

Driving Innovation in Crisis Management for European Resilience

## D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1

Document Identification			
Due Date 31/12/2015			
Submission Date	01/02/2017		
Status	Final		
Version	3.0		

Related SP / WP	SP8/ WP840	Document Reference	D840.21
Related Deliverable(s)	D92.11, D92.21, D92.12, D92.22, D93.21	Dissemination Level	PU
Lead Participant	PRIO	Lead Author	Stine Bergersen
Contributors	EOS	Reviewers	Chiara Fonio (JRC)
			Marcel van Berlo (TNO)

#### Keywords:

Societal Impact Assessments, crisis management functions, positive/ negative assessments, societal impact criteria.

This document is issued within the frame and for the purpose of the *DRIVER* project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement No. 607798

This document and its content are the property of the *DRIVER* Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the *DRIVER* Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the *DRIVER* Partners.

Each DRIVER Partner may use this document in conformity with the DRIVER Consortium Grant Agreement provisions.



## Document Information

List of Contributors			
Name	Partner		
Stine Bergersen	PRIO		
Mareile Kaufmann	PRIO		
Klaudia Tani	EOS		

	Document History							
Version	Date	Change editors	Changes					
1.0	2014-12-31	PRIO, ARC	Submission of original versions of D92.11, D92.21, rejected.					
1.1	2015-10-29	PRIO	Merge of 92.11 (M8), 92.12 (M19), 92.21 (M8), 92.22 (M20) and 93.21 (M19) into one deliverable with a focus on the SIA assessments.					
			Revision of the SIA aspects from D92.11 and D92.21, as well as merge with SIA aspects of D92.12; D92.22 and D93.21. following new deliverable setup.					
			This deliverable is completely restructured, and is based on the framework presented in D840.11.					
			Assessments have been completely updated and revised according to new function system, new insights and project progress; they also point not only to negative, but also positive impacts.					
			More information on changes are in the introductions to each deliverable.					
1.2	2015-12-14	JRC	Review performed					
1.3	2015-12-17	PRIO	Revision according to reviewer's comments and submission to quality check by Atos					
1.4	2015-12-18	ATOS	Quality Check Performed					
1.5	2016-01-04	PRIO	Final changes after quality check					
2.0	2016-01-18	ATOS	Final version to be re(submitted). By Mareile Kaufmann & Stine Bergersen (PRIO)					

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1				Page:	2 of 159	
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



Document History					
2.1	2016-11-29	PRIO, EOS	Revisions performed according to internal review and Year 2 ad hoc review		
2.2	2017-01-17	JRC, TNO	Review performed		
2.3	2017-01-17	PRIO	Revised draft according to review		
2.4	2017-01-17	ATOS	Final draft ready for review by ATOS		
3.0	2017-02-01	ATOS	Final version submitted		

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					3 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



## Table of Contents

Pro	oject D	escription	8
Ex	ecutive	Summary	9
1	Intro	duction	. 10
	1.1	Purpose of deliverable	. 10
	1.2	Structure of the deliverable	. 12
2	Asse	ssments, examples, recommendations for functions concerning civil society resilience	. 14
	2.1	Community Engagement	. 14
	2.1.1	Training Communities for Psychosocial Support	. 14
	2.1.2	Building & Measuring Community Resilience	. 16
	2.1.3	Volunteer Management (Incl. Crowd Tasking)	. 18
	2.2	Crisis communication	. 21
	2.2.1	From Crisis Managers to Citizens (public)	. 21
	2.2.2	From the Citizens to Crisis Managers	. 28
3	Asse	ssments, examples, recommendations for functions concerning strengthened responders	31
	3.1	Identification & Awareness	. 31
	3.1.1	Gap Analysis for community resilience	. 31
	3.1.2	Situational Analysis & Impact Assessment	. 36
	3.1.3	Early Warning, Risk Analysis & Forecasting	. 44
	3.1.4	Identification of Critical Infrastructure	. 49
	3.2	CM Coordination, Command & Control	. 55
	3.2.1	Tasking and resource management	. 55
	3.3	Information Management	. 60
	3.3.1	Collection & Storage of Data	. 60
	3.3.2	Facilitating Data Processing (Incl. Operational Data Lift)	. 69
	3.3.3	Analysis & Evaluation	. 74
	3.3.4	Communication between first responders	. 80
4	Asse	ssments, examples, recommendations for functions concerning learning across borders	. 89
4	4.1	Competence- building for decision- makers and organizations	. 89
5	Over	view of relevant Criteria per Function	. 96

