- If any of your skin has the harmful substance on it, use a dry tissue or similar absorbent materials to either soak it up or brush it off. This will help to remove the substance from your skin. If your skin is itchy or burning, then rinse the affected area continually with as much water as possible.
- When emergency responders arrive, they may ask you to remove your clothing to your underwear and then wash yourself all over in a shower system that they will set up at the scene.
- You should not put your old clothes back on after removing the substance from yourself. Emergency responders will help to provide you with clean, uncontaminated clothing.

3.5. Work Package 6 Input

Exercise planning, although affected by the ongoing pandemic has continued to evolve in terms of the objectives the PROACTIVE project is aiming to achieve. Strategically, in partnership with eNOTICE, the exercises will evaluate the effectiveness of responses to a CBRNe incident focusing on harmonisation of procedures and tools that support the needs of civil society, including those citizens that are vulnerable. Tactically, the first field exercise aims to test combinations of selected tools and evolving procedures in response to a CBRNe attack incorporating the direct participation of members of civil society that includes vulnerable citizens and non-trained staff. Work package 6 has produced a list of 10 Tactical objectives aiming to address this strategy, some of which can utilise the PROACTIVE Web Based platform and Mobile Applications to do so:

Table 5 - Work Package 6 input to the Technology Toolkit

WP6 Joint exercises, evaluation and validation of the tools	WP4 Toolkit for LEA's and Security Policy Makers
Tactical Objectives	
To benchmark current practices against the recommendations from WP1, D3.1	Current practices highlight Mobile Applications are not used as a form of communication between LEAs and Citizens, largely as they are not available.

To test the effectiveness of the PROACTIVE App in supporting the needs of Civil Society	Section 3.3 Highlights the needs of the Civil Society. The Technology Toolkit has been developed to address these needs and will be tested in workshops, tabletop exercises and the field exercises.
Test if appropriate consideration is given to delivering policy and procedures to assist those with mobility issues (e.g., animals and mobility aids) during CBRNE incidents	The PROACTIVE research suggests current policies and procedures are not available and have made recommendations to address this. The recommendations and future policies/ procedures can be shared through the Technology Toolkit.
To further understand the needs of different vulnerable groups during CBRNe incidents	From the perspective of the Technology Toolkit, it has been developed in reference to international guidelines of the W3C. Please refer to section 3.7 for further details.
To test that messages are pitched at an appropriate level in terms of language and complexity	To support this objective, the Technology Toolkit supports multiple formats for data upload, providing the LEAs with the option to upload any content they deem appropriate.
To test the effectiveness of pre-planning and pre-incident information during emergency communication with the public	Following initial discussions as part of T6.2, it has been agreed some form of pre-planning and pre-incident information will be included in the Technology Toolkit. The Technology Toolkit will then be shared with half of the participants to test the effectiveness of the information during the field exercise.
To test the provision and suitability of public health messaging in an emergency	To support this objective, the Technology Toolkit includes a feature for LEAs to share information as live alerts during an emergency.
To gain an understanding of the additional requirements created through involving Civil Society in CBRNe exercises	The Technology Toolkit has been developed based on the research developed to date. Further development/ optimisation is expected based on the feedback received during upcoming tabletop exercises and planned field exercises.
To test if pre-planned information provided by authorities has been deployed in a consistent way and has been understood	To support this objective, the Technology Toolkit supports multiple formats for data upload, providing the LEAs with the option to upload any content they deem appropriate.
To gain an understanding of factors that may increase public compliance during CBRNe incidents	To support this objective, the Technology Toolkit supports multiple formats for data upload, providing the LEAs with the option to upload any content they deem appropriate. In addition, the concept of using an App during an incident will be tested.

The development completed to date regarding the PROACTIVE Web Based platform and Mobile Applications is based on research completed in WP1, WP2, WP3, WP5 and WP8. The planned tabletop exercises and field exercises will then not only act to verify the development completed to date but also to provide further optimisation of the PROACTIVE Web Based platform and Mobile Applications in terms of new features and updates/ amendments to existing features, as reflected in objectives 1, 2 and 8 in *Table 5 - Work Package 6 input to the Technology Toolkit*.

The remaining objectives in *Table 5 - Work Package 6 input to the Technology Toolkit*, refer specifically to the content that is or should be available and how effective it is in terms of supporting citizens and LEAs in managing the response to an emergency. The PROACTIVE Web Based platform and Mobile Applications have been developed to support communication through multiple methods; live alerts/ notifications, pre-incident information, sharing images and incident updates and content will also be shared via multiple formats; text, images, videos with subtitles, audio files etc. The flexibility of the PROACTIVE Web Based platform and Mobile Applications will enable the objectives listed to be tested providing valuable feedback for future development and research, not only in terms of the features available, but also the content.

3.6. Work Package 8 and 10 Input

Table 6 - Work Package 8 and 10 Input to the Technology Toolkit identifies the key areas relevant to WP4, derived from the deliverables documented in WP8. Each of the key points have been individually commented on to show their direct affect within the PROACTIVE Web Based platform and Mobile Applications.

Table 6 - Work Package 8 and 10 Input to the Technology Toolkit

WP8 Legal, Ethical and Acceptability Requirements	WP4 Toolkit for LEA's and Security Policy Makers
DATA PROTECTION	
Users of the system will be made aware of the limitations of the Toolkit, 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.	Rinisoft and ETICAS have finalised the privacy policy for inclusion in the Toolkit. It will be mandatory for a user to agree to the privacy policy before registering. In addition, an extended version of this policy will be available through a link on the home page at all times. The privacy Policy is available in Annex C.
Minimal Data to be Collected/ Stored according to D8,1 and D10.4. When (if) registering, the users' profile shall not demand any personal data. All data requested must be volunteered by the user and not compulsory. Only data which is necessary for the functioning of the system are to be collected. All data collected through the system are only to be used for the stated purposes.	Following the principle of data minimization, it has been agreed the only data to be collected during the registration process is an active email account. The purpose of this is to access additional functionality within the system (sharing incident information), to reset a forgotten password, to receive optional incident notifications and, where applicable for contact by the LEAs in relation to an incident.