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					4 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



6	Ove	rview of all recommendations	99
	6.1	Recommendations for community engagement	99
	6.1.2	1 Training Communities for Psychosocial Support	99
	6.1.2	2 Building & Measuring Community Resilience	100
	6.1.3	3 Volunteer Management (Incl. Crowd Tasking)	100
	6.2	Recommendations for crisis communication	101
	6.2.2	1 From Crisis Managers to Citizens (public)	101
	6.2.2	2 From the Citizens to Crisis Managers	102
	6.3	Recommendations for Identification & Awareness	103
	6.3.2	1 Gap Analysis for community resilience	103
	6.3.2	2 Situational Analysis & Impact Assessment	104
	6.3.3	3 Early Warning, Risk Analysis & Forecasting	106
	6.3.4	4 Identification of Critical Infrastructure	107
	6.4	Recommendations for CM Coordination, Command & Control	108
	6.4.2	1 Tasking and resource management	108
	6.5	Recommendations for Information Management	109
	6.5.2	1 Collection & Storage of Data	109
	6.5.2	2 Facilitating Data Processing (Incl. Operational Data Lift)	112
	6.5.3	3 Analysis & Evaluation	113
	6.5.4	4 Communication between first responders	115
	6.6	Recommendations for Competence- building for Decision- makers and organizations .	117
7	Con	clusions & way ahead: utilizing SIA throughout the project and key recommendations	119
	7.1	SIA training for the DRIVER consortium	119
	7.2	Potential risks and challenges	120
	7.3	SIA questionnaire, including key recommendations	120
8	Refe	erences	122
A	nex 1-	Societal Impact Assessment Questionnaire	134

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					Page:	5 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# List of Figures

Figure 1: The Societal Impact Assessment component in DRIVER	11
Figure 2: SIA Framework	98
Figure 3: SIA Criteria	159

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	6 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# List of Acronyms

Abbreviation / acronym	Description
СМ	Crisis management
Cf.	See reference
E.g.	For example
D	Deliverable
EU	European Union
D	Deliverable
DoW	Description of Work
Ibid.	As above
ICT	Information Communication Technology
ID	Identification
i.e.	in effect/that is
NSA	National Security Authority
PSS	Psychosocial Support
Pos	Portfolio of Solutions
SIA	Societal Impact Assessment
SP	Sub-project
SOTA	State of the Art
Т	Task
UAV	Unmanned Aerial Vehicles
USA	United States of America
WP	Work package

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					
Reference:	D840.21	D840.21         Dissemination:         PU         Version:         3.0         9					



## Project Description

**DRIVER** evaluates solutions in three key areas: civil society resilience, responder coordination as well as training and learning.

These solutions are evaluated using the DRIVER test-bed. Besides cost-effectiveness, DRIVER also considers societal impact and related regulatory frameworks and procedures. Evaluation results will be summarised in a roadmap for innovation in crisis management and societal resilience.

Finally, looking forward beyond the lifetime of the project, the benefits of DRIVER will materialize in enhanced crisis management practices, efficiency and through the DRIVER-promoted connection of existing networks.

#### **DRIVER Step #1: Evaluation Framework**

- Developing test-bed infrastructure and methodology to test and evaluate novel solutions, during the project and beyond. It provides guidelines on how to plan and perform experiments, as well as a framework for evaluation.
- Analysing regulatory frameworks and procedures relevant for the implementation of DRIVERtested solutions including standardisation.
- Developing methodology for fostering societal values and avoiding negative side-effects to society as a whole from crisis management and societal resilience solutions.

#### DRIVER Step #2: Compiling and evaluating solutions

- Strengthening crisis communication and facilitating community engagement and selforganisation.
- Evaluating solutions for professional responders with a focus on improving the coordination of the response effort.
- Benefiting professionals across borders by sharing learning solutions, lessons learnt and competencies.

#### DRIVER Step #3: Large scale experiments and demonstration

- Execution of large-scale experiments to integrate and evaluate crisis management solutions.
- Demonstrating improvements in enhanced crisis management practices and resilience through the DRIVER experiments.

DRIVER is a 54 month duration project co-funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 607798.