Users of the system will be given the ability to opt out of the collection of personal and sensitive data about him or her or any 2-way communication	Users will not be requested to provide any personal data as a compulsory action (excluding email addresses and IP addresses). Any data they choose to share, text/ images/ location information is optional. Users will also have the right to subscribe/ unsubscribe to any automated incident notifications
Any personal Data collected is to be made available to the user upon Request and Users will have the right to access their personal data from the system and will have the right to rectify it, if needs be.	The minimal personal data collected will be made available to the user through their 'profile' section to update and amend. They will also have the option to unregister at any point. The amount of personal data to be subjected to ARCO requests (access, rectification, cancellation and objection) will be limited and adequately documented to ensure these rights.
Information on the Use of Cookies to be provided	Following the principles of security and purpose limitation, the toolkit will not use cookies for collecting data or tracking, but will use a cookie for logging in, which will identify the user to Rinisoft and will be used to determine what parts of the site they may access and what actions they may perform (for example the ability to share incident information or access restricted documents)
All data collected, stored, processed and retrieved by the system will be held and transferred through highly secure systems to prevent loss, damage or unauthorised access. Integrate security mechanisms of avoiding unauthorized access to pre-incident, real time and post-incident information. These systems should not be based outside the EU unless absolutely necessary. Establish security mechanisms, tools and protocols such as data pseudonymization, anonymization and encryption, to avoid data breaches.	The Toolkit uses an AWS server which is highly secure and allows for interoperability. It provides security concerning unauthorized access and storage encryption. Data breaches were tested in a working session conducted in February 2021. Based on the current testing deployment, data is also encrypted when it is transferred across the network (https). During a real deployment, the data will be encrypted as follows: • While crossing the network (HTTPS) • At rest, when stored on disk in the database (AES Disk Encryption) • When being transferred between the database and the application (TLS)

Images, voice recordings and video can be classed as personal data and need to be held as securely as other forms of personal data. This is especially the case if the image or voice of an individual who has not consented to using the system is inadvertently captured by a consenting user. In these cases, very careful consideration should be given before these materials are released on the public.	Extensive discussions with the LEA's during the progress meetings allowed us to implement a process that meets this requirement, as follows. User shares incident details (including optional images). Incident sits in a holding queue for review by the LEAs. Once authorised the LEA will share a separate incident report with the relevant details to the public. This data filtering process will ensure secure data management, minimize risks of discrimination, privacy breaches and false positives.
System should allow for both registered and anonymous users.	To achieve maximum impact, this recommendation was discussed at several meetings with the consortium LEA's. It was agreed only registered users would be able to report an incident, however ALL users would have access to any pre, during, post incident information.
Users will be notified of the parties to whom the data may be transferred, the conditions for transferring the data to third parties, and the rights of the individual (data subject) concerning further processing of their personal data. System shall not disseminate personal information.	There is no intention to transfer data to third parties outside of the consortium. However, should this change, users will be made aware through the privacy policy, which will have to include explicit information about these third parties and data exchange purposes. Recommendations for the management of the system in D8.4 will address these policy options, providing recommendations for the system's governance.
Maps must be designed in such a way that no particular home or address can be identified.	The map used allows only for the general street area to be identified and not a person house to account for this recommendation. However, as the user has the ability to free text an address, the additional measure of pre-approving information before being made public will protect addresses being identified publicly.
Users shall be required to sign a consent form and disclaimer before accessing the data.	The App will be tested by the PSAB and CSAB members as well as during the planned field exercises. It was agreed that a consent form will be signed and collected outside of the App to ensure consistency. A separate consent protocol, including a complete Privacy Policy, has been developed and integrated into the Apps/Web.

ACCEPTABILITY	
Effort expectancy, including meaningful navigation, clear sections for each function, multilanguage and intelligible branding should be considered by design.	The branding is consistent and clear across the Web Based Platform and Mobile Applications. The navigation, web pages and use of communication methods (text, images pictographic) have been chosen considering the use of a screen reader by citizens who are visually impaired.
Social influence should be ensured through inclusive visualization and communication in terms of gender, disability and age. Multiple sources of information should be available.	The content within the PROACTIVE Technology Toolkit is free source, meaning the owner (LEA) has the option to include all relevant sources of information in multiple formats. Still, possible gender, race, age or other relevant biases will be assessed in D8.4.
PROACTIVE should foster access in terms of transparency to the systems information. This includes data about functionalities, goals and security conditions of the app.	The above-mentioned Privacy Policy has been designed taking these aspects into account. Recommendations for the management of the system in D8.4 will also address these aspects.
Monitor and prevent algorithmic bias and discrimination.	The protocol for filtering collected data by end-users addresses this aspect. This aspect will also be considered as part of D8.4 social impact assessment.
Develop tools and protocols for examining the accuracy, quality and veracity of personal data used in CBRNE incidents.	The protocol for filtering collected data by end-users addresses this aspect.

The key points have been divided into 2 areas of interest, Data Protection and Accessibility. To determine the relevant actions to be taken during the development phase, ETICAS and Rinisoft held several meetings to ensure the key points were reflected in the PROACTIVE Web Based platform and Mobile Applications.

Data collection and data purposes are highlighted throughout Table 6, when determining the best approach to ensure legal and ethical compliance, taking into consideration the functionality and purpose of the PROACTIVE Web Based platform and Mobile Applications it was agreed minimal personal data would be collected. The interim version only requests an email address and password as mandatory for registering. Other data includes free text and images which the citizen may choose to upload for information. This data is not shared with the public unless it has been verified by the LEA responsible for the PROACTIVE Web Based platform and Mobile Applications. The full details of data usage are detailed in the privacy policy which is available within the PROACTIVE Web Based platform and Mobile Applications are accessible to those using a screen reader. It is important to note that future iterations, following the planned workshops and field exercises may alter the way data is captured and used. The ethical and legal implications will always continue to be referenced and an updated privacy policy will be provided if necessary.

Similar to the recommendations from previous WPs listed in this deliverable, acceptability is highlighted through the ethical requirements as detailed in Table 6. This includes the design of the system, in terms of navigational aspects and ensuring all abilities of citizens, including those more vulnerable are considered. The other element of accessibility incorporates the concept of transparency, in terms of the intended purpose of the PROACTIVE Web Based platform and Mobile Applications but also the data being collected. To ensure this requirement is met, protocols for system usage are in place regarding the filtering of data and any further management issues, particularly around data breaches, will be addressed in Deliverable 8.4.

3.7. Accessibility Functionality for Vulnerable Citizens

Accessibility in terms of the PROACTIVE Web Based platform and Mobile Applications has been a key priority from the initial development phases. The research from previous Work Packages, identified in this deliverable, indicate some of the barriers to using a Mobile Application is the necessity, battery life and accessibility. Accessibility has been addressed from the technical perspective, including the layout, design, features and content.

Accessibility during development

When developing the PROACTIVE Web Based platform and Mobile Applications, two key categories of vulnerable user groups were identified, sighted and non-sighted. To accommodate non-sighted users, a number of design features had to be considered during the development phase, these included the formatting of headings, lists, graphics and logos, sequences and hierarchies as well as colour contrast ratios and self-speaking links. Once developed the engineers were able to use a number of available tools to test the accessibility, in particular a screen reader and keyboard. The PROACTIVE Web Based platform and Mobile Applications will be further tested by the CSAB members to verify the accessibility and identify any further adaptations that can be considered.

Accessibility through content

When it comes to communication between LEA's and Citizens, including those more vulnerable, the content proposed for inclusion in the PROACTIVE Web Based platform and Mobile Applications ranges from pre-incident information, live alerts, incident reporting and additional resources. The information itself should be concise, non-complex and use a mixture of text, pictographs and images to convey the message. The delivery method should be flexible in terms of text, video (sign language and/or with subtitles), audio files etc. The PROACTIVE Web Based platform and Mobile Applications have been developed with this flexibility in mind, supporting free text for live alerts and the option to upload multiple data formats for sharing information. In addition, the data, where possible will be available as plain text built into the web page to support screen readers and as a downloadable document, for printing and dissemination.

Beyond these dimensions of accessibility, other design elements or functionalities have been identified with the help of the members from the civil society in the Mobile Application co-design process (see section 3.3).

4. END USER REQUIREMENTS

The initial end user requirements were derived from the Description of Action in terms of the work completed in Work Packages 1, 2, 3, 5, 6 and 8 and the experience of Rinisoft, which provided a baseline for the minimal functionality of the system, including the web collaborative platform, and mobile applications. The full list of the overall proposed requirements can be found in Annex A and were discussed with all consortium members during Progress Meetings 3 and 4. From this, the core requirements were agreed, and the initial designs were implemented, detailing the graphic user interface and the key functionalities in relation to the original proposed exercise, scheduled for M18 in Rieti, Italy. However, due to the ongoing COVID-19 pandemic, and the proposed first exercise being postponed, further feedback has been sought through network partners and planned webinars. Due to the proposed iterative development of the PROACTIVE system, we realise further requirements will be identified, particularly in relation to customisation for the project scenarios. Further requirements for the web collaborative platform and mobile application for LEAs and Security Policy Makers will be documented in D4.2, and D4.3 respectively, both of which are due in M36.

4.1. Core Requirements

Table 7 - Core Requirements, provides the high-level core requirements identified in preparation for the initial version of the web collaborative platform and mobile applications for both the LEAs/Security Policy Makers and Vulnerable Citizens, a more detailed list of core requirements can be found in Annex B at the end of this deliverable and will be referenced for future development as required. It is important again to highlight the core requirements will not differ between the mobile applications for the LEAs/Security Policy Makers and Vulnerable Citizens, the way they are used may however vary.

The design phase included a detailed consultation with the project partner LEAs who proposed core requirements and reviewed the final list. It is important also to note, during the design phase Rinisoft discussed elements of security, ethical procedures and legal requirements with consortium partners involved in WP8 and in particular with the WP8 leader ETICAS to ensure the system is compliant with all these important requirements. The 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. ETICAS will aim 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. These 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.

Table 7 - Core Requirements

CORE REQUIREMENTS	
Graphic User Interface	Simple design reflecting PROACTIVE branding. Accessibility across web collaborative platform and both Mobile Applications
Direct Messaging	The ability for LEAs and Security Policy makers to interact privately. The ability for citizens to send direct messages will vary between scenarios
Forums	Open discussions between all stakeholders
Registration	Not mandatory – registering will increase level of access rights
Legal & Ethical Requirements	Working with ETICAS and CBRNE, GDPR, disclaimers and consent forms will be factored into the system
Notification of Incidents	Notify LEAs of an incident using a map-based system
Data Storage	Secure storage of information input to system
Geo-Location	The ability for the system to recognise the location of an incident(s)
Information Sharing	Ability to share pre-incident information with all users in multiple formats (text, video, audio)
Missing Loved Ones	Ability to locate humans and pets during an incident
Contact Information	List of organisations relevant to vulnerable groups

4.2. Functional Requirements – First Field Exercise

The consortium originally agreed it would be beneficial to have the first iteration of the system available for testing during the first field exercise in October 2020. The system would have limited functionality as per *Table 8 - Functionality* for *the first field exercise*, to enable users to provide initial thoughts on usability and content. As the exercise is no longer happening in M18, the App will now be presented at the PROACTIVE mid-term conference on the 28th of October 2020. Future updates of the web-collaborative platform and mobile application for LEAs/ Security Policy Makers will be included in D4.2, D4.3 respectively.

The first field exercise has now been proposed further. Following discussions with CBRNE Ltd, the Mobile Application for Civil Society, (including Vulnerable Citizens) will be the primary focus for feedback, however, to enable this, the functionality for the web-collaborative platform and mobile application for LEAs/ Security Policy Makers will have to be developed in parallel to support

information sharing and bi-directional communication. Allowing for the additional time, the intention is to further develop the functionality to include some additional features in

Table 9 - Access Levels, in particular the forum capabilities to enable the exercise to gather feedback during and following the event.

Table 8 - Functionality for the first field exercise

Functionality	
Inter-Agency Information Sharing	The ability to converse directly with relevant stakeholders to discuss operational aspects in terms of information sharing
Pre-Incident Information	Information from T5.1 will be available in the system for users to reference
Post Incident Information	Information post incident to be provided to stakeholders, specific to the scenario exercise as a lesson learnt.
Links to Available National Apps	Countries with existing Apps for crises events will have the link signposted in the PROACTIVE portal
Notification Alerts	Live notifications to be provided by LEAs at all stages of the incident
Existing News Feeds	News feeds from the relevant countries/ areas will be linked to the PROACTIVE Mobile Application, to create a central hub for information
Data Analysis	LEAs will have access to data, specifically number of users on the platform and at what stages the platform was used etc.

4.3. Functional Requirements - User Categories

Initial discussions with the end users in the consortium highlighted a number of differences related to functionality in terms of access rights for different user groups, which inevitably affects the way the system will be used by each group.

Table 9 - Access Levels, highlights the core features identified in Section 3.1 and 3.2 broken down to address the features which will be available to LEAs and Security Policy Makers. LEAs will have additional access to the 'Admin' functionality of the system, essentially controlling the information being shared internally and publicly. This will however vary on a scenario-by-scenario basis; the table below shows the highest level of access for Security and Policy makers and will be reviewed during each of the planned exercises. Access levels for public users (including Vulnerable citizens) can be found in D5.3.