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



### Executive Summary

By using the DRIVER Societal Impact Assessment (SIA) framework, this deliverable provides the first full set of assessments of the positive and negative societal impacts, that a wide range of crisis management (CM) solutions, with their many functions, may have. The assessments are not final, but are the vantage point for the further practical implementation and development of the SIA component in DRIVER, e.g. via SIA training sessions for the consortium. Thus, the assessments will be more advanced in the second version, as they will capitalize on various forms of concrete feedback from the partners and experts working with the concrete solutions. The conducting, collection and presentation of this current comprehensive set of SIAs for the CM context, is the first step to innovate the SIA approach in CM, by providing for not only a set of basic already applicable assessments and recommendations, but also a concrete methodology and tool (the SIA framework delivered in D840.11) that can be used for implementing such assessments systematically in CM. Furthermore, both the methodology and the set of assessments are designed and categorized in such a way that they are also relevant and applicable beyond the project. By employing and implementing the full SIA component (the SIA- framework, -assessments and -training modules), concrete advice and recommendations are given on how to mitigate unintended negative side-effects on society at large, and how to identify the unexplored positive societal impact and potential of CM solutions.

Chapter 1 introduces how this deliverable is part of the SIA component in DRIVER, explains how it feeds into other relevant deliverables, and vice versa. The component is designed specifically to ensure the integration of societal impact assessments across all SPs (with a focus on the solution providers in SP3, 4, 5). Chapters 2-4 then provides assessments, examples and recommendations for 16 different functions concerning civil society resilience (mainly SP3 matters), strengthened responders (mainly SP4 matters) and learning across borders (mainly SP5 matters). For every assessment in all the three chapters, a summary is given, connecting the key issues and recommendations for fostering positive societal impacts in the different assessment categories. Chapter 5 then shows the full overview (using the SIA framework) of which criteria can be linked to which function, as per the assessments in chapter 2-4. Chapter 6 presents a complete collection of all the recommendations from all the assessments, grouped by the functions they were written for. Chapter 7, the conclusions, describes the way ahead for the integration of societal impact assessments throughout DRIVER and beyond. In annex, the SIA questionnaire can be found, which is a practical and concrete tool for implementing the assessment process. The questionnaire serves as a condensed version of this deliverable, as it provides the four key assessments per CM function. Chapter 8 contains the references for this document.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	Page:	9 of 159			
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



## 1 Introduction

### 1.1 Purpose of deliverable

While the DRIVER framework and methodology for "SIA- Societal Impact Assessments" was developed in D840.11, D840.21 utilizes this framework to make assessments of the concrete societal impacts of crisis management (CM), which are difficult to assess via cost benefit analyses or other methods for impact calculation. In doing so, the deliverable draws attention to the ways in which CM solutions – with their many different functions - create secondary negative or positive impacts on society. It points to those effects that cannot be measured or addressed through clear code, checklists or calculatory models, but that nonetheless play an important role for successful crisis management.

The deliverable presents a wide range of potential impacts, such as *secondary in/securities* (e.g. unease and calmness, misuse and protection) *core societal and ethical principles* (i.e. participation, diversity), *sustainability, political and administrative principles* (i.e. accountability, transparency), *legitimacy, legal values* (i.e. in/justice) and particularly relevant *fundamental rights* (i.e. non-discrimination, privacy). The analytical object of these assessments are all the functions that the CM solutions in DRIVER have, but they are also a realistic reflection of CM functions more generally (i.e. beyond the scope of DRIVER). By applying the 25 assessment criteria to 16 of the DRIVER CM functions, this deliverable provides a large set of ready-made societal impact assessments, to identify the unexplored societal potential of CM solutions. The assessments are not final, and will be more advanced, once they are further developed and implemented into the project. However, they already serve as the starting point, and provide concrete recommendations to the crisis managers working with the respective solutions/ functions on how to assess unintended positive and negative side-effects on society at large.

Acknowledging that it is the crisis managers working with a concrete solution that have unique expertise of this solution and its (technical) functions, the aim of the SIA component in DRIVER is not only to raise awareness about how these functions can also produce societal impacts, and to stimulate critical thinking, but it also provides for – and demonstrates – an applicable methodology and tool, to enable crisis managers to conduct such assessments themselves. Using the SIA framework, the current document provides guidance through concrete recommendations about how to foster positive societal impacts and how to avoid negative side-effects on society. The societal impact component in DRIVER is designed to provide a concrete tool and methodology for doing SIA, to take account of the positive and negative societal impacts of CM activities on society.