Table 9 - Access Levels

Functionality	LEAs	Security Policy Makers
Display EU flag and Grant Number	Yes	Yes
Privacy Policy, data protection and access to potential data, consent form and disclaimer	Yes	Yes
Register/ Login (only email addresses) Option to subscribe to additional information (tick box)	Yes – mandatory	Yes – mandatory
Link to 'About PROACTIVE' Page	Yes	Yes
Contacts Page (LEAs/ Policy Makers/ Hospitals/ Health Advisors etc)	Yes	Yes
Link to Direct Messaging	Yes	Yes - will vary per scenario
Link to Forums	Yes	Yes
Link to CBRNe Information	Yes (to include operational and policy information)	Yes (to exclude operational information if confidential)
Link to Available Support Tools (Existing Apps/ websites)	Yes	Yes
Link to push notifications (automated early warnings)	Yes (multiple data formats)	Receive only (multiple data formats).
Link to available News Channels	Yes	Yes
FAQ page (pre, during and post incident)	Yes	Yes

5. SYSTEM REQUIREMENTS

5.1. System Functionality

Following a technical analysis of the user requirements, the following section outlines the non-functional requirements, whereby the user requirements are reviewed to determine the systems operational functionality. This covers areas such as the legal, ethical, security, accessibility, scalability, usability and deployment. The system will be made up of two main components:

5.1.1. ASP.NET Core 3 Stateless Web Service

- Hostable on traditional on-site or cloud servers;
- Hostable as a stateless Lambda service on AWS or Azure;
- Backed by Postgres 13 SQL server.

5.1.2. Angular 9 Reactive Web Application

- Reactive design supports all device sizes, smart phone, tablet & pc;
- Available as a Progressive App on iOS and Android;
- Designed as an accessible application with simple UI;
- Supports screen readers and other accessibility tools.

Figure 2 Linux Based Server shows the logical topology of an example single server deployment of the Proactive Application. The top half of the diagram shows the supported devices & web browsers (Safari, Firefox & Google Chrome), which allow the users to connect to the Server via a secure HTTPS connection. The bottom half of the diagram shows the connections & relationships between the installed components on the server:

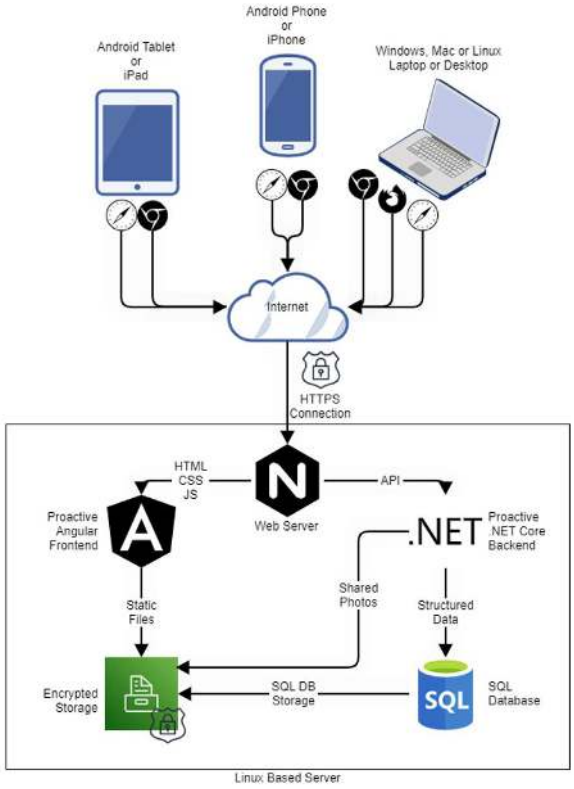


Figure 2 Linux Based Server

5.2. System Security

The system will enforce the following security protocols:

- SQL Data Protected by Full Drive Encryption: aes-xts 256;
- Client-Server communication protected by Transport Layer Security (HTTPS);
- System access is controlled by application-level authorisation. Unauthorised users (not logged in) and members of the public may not view sensitive information or edit publicly accessible information directly. In addition, API Key authorisation will be available for external integrations.

5.3. System Interoperability

- The PROACTIVE platform exposes a secure REST API that allows for external systems to integrate;
- The integration API can be used by authorised partners to push data into the system in real time;
- The home page has links to external applications and resources.

5.4. Graphic User Interface

The PROACTIVE portal's GUI is an Angular 9 Reactive web application that provides users with an accessible user interface to carry out the main functional interactions required of the PROACTIVE platform. The GUI is designed to cater for a diverse range of users and devices, supporting:

- Landscape and Portrait aspect ratios;
- Screen sizes from 10cm to 50+cm;
- iOS phones and tablets;
- Android phones and tables;
- Laptop & Desktop browsers; Chrome, Firefox, Edge, Opera and more;
- Screen readers & accessibility tools;
- Progressive Web App to provide offline functionality and asynchronous file uploads.

5.4.1. PROACTIVE Portal Login and About Us Pages

Allows registered users and site admins (LEAs) to log into the portal and access application features not available to unregistered users. It is not however mandatory to login to the portal, information on CBRNe issues will be available without registering. Project information for members of the public; this page details the grant agreement information in addition to the purpose of the project. Should users require further details they will have the option of requesting further information through the PROACTIVE email or via the website.