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



This deliverable presents the first version of the full set of DRIVER societal impact assessments. The framework for conducting these assessments was developed in D840.11, and is designed to assess societal impacts for CM functions that are central in DRIVER, but also for CM in general. Both, the framework and the assessments are integrated into a first version of training modules (in D840.31). These modules are used in training sessions with the DRIVER consortium throughout 2017. The aim is to equip the DRIVER partners with the necessary skills to use the SIA methodology to conduct their own SIAs. During the training sessions, the assessments are discussed and new assessments are conducted. Through that, the crisis managers working with the various solutions learn how to utilize the framework and conduct societal impact assessments themselves. Feedback mechanisms are integrated into training material (D840.32) to ensure that insights gained during training sessions and trials are collected.

This collected feedback is finally used to refine the full SIA component (framework, assessments, and training modules) towards the end of the project. These final project outputs, i.e. the refined version of the SIA framework, the updated assessments and the training modules are available, as a complete approach to doing SIAs in CM research, to interested parties beyond the project. As such, they serve as a vantage point for innovation in CM: they provide for a methodology, a set of assessments and training material to implement SIA in CM research. Since they are open access, they can be utilized to make SIA a standard procedure in future CM projects and European CM at large, and they can be used as a basic reference model for SIA that can be continuously improved and adapted for specific purposes.



Figure 1: The Societal Impact Assessment component in DRIVER

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



This deliverable includes and builds upon several deliverables that were part of the original DoW.<sup>1</sup> The key idea and purpose of the assessments is:

- a) to acknowledge that societal impacts can be *both positive and negative*, at the same time<sup>2</sup>
- b) to *be part of a concrete methodology* on how to do CM in a way that avoids negative impacts and creates opportunities to foster societal resilience
- c) to *create awareness* and *incite critical thinking* about CM measures and *give room to weighing the pros and cons* of CM from a societal perspective.

The assessments presented here include re-worked and updated assessments and recommendations that are also based on re-worked and updated functions and assessment criteria (cf. D840.11). This version will be updated once again in M47 (version 2). This deliverable in particular compiles a catalogue of the most central recommendations in the final chapter. Furthermore, this catalogue is part of a questionnaire that will be used during training sessions and trials to give feedback to WP840. Through that, WP840 ensures to obtain feedback from all partners. This feedback will make assessments, and its examples and recommendations even more advanced in version 2.

### 1.2 Structure of the deliverable

For a detailed introduction to the framework, and to the different parts of a Societal Impact Assessment, see Chapter 3.5. of *D840.11 Societal Impact Assessment Framework*, should be consulted. The rest of this deliverable focuses on the assessments themselves. The following chapter gives assessments, examples and recommendations for different functions concerning civil society resilience (mainly SP3 matters). Chapter 3 focuses on assessments, examples and recommendations that concern strengthened responders (mainly SP4 matters) and Chapter 4 provides assessments, examples and recommendations that focus on learning across borders (mainly SP5 matters). Even though the assessments are structured according to the different SP's foci, the SIA framework points out that many assessments are equally relevant for solutions and functions of other SPs. This is why each assessment starts out by listing all the DRIVER tasks for which the assessment is considered relevant. After each assessment in chapter 2-4, a summary is given, connecting the key issues and recommendations for fostering positive societal impacts in the different assessment categories. This draws together the issues, and demonstrates the interlinkages between the different criteria. Chapter 5 then shows the full overview of which criteria can be linked to which function, as the assessments in Chapter 2-4 have shown. Chapter 6 presents a complete collection of all the

<sup>&</sup>lt;sup>2</sup> As opposed to earlier versions, e.g. in D92.11 and D92.21, which foresaw separate deliverables for negative and positive assessments, here, these are combined. This deliverable is thus a revised version 1 of the assessments that combines guidance on the creation of "secondary insecurities" (former task T92.1), "societal costs incl. negative impacts" (former task T92.2) and "positive societal impact (former task T93.2). The main intention of combining these different impacts in one framework is to get a wholesome picture of potential positive and negative impacts to be considered together.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	12 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>1</sup> D92.11 (rejected), D92.12 (due in M19), D92.21 (rejected), D92.22 (due in M20) and D93.21 (due in M19).



recommendations from all the assessments, grouped by the functions they were written for. Chapter 7, the conclusions, describes the way ahead for the integration of societal impact assessments throughout DRIVER and beyond. In annex, the SIA questionnaire can be found, which is a practical and concrete tool for implementing the assessment process. The questionnaire serves as a condensed version of this deliverable, as it provides the four key assessments per CM function. Chapter 8 lists the references for this document.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	13 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



## 2 Assessments, examples, recommendations for functions concerning civil society resilience

### 2.1 Community Engagement

2.1.1 Training Communities for Psychosocial Support

#### Related WP and Tasks: WP32, WP33, WP55

A common aim of training activities in the area of community resilience is to raise their preparedness and their response capacities. These trainings can have different contents such as first aid, introductory courses to risk reduction or trainings on how to cope with stressful psychological situations after the occurrence of a disaster (WP32). At this point it is necessary to remind that communities are not only geographical units. That people are living close together in a small village does not automatically mean that they have much to do with each other [1]. Community has also another (sometimes imagined) dimension where membership to the community is prescribed and based on common characteristics that are shared with members and differentiate then from other groups (such as school classes, music clubs, religious associations or social media groups) [137]. To only mention a few examples of potential challenges. In WP32 we use a train the trainer cascade to train affiliated volunteers to cope with stressful psychological situations and also to enable them to provide psychological support to the affected population (T32.2, T32.3, and T32.4). Especially when training activities are aimed at the population, potential several detrimental impacts shall be taken into consideration. In addition, in WP33 we test methods and material with CM professionals to better interactively engage with communities so that they are better prepared in case of crisis. This includes the provision of guidelines as well as training activities. When CM professionals train communities both the trainer-trainee as well as the CM professional – lay public power relation shall be reflected in order to build mutual trust.

### Assessments

#### Social cohesion & Solidarity, Participation, Suspicion-Trust, Non-Discrimination

Training for and with communities with the aim of raising resilience has mostly positive effects such as the strengthening of existing networks and building up new interpersonal relations, leading to strengthened and overlapping social networks and an increased resilience. But as described above community is not all about social cohesion. Members of communities share commonalities with

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	14 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



group members but also differences with other groups [64]. Also within one community there is no absolute homogeneity, but communal identities especially related to certain events and experiences prevail. Group identities transform when needed [137](e.g. kin relationships between community leaders and certain members).

• **Recommendation:** When engaging with communities as a trainer you should ensure that all participants can speak or contribute in an equal way, promoting a climate of openness. Also think of power relations between members of the community which may not be visible and hinder certain members to speak freely. Also reflect about the power imbalance between trainer (CM professional) and trainee (lay public). Thus, foresee both a joint discussion and anonymous written feedback mechanism so that people are able to articulate their views.

#### In/justice & In/equality, Non-Discrimination, Diversity & Cultural and Gender Sensitivity:

Training may exclude some groups within the population (e.g., as training with communities relies heavily on communication, it can happen that due to language issues some part of the population is excluded). The selection of potential volunteers to assist with translation or any other relevant task may influence social cohesion in a negative way. If as mentioned the community is not homogeneous and there exist grievances amongst them, choosing volunteers from any side may be considered discriminatory. When members of specific groups are discriminated against on grounds of their nationality, gender, language, ethnicity, class, and/or religion.

• **Recommendation:** When designing training curriculums and selecting participants, ensure that socio-cultural diversity is taken into account. The curriculum and the profile of trainees has to also be as inclusive as possible, especially since members of specific groups, such as migrant communities and social minorities, are often underrepresented within CM professionals and volunteers. Because of increased diversity in the population [64], trainers have to be able to deliver training activities to various societal target groups and take into account their different cultures.

#### **Misuse- Protection:**

Trainers engaging with communities may overestimate their skills and exceed their competences. This is especially critical in the case of giving psychosocial support to the public, where overestimation may lead to the failure of directing participants to a qualified psychologist or psychotherapist.

Recommendation: As CM organisation providing PSS (psychosocial support training) training, select PSS-Trainers carefully to guarantee that confrontation techniques and methods of self-awareness are applied rightly and that trainers do not overestimate their skills. Also, think about regular external evaluation of your trainers. Having a qualified psychologist in the host organisation overseeing the development of PSS training programmes and monitoring their application can assure the proper application of the former points.

#### Privacy & Data Protection:

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



Although it is indeed possible to reuse personal data while still adhering to legislation and ethical guidelines [65], the minimum requirement is that protection of the data shall always be ensured according to privacy & data protection legislation.

• **Recommendation**: Ensure conformity with European data protection legislation and rights and cultural customs related to privacy. Also when collecting and processing private data at trainings, the informed consent of participants is mandatory.

#### Participation

Trainees should be given the opportunity to participate in the design and improvement of the training curriculums. If, for example, participants provide feedback on the training and their input is ignored or their proposed improvements not included in future training rounds, they will have the feeling of being excluded and may not be willing to participate again.