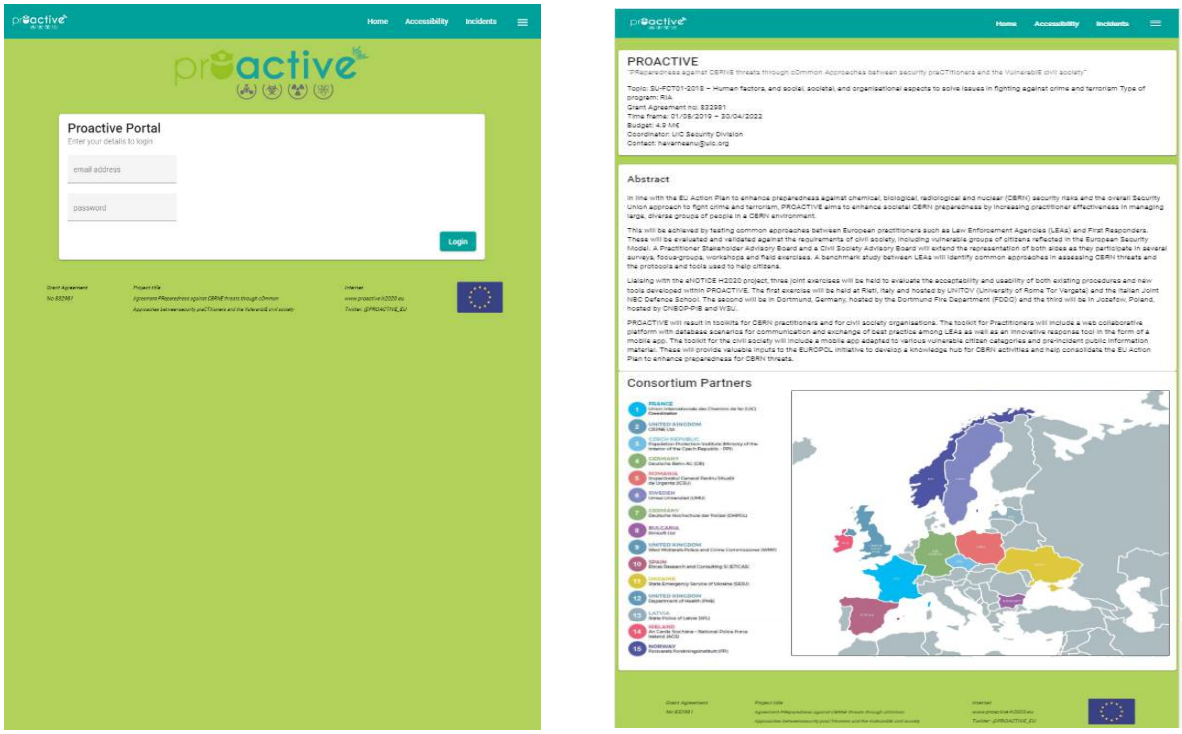
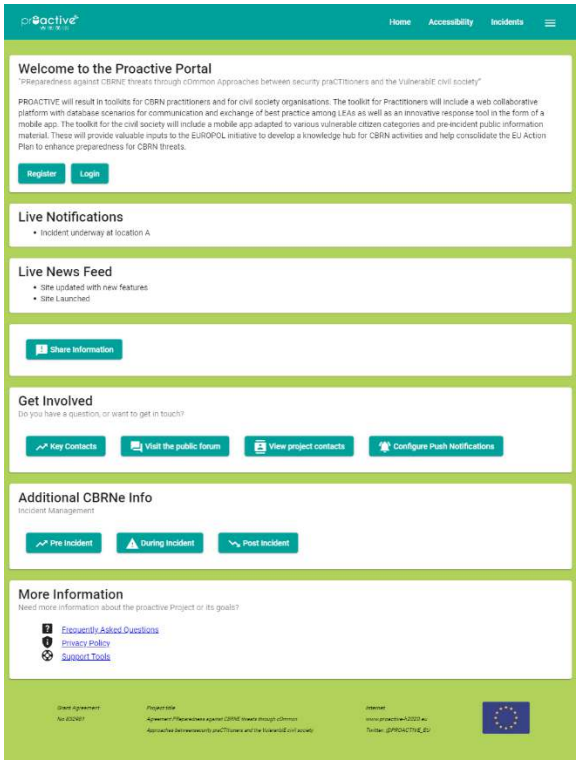


Figure 3 Registration and About Us Pages

5.4.2. Portal Home Page and Key Contacts

A landing page for users containing up to date notifications and news feeds along with links to external information sources and contacts. This will act as the central hub for the technology, enabling users to navigate to the relevant areas of interest. This page will also act as a main notification page, providing users with live updates either directly through the PROACTIVE Mobile Application or through link to national systems and news channels.



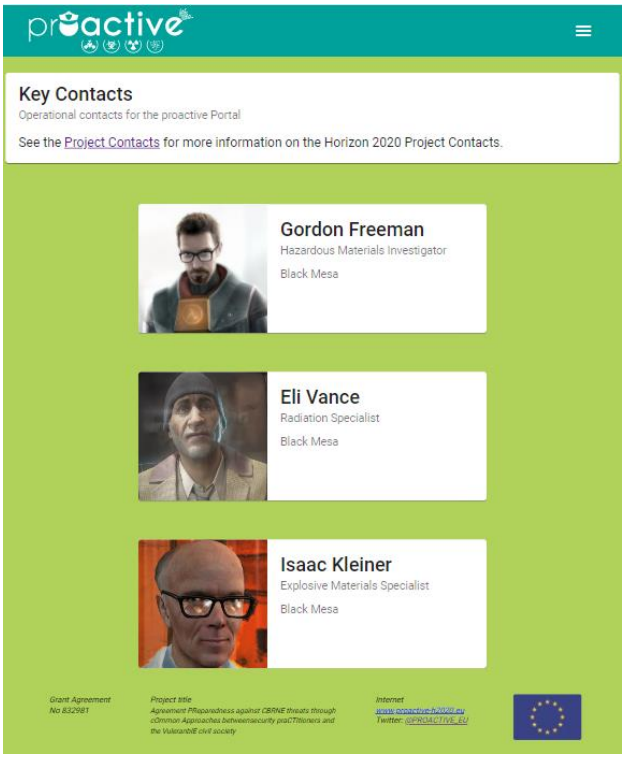


Figure 4 Home Page and Key Contacts

5.4.3. Information Sharing

Live updated map of current incidents along with a summary of incident status. Registered users will have the capability to notify of an incident in their area. Basic details including date logged, the status and type of incident will be required in addition to the location. All incidents will be moved to a holding queue, in which LEAs will have direct access to the review and verify the incident. Once validated the LEA can then choose to release an update on the incident utilising the map functionality available in the Mobile Applications. Furthermore, LEAs will have the option to monitor and update the incident using the live notifications functionality once the incident has been investigated.