- **Recommendation**: Training curriculums should also pay special attention to how to establish a sphere of trust among trainers and trainees and include adequate evaluation and feedback mechanisms.
- 2.1.1.1 Summary of recommendations: Fostering positive societal impact when working with solutions for training communities for psychosocial support:

Training communities can be a very challenging task. Since communities are diverse in many aspects of their day to day lives, trainers need to be aware of the ongoing power imbalances, grievances and language barriers. To create a sense of inclusiveness, trainers have to be perceived by the population as trust worthy. To hinder discussions with certain marginalised peoples trust is key. In addition, sociocultural diversity should be taken into account from the early writing of the trainings. Because of increased diversity in the population [64], trainers have to be able to deliver training activities to various societal target groups and take into account their different cultures. Trainers should be very carefully chosen by the requesting authority. Trainers need to be inclusive in order to hinder participation and openness. Participants also need to be ascertained that their personal details will remain disclosed and follow rules and regulations currently in place. This facilitates trust. Participants also need to be aware that they can evaluate their trainers. This process would allow them to feed back to the authorities in case they felt unease with the trainer or if the training was insufficient.

#### 2.1.2 Building & Measuring Community Resilience

#### Related WP and Tasks: WP33, WP34, WP36

Establishing a baseline status of the vulnerabilities or capacities of a person or a territorial entity such as a city. A local government is needed to assess the change of behaviour and the effectiveness of interventions. Nevertheless, the discussions on measuring disaster resilience comes to the conclusion that establishing metrics and standards for measuring resilience remains a significant challenge as there is no consensus on how to measure it [2] [61]. The point is that resilience can't be observed

Document name:	D840.21 – A guid functions – Versic	840.21 – A guide assessing unintended societal impacts of different CM unctions – Version 1					
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



directly but must derive from indirect indicators that need to be assessed with a baseline measure before of an intervention or disaster and then a long time after. Most current attempts to measure resilience define a set of desired characteristics for individuals, households, communities, systems, regions or countries that are considered resilient [66]. The method is using a bottom-up approach while at the same time being based on general theories of resilience. In most measurements, characteristics such as physical, economic (e.g. income, productivity), social (e.g. community network, civic engagement), political, institutional are used. Then also more quantitative approaches are used to get the respective data from stakeholders such as the population. Challenges pertaining to this could potentially derive from WP33 we experiment with an interpersonal method to gather information on community resilience indicators in order to be able to measure community resilience. Missing information on the reason and the exact procedure on side of the participants may lead to unease. And WP34 experiments with assessment tools for local government resilience assessment in order to identify gaps and define action plan for all stakeholders. It is based on a participative discussion methodology.

### Assessments

#### Transparency, Privacy & Data Protection, Unease-Calmness, Suspicion-Trust:

When assessing resilience, it is important to communicate transparently what kind of data is being used. It is important to make clear that not the performance of individuals is assessed using rather abstract categories such as the well-being before and after a disaster, b) the vulnerability, c) the resilience capacities to cope, adapt, and transform in case of a disaster (e.g. % of population with access to risk information), d) disaster-related shocks, losses and stress, etc. In the case which sensitive data is collected from individuals, adequate data protection measures must be taken and communicated to the participants. Also failing to communicate the reasons behind your research may lead to unease and suspicion and could prevent people to give the needed data.

• **Recommendation:** Explain in easy terms what you are doing and what is the expected added value for the participant. An added value at the individual level may promote further motivation.

#### Misuse-Protection, Dignity, Non Discrimination:

How are the results from the measurements represented, and who is having access to it? A metric or colour coding (red, yellow or green) might be good for decision makers and planners to get a quick overview of the resilience status of a territory, while there are also arguments against a quantification of resilience [66]. Also one could think that after knowing their score, the population will immediately strive to improve and sharing the score online, might lead to "positive "competitiveness. But publicly sharing scores or other forms of visualisation, such as colour codes can also lead to stigmatisation of a community.

• **Recommendation**: Any practitioner working with crisis management solutions shall be careful with sharing a quantitative visualisation of the resilience assessment. Such graphical

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	17 of 159	
Reference:	D840.21	D840.21         Dissemination:         PU         Version:         3.0						



representations might be appropriate for decision makers to get a quick overview, making them available to the public might trigger stigmatisation, which is especially problematic, when the assessments rely on very small samples.