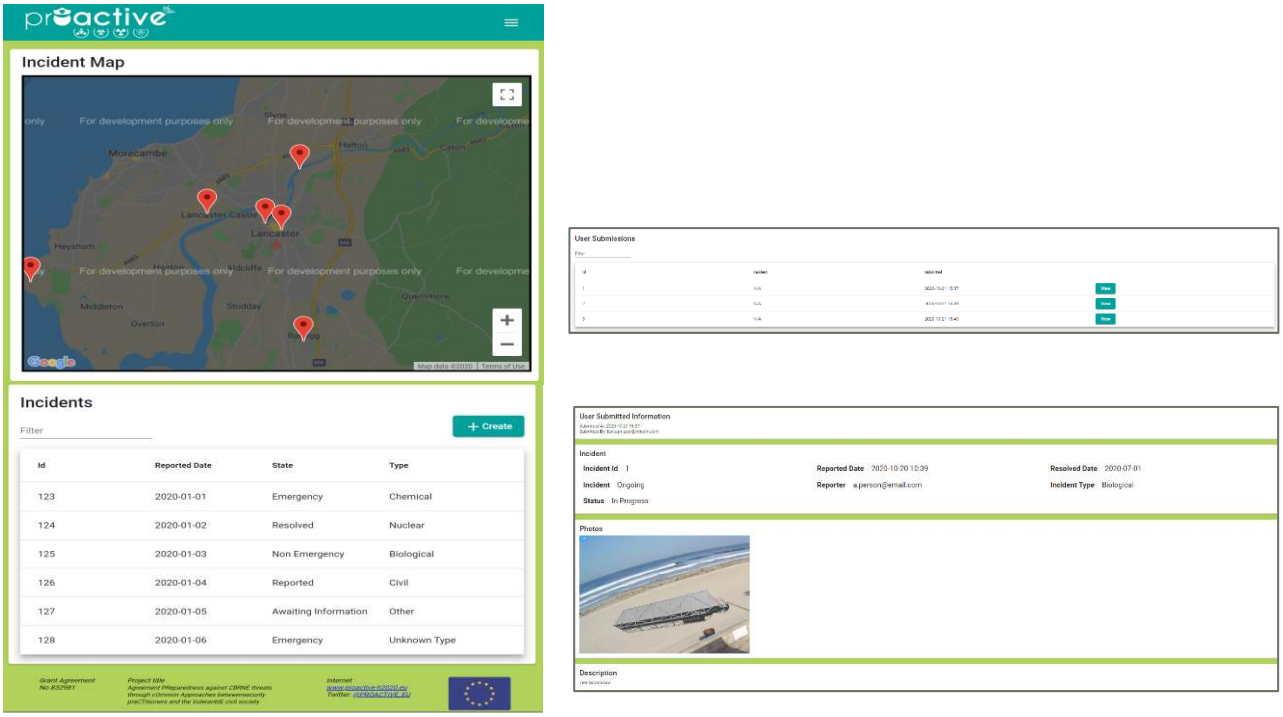


Figure 5 Information Sharing

6. CONCLUSION

The Web Collaborative Platform and Mobile Application for LEAs and Security Policy Makers will be developed based on an iterative approach in line with the three field exercises planned during the lifetime of the PROACTIVE project. This deliverable documents the requirements captured prior to the 1st exercise utilising the access we have had to the end users within the consortium and the existing PSAB network. Future iterations of the system development are expected to be customised in relation to the exercises planned and will create a feedback loop for system optimisation as shown in *Figure 6 Feedback Loop* Initially focus will be placed on the CSAB requirements, then the PSAB and the final exercise will amalgamate the two. To date, the development has focused on the core functionality, which will span across the exercises aiming to gather end user feedback to feed into the development loop. The next phase of the development will be to incorporate the current available content, effectively showcasing the usability and purpose of the system during and post mid-term conference. Further requirements will be documented in D4.2 and D4.3 respectively.

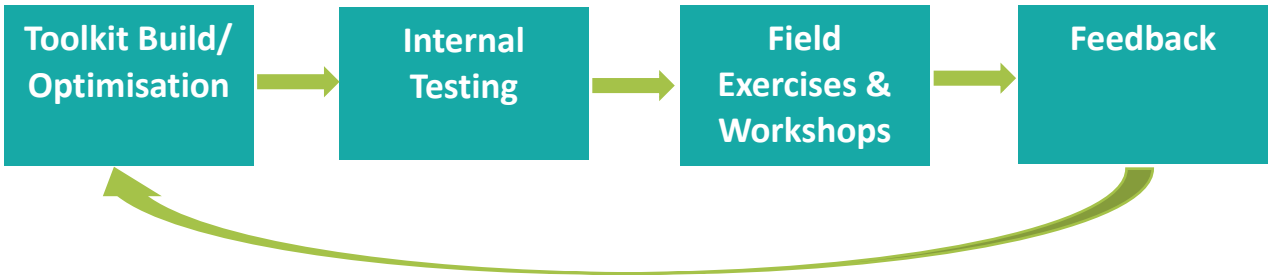


Figure 6 Feedback Loop

7. ANNEX A – USER REQUIREMENTS MATRIX

#	User/ Functional Requirements	Requirement Category	Importance (Must/ Should/ Could)
1	System shall be multilingual; so as to not neglect parts of the communities inside a country. Auto translate issues to be considered.	General	Must
2	System must be extensible/ customisable; the required scope must allow all member states to have a version specific to their location.	General	Must
3	System required to be engaged the younger generation, including a form of "entertainment" (i.e., basic games, weather, fitness etc.) to encourage use through familiarity	General	Could
4	Required to be accessible via the Police secure networks	General	Must
5	System required to be user friendly, familiar and simple in design (GUI)	General	Must
6	System to incorporate 2-way communication (1:1; 1: Many and Many: Many (Forum) and accounting for privacy factors)	General	Must
7	Separation of access and views between user groups; Admin, PSAB and CSAB	General	Must
8	System required to provide settings for accessibility (Font Size & Type, Colour of Screen, audio options for the visually impaired/ or those with dyslexia, and sign language videos for those with limited hearing etc.	General	Must
9	System to be accessible via multiple devices (PCs, Laptops, Tablets, Smartphones)	General	Should
10	Market the system for the relevant audiences. employ effective educational programs and public information campaigns	General	Should
11	System is required to automatically drive (push effect) users to social media, relevant event websites, news feeds etc and vice versa (pull effect)	Interoperability	Should
12	System is required to provide links to existing applications, e.g., WhatsApp, Skype etc.	Interoperability	Should
13	System is required to integrate with existing LEA systems (may be security implications)	Interoperability	Must
14	Images and videos of children can have particular data protection issues and should be reviewed carefully before being made public.	Legal and Ethical	Must

15	Images, voice recordings and video can be classed as personal data and need to be held as securely as other forms of personal data. This is especially the case if the image or voice of an individual who has not consented to using the system is inadvertently captured by a consenting user. In these cases, very careful consideration should be given before these materials are released on the public.	Legal and Ethical	Must
16	All data collected through the system are only to be used for the stated purposes.	Legal and Ethical	Must
17	Users should not feel pressured to supply personal or sensitive information that they do not wish to share.	Legal and Ethical	Must
18	Only data which is absolutely necessary for the functioning of the system are to be collected.	Legal and Ethical	Must
19	System should allow for both registered and anonymous users.	Legal and Ethical	Should
20	All data collected, stored, processed and retrieved by the system will be held and transferred through highly secure systems to prevent loss, damage or unauthorised access. These systems should not be based outside the EU unless absolutely necessary.	Legal and Ethical	Must
21	Users of the system will be given the ability to opt out of the collection of personal and sensitive data about him or her.	Legal and Ethical	Could
22	Users will be notified of the parties to whom the data may be transferred, the conditions for transferring the data to third parties, and the rights of the individual (data subject) concerning further processing of their personal data	Legal and Ethical	Must
23	Users will have the right to access their personal data from the system and will have the right to rectify it, if needs be.	Legal and Ethical	Must
24	Users will have a right to change their mind and withdraw any personal data which is sent.	Legal and Ethical	Must
25	When (if) registering, the users' profile shall not demand any personal data. All data requested must be volunteered by the user and not compulsory. 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.	Legal and Ethical	Must
26	System shall not disseminate personal information.	Legal and Ethical	Must
27	Users of the system will be made aware of the limitations of these services, the extent of data to be collected (including their IP address), their right to	Legal and Ethical	Should

	remain anonymous and the purposes for which this information will be used.		
28	Maps must be designed in such a way that no particular home or address can be identified.	Legal and Ethical	Must
29	Users shall be required to sign a consent form and disclaimer before accessing the data.	Legal and Ethical	Must
30	User shall be required to register to receive an associated profile.	Citizen and Practitioner	Should
31	Registration shall require a valid email and password to sign in and validate profile.	Citizen and Practitioner	Should
32	Up-to-date real time information to be provided via all methods of communication, not just pre-incident.	Citizen and Practitioner	Must
33	The system will enable users to report incidents or request information using multiple media options; free text, audio, video.	Citizen and Practitioner	Must
34	Pre-incident Information should be made available to the users through multiple media options; free text, audio, video.	Citizen and Practitioner	Should
35	Pre-incident information should be culturally appropriate, easy to understand, and non-complex, thereby allowing the information to be accessible for all.	Citizen and Practitioner	Must
36	Pre-incident information should be delivered by a credible spokesperson	Citizen and Practitioner	Must
37	The system shall provide customisation to the end user; they can select topics they are interested in or functionality suitable to them.	Citizen and Practitioner	Should
38	Information should incorporate answers to popular questions	Citizen and Practitioner	Must
39	Citizens shall be able to change their method of contact at any point. For example, written, audio, video communication	Citizen	Should
40	Citizens shall be able to view public reports about local issues or policies around CBRNe.	Citizen	Should
41	System required to provide a subscription for receiving direct notifications (sms or emails). The system should recognise the needs of that particular user.	Citizen	Could
42	The system shall provide feedback to citizens who choose to leave their name and contact details.	Citizen	Could
43	The system will allow citizens to report a CBRNe activity in their local area	Citizen	Must
44	The system should consider novelty, e.g., cartoon characters) and pictograms where appropriate to reduce the issue of language barriers.	Citizen	Should

45	The system should host an FAQ page to provide the end users with useful advice about the website itself or about particular situations in their area	Citizen	Must
46	The system shall have a database of information on accommodation, help lines, charities and any relevant contacts to be used prior to, during or post CBRNe attack. (Database should be searchable).	Citizen	Could
47	The User should have the option to contact and review specific virtual communities not necessarily in the same geographical area.	Citizen	Should
48	Accompany information with facts or proof to provide robustness	Practitioner	Could
49	System shall not drain practitioner resources.	Practitioner	Must
50	System shall provide the ability to run awareness campaigns for CBRNe preparedness.	Practitioner	Must
51	System to provide a private channel of communication between LEAs, authorities, stakeholders etc	Practitioner	Could
52	Information which is publicly disseminated should be validated before it is published	Practitioner	Must
53	The system is required to have an admin user, being someone who is responsible for the overall system.	Practitioner	Must
54	System shall enable the user to view data analytics visuals to gain intelligence. For example, number of users on site etc.	Practitioner	Should
55	System required to appear independent of the authority owning the application to encourage use and engagement.	Practitioner	Should
56	System is required to be available for cache data in areas where internet is not available	Practitioner	Must
57	Integrate with existing CBRNe sensors used by K9s and drones to understand threat level	Practitioner	Could
58	System will enable policies to be uploaded by practitioners and downloaded by interested parties. Format should include text documents, audio and video files.	Practitioner	Should
59	Consider the information being shared so as not to instil panic and worry	Practitioner	Must
60	Communication should focus on ensuring the protection of public health	Practitioner	Must
61	Incorporate up-to-date evidence-based advice in guidance and policies	Practitioner	Should
62	Include information on how first responders should communicate with the public in emergency situations (communication strategy in policies)	Practitioner	Must
63	Include clear strategies on how to manage vulnerable groups	Practitioner	Must

64	Review discrepancies in documentation between authorities and countries	Practitioner	Must

8. ANNEX B – DETAILED CORE REQUIREMENTS

Web Development Platform for LEAs and Policy Makers
Documented in the Description of Action The platform design should incorporate a consistent interface and branding using the PROACTIVE colours. Bi-Directional Communication between LEAs and Security Based Policy Makers required via direct messaging and forums. Must have provision for text, images, videos and pdf documents. Platform must have restricted access via a registration method. The platform will have 2 levels: 'Admin and User'. Platform must provide reporting tools (including visualisation methods) for LEAs to monitor communities, assess risks, assess threats, assess vulnerabilities, assess incidents, allocate resource. Platform will be highly customisable and can be parameterised according to the context of a specific scenario (location - map based), type of incident, policies required for specific incident etc). The user will select their preferred location when they log in. The platform will use a GIS-based backend, for the geo-located data gathered, enabling the GIS-oriented data storage, management and analysis. The LEAs will be reliant on a map to record incidents, manage/ allocate resources and potentially record images to the specific incidents on a map. Data storage required within the platform to store policies and other data. Formats to include pdf documents, video clips, images and audio files. **Additional Requirements from End Users** The platform provides the capability to access and exchange emergency-related information directly with citizens (push effect) and other LEAs/ Policy Makers pre-incident, real-time and post incident using multiple media options. The content and credibility of the information will be up to the LEAs and Policy makers. Include information on how first responders should communicate with the public in emergency situations (communication strategy in policies) and guideline for how to deal with vulnerable citizens. The platform must allow LEAs and Policy makers to upload and download data (pdf, videos, images, audio files). The platform static content shall be initially in English (to reflect NATO standards). The static content will be manually changed to Italian, German and Belgian/Flemish for the planned pilots.

The platform must be available via Police Secure Networks and must not identify in a category which government or security blocks – e.g., gaming, gambling, social media etc. The system will need to be certified and tested by Police IT & Digital teams to meet stability and security standards.

The platform must be able to integrate with existing LEA systems. This is 3rd party dependable and may not be feasible within the project.

The platform must consider the common definitions of a threat, event, scenario, etc. in different member states. A translating (event/incident coding) module may be needed in the PROACTIVE tool to ensure that Practitioners use the same codes or references about the same event / alert level. This is reliant on all member states providing information on their definitions. To create a module would be a project on its own.

Users of the Platform are required to read and verify (tick box) a privacy policy, data protection and access to personal data, consent form and disclaimer electronically before they can access the system.

Users of the platform will be required to provide a valid email address, organisation and name/ position to use the system. No other personal information.

The platform will enable LEAs and Policy makers to create an FAQ page with useful advice about the website itself or about particular situations in their area.