## 2.1.2.1 Summary of recommendations: Fostering positive societal impact when working with solutions for building & measuring community resilience

Measuring resilience is quite challenging [66]. Whichever quantitative or qualitative method is used has to be easily explained to people in order to facilitate motivation and interest in increasing their resilience. Graphs and mapping of quantitative data is not easily understood by communities and for this reason the easier presented by decision makers the less problematic the presentation to the public.

#### 2.1.3 Volunteer Management (Incl. Crowd Tasking)

#### Related WP and Tasks: WP36, T36.2, T36.3, T36.4, WP43 (T43.4), T44.3

In the past decades, individuals and groups which are not previously affiliated with the CM system, and spontaneously offer their help, have become a more and more common phenomenon in the aftermath of major disasters. The willingness to help is especially high when people are emotionalised by extensive mass media coverage of the disaster situation (cf. communication to the public), thus forming a sort of "imagined community" [3]. In the last years the spontaneous offers to help are not solely triggered by traditional mass media, but are nowadays self-organised through social media, often bypassing the response and setting up parallel structures to those foreseen by CM procedures. Especially through social media, the crisis managers now have new opportunities to organize and give tasks to volunteers through such channels. Such Crowd Tasking could for example mean that a crisis centre can give volunteers within a certain area a particular task. However, volunteers are not necessarily trained and cannot replace first responders [148]. Spontaneous unaffiliated volunteers who self-organise through social media are both a resource for CM as well as a potential threat when endangering themselves, or affected people by bypassing the response. Thus, it is important to ensure that people willing to help are given safe and appropriate responsibilities.

### Assessments

#### **Privacy & Data Protection:**

For making the spontaneous willingness of the lay public available to the crisis managers there are two possibilities: pre-registration in the preparation phase and ad-hoc integration in the response phase. In both cases, there is a process where data, such as personal data, skills, preferred contributions/usage is collected from the (potential) spontaneous volunteers. On the one side, this data is needed for making the best possible use of the volunteers, taking into account individual

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	18 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



properties and competences, such as spoken languages, profession or conditions that hinder certain types of contributions. On the other side these data collection processes must make sure to strictly adhere to European and national data protection legislation.

• **Recommendations:** Operators should ensure and actively communicate that security measures were taken and that the users data is safe and only used in case of crisis to facilitate rescue missions. It will help building up a trust relationship with the population. When designing registration procedures ensure that privacy relevant information is represented in a transparent, understandable and user friendly way.

#### Misuse- Protection:

When it comes to using IT or conceptual solutions for coordinating spontaneous volunteers, not only the issue of misuse of data [82] but also of the manpower of the volunteers could arise. This can be the case when spontaneous volunteers are used for purposes other than assisting the response and the beneficiaries (e.g. for refurbishing a fire station).

• **Recommendation:** In order to not create suspicion regarding the effort from the population or to misuse volunteers for other tasks than originally indented, a four-eye principle<sup>3</sup> should be put into place, ideally separating the level that a) requests b) alerts and deploys the volunteers and c) the level which gives clearance to the deployment.

#### Trust- Suspicion, State-Citizen-Relationship:

Another dimension relevant for organisations, who are wishing to foster the engagement of the community, is trust. Not every organisation may be perceived as trustworthy enough by the population [67] to register their data or offer their assistance to them – and thus - might not be a proper operator of such unaffiliated volunteer management solutions. This might be the case with organisations not well-established in the volunteering sector or also with government agencies. Especially governmental agencies may have the additional challenge, that seeking for support from the population might be perceived as outsourcing public duties to the private sector, thus influencing the state-citizen-relationship.

 Recommendation: Before officially launching unaffiliated volunteer management programs, potential host organisations shall commission an independent survey to find out whether it would be accepted as host organisation by the envisioned target groups. In any case it might be advisable to partner with civil society organisations used to work in community engagement and use trusted and appropriate communication channels for reaching out to the target groups.

<sup>&</sup>lt;sup>3</sup> This principle is described as following by United Nations Industrial Development Organisation: « The four-eyes principle means that a certain activity, i.e. a decision, transaction, etc., must be approved by at least two people. This controlling mechanism is used to facilitate delegation of authority and increase transparency ». Available at: <a href="http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html">http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html</a>

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	19 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



#### Social Cohesion & Solidarity, Participation:

Spontaneous unaffiliated volunteers who self-organise through social media are both of added value, as they are living in solidarity and securing social cohesion through their provision of citizen-to-citizen help; as well as potentially obstructing professional response if bypassing it or when endangering themselves or others. Thus it is important to ensure that people willing to help are given safe and appropriate possibilities for participation in assisting the response.

 Recommendation: Crisis Managers responsible for applying organisation and mobilisation concepts shall see the willingness to help as chance to foster social cohesion and shall provide the organisational (e.g. safe procedures) and legal framework (e.g. insurance coverage for time on mission) for individual spontaneous volunteers as well as for grassroots initiatives to assist.

#### Diversity, Cultural & Gender Sensitivity:

Unlike assistance of the lay public gives the chance to complement the skills and competences of the responders with new skills.

• **Recommendation**: When selecting the target group for the organisation and mobilisation concept, operators shall not only think in "hard" operational efficiency parameters easy to be benchmarked (e.g. time to shovel 100 sandbags) but also "soft" parameters such as interpersonal skills relevant for cultural mediation.

#### Sustainability, Unease-Calmness:

Spontaneous volunteers who offer their help are mostly helping for a limited time. In general, attention in the media is positively related to individual's willingness to help or to take action [62]. For sustainability of spontaneous management solutions it is important not to simply close down management operations but integrate them into program planning and contingency planning of CM organisation.

Recommendations: Even if the willingness to help is temporarily restricted to the aftermath
of a disaster, where it is needed most, people who spontaneously volunteered once may
want to help again. Thus CM organisations can establish pools of "potential" spontaneous
volunteers. This function works best when pre-registering and asking them what kind of
contributions they could imagine making. When establishing structures for managing
spontaneous volunteers don't mix up these activities with your recruitment activities for
regular CM volunteers. Better see spontaneous volunteers as additional flexible "time
donation". If you proactively try to persuade them to become regular volunteers this can
lead to unease on side of the volunteers.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	20 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



## 2.1.3.1 Summary of recommendations: Fostering positive societal impact when working with solutions for Volunteer Management (Incl. Crowd Tasking)

Even if the willingness to help is temporarily restricted to the aftermath of a disaster, where it is needed most, people who spontaneously volunteered once may want to help again. Thus CM organisations can establish pools of "potential" spontaneous volunteers. This function works best when pre-registering and asking them what kind of contributions they could imagine making. But before launching these types of initiatives, host organisation need to figure out if it is feasible to host an unaffiliated volunteer management program. It also has to be ensured that these initiatives are not mixed with recruitment in the organisation.

Operators should also ensure and actively communicate that security measures were taken and that the users data is safe and only used in case of crisis to facilitate rescue missions. It will help building up a trust relationship with the population. When designing registration procedures ensure that privacy relevant information is represented in a transparent, understandable and user friendly way. : In order to not create suspicion regarding the effort from the population or to misuse volunteers for other tasks than originally indented, a four-eye principle<sup>4</sup> should be put into place, ideally separating the level that a) requests b) alerts and deploys the volunteers and c) the level which gives clearance to the deployment. Volunteers from different backgrounds must all have access to this opportunity. Operators should not discriminate between individuals.

#### 2.2 Crisis communication

#### 2.2.1 From Crisis Managers to Citizens (public)

#### **Related WP and Tasks:** WP35, T36.2, T43.4, T44.3

Also the communication from crisis managers to the public is a core function of crisis management and is relevant in all phases of crisis management. Before the occurrence of a disaster, the awareness of the public towards different risks can be raised and actions fostering individual preparedness can be promoted (35.4). In early warning phase, the population is alerted using all available communication channels about upcoming hazards and on the appropriate protective measures they shall take [139]. In the aftermath of a disaster it is important for crisis managers to keep the population informed on the development of the situation while not jeopardizing the operations. In this phase, communication to the public is also closely linked with community engagement (WP3, T43.3), as the attention on side of the population is high same as the willingness to take actions. Community engagement will be decided rapidly according to the social media monitoring, analysis of public concerns and knowledge gaps [140]. Knowledge on how to address particular stakeholder

<sup>&</sup>lt;sup>4</sup> This principle is described as following by United Nations Industrial Development Organisation: « The four-eyes principle means that a certain activity, i.e. a decision, transaction, etc., must be approved by at least two people. This controlling mechanism is used to facilitate delegation of authority and increase transparency ». Available at: <a href="http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html">http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html</a>

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	21 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



groups via media can help channel the willingness of the public to help in a way that assists and does not obstruct the response. Communication from crisis managers to the public includes all communication channels, relatively new ones such as social media (Twitter, Facebook etc.) as well as traditional media such as radio