The platform will enable LEAs and policy makers to provide/ signpost users to other relevant sites/ contacts for useful information, for example accommodation, help lines, charities etc, suggestions to date include:

https://eena.org/mobile-apps-during-covid-19/

https://eena.org/online-platforms-supporting-public-health-authorities-during-covid-19/

Mobile Application for LEAs and Policy Makers
Documented in Description of Action
The mobile application for LEAs and policy makers should incorporate a consistent interface and branding using the PROACTIVE colours. Bi-Directional Communication between LEAs and Security Based Policy Makers required via direct messaging and forums. Must be provision for text, images, videos and pdf documents. Mobile Application for LEAs and Policy makers must have restricted access via a registration method. The App will have 1 level of access: User. Mobile Application for LEAs and Policy makers must provide reporting tools (including visualisation methods) for LEAs to assist in: monitor communities, assess risks, assess threats, assess vulnerabilities, assess incidents, allocate resource. Mobile Application for LEAs and Policy makers will be highly customisable and can be parameterised according to the context of a specific scenario (location - map based), type of

incident, policies required for specific incident etc). The user will select their preferred location when they log in.

Mobile Application for LEAs and Policy makers will use a GIS-based backend, for the geo-located data gathered, enabling the GIS-oriented data storage, management and analysis. The LEAs will be reliant on a map to record incidents, manage/ allocate resources and potentially record images to the specific incidents on a map.

Mobile Application for LEAs and Policy makers allows access to sensitive information about incidents and communities in real time.

Mobile Application for LEAs and Policy makers allows communications (voice, text and video) between Practitioners and required stakeholders to dispatch emergency-related information to First Responders.

Mobile Application for LEAs and Policy makers provides the capability to access and exchange emergency-related information with their chains of command and, when useful, directly with citizens.

Mobile Application for LEAs and Policy makers provides the capability to access and exchange emergency-related information directly with citizens (push effect).

Additional Requirements from End Users

Mobile Application for LEAs and Policy makers provides the capability to access and exchange emergency-related information directly with citizens (push effect), and other LEAs/ Policy Makers pre-incident, real-time and post incident using multiple media options. The content and credibility of the information will be up to the LEAs and Policy makers.

The Mobile Application for LEAs and Policy makers static content shall be initially in English (to reflect NATO standards). The static content will be manually changed to Italian, German and Belgian/Flemish for the planned pilots.

The Mobile Application for LEAs and Policy makers must be available via the Police Secure networks and must not identify in a category which government or security blocks – e.g., gaming, gambling, social media etc. The system will need to be certified and tested by Police IT & Digital teams to meet stability and security standards.

The Mobile Application for LEAs and Policy makers must be available for cache data in areas where the internet is not available and should be uploaded automatically when it becomes available.

Users of the Mobile Application for LEAs and Policy makers are required to read and verify (tick box) a privacy policy, data protection and access to personal data, consent form and disclaimer electronically before they can access the system.

The Mobile Application for LEAs and Policy makers must provide an option to view and validate any content uploaded to the portal.

Users of Mobile Application for LEAs and Policy makers will be required to provide a valid email address, organisation and name/ position to use the system. No other personal information.

The Mobile App for LEAs and Policy makers must provide the ability to report and view an incident at a specific location using a map. The Mobile App for LEAs and Policy makers will be able to upload and download data (pdf, videos, images, audio files). The Mobile App for LEAs and Policy makers will provide the users with useful advice about the website itself or about particular situations in their area via an FAQ page. The Mobile App for LEAs and policy makers will signpost users to other relevant sites/ contacts for useful information, for example accommodation, help lines, charities etc. The Mobile App for LEAs and policy makers will be compatible with tracking devices already in the market used to track people who are liable to go wondering (for example dementia patients).

9. ANNEX C – PRIVACY POLICY

PROACTIVE PRIVACY POLICY

The chart down below is intended as a summarized version of the Privacy Policy. Given its simplicity, we suggest its use when the user is going to give consent, instead of the long version. This would be in accordance with a layered approach to the right to be informed.

Who is responsible for the treatment of the data?

The Data Controller is the PROACTIVE Coordinator – Union Internationale des Chemins De Fer

The Data Controller email address is: bedel@uic.org

What personal data is to be collected?

We will collect your email only in the case you register to the system. This email may contain personal identifiers or not. No other personal data will be provided by you, besides possible indirect identifiers such as IP numbers.

Why is the data being collected, for what purpose?

Data will be collected for exchanging information about CBRNe events between the data controller and users. Moreover, statistics regarding users will be elaborated in order to improve the functionality of the apps/website. Cookies are used and stored in the browser so that you do not need to login again and again (see cookies policy below). We process your data within our submission server on the website.

The following is a list of data purposes:

1. Providing guidance in case of unexpected CBRNe events
2. Communication
    a. Between Citizens and LEAs/ Policy Makers
    b. Between event participants
3. Statistics – we will collect:
    a. Number of Registered Users
    b. Number of Incidents and who shared them (email address)
    c. Data being accessed in the platform by the user.
4. Sharing information on live events as they happen.
5. Audits – LEAs may use the information shared by the public as part of their investigations.
6. Receive live Notifications about an event to the device the user has registered with (this can be opted out of by the user)

On what basis is the data being processed?

1. Providing guidance: The legal basis is your consent.
2. Communication: The legal basis is your consent.
3. Statistics: The legal basis is our legitimate interest in improving out service and your consent.
4. Sharing information on live events as they happen: the legal basis is your consent.
5. Audits: The legal basis is our legitimate interest in improving out service and your consent.
6. Receive live Notifications: the legal basis is your consent.

Your personal data are removed after the project exercises and testing activities. Only the consortium partners stay registered until the end of the project.

Who is your data shared with?

During the PROACTIVE project your data will not be shared with third parties. However, some of the data transfers could go to countries that do not belong to the European Union, such as the UK (PROACTIVE partner: CBRNE). Decisions of adequacy, guarantees, binding corporate rules or specific situations applicable.

What are your rights?

As a resident in the European Union, you enjoy a set of rights over your data. According to the GDPR, you have the right to ask us to give you access to your data, rectify it, erase it, restrict its processing, as well as the right to data portability and to object to its processing. You have the right to oppose being subjected to purely automatic decisions and to withdraw your consent at any time. In order for you to exercise these rights, you should get it to touch with our Data Controller, Mr. Francis Bedel, through the following email: bedel@uic.org

You should attach documentation that helps our team to identify you and what right you want to exercise and to what extent. You will get a response within a month from the time of receiving your email. If we take longer to reply, you will be informed about the reasons for the delay. In case you are not satisfied with our decision, you also have the right to contact supervisory authorities. You can contact you national Data Protection Agency. You also have the right to file a complaint with supervisory authorities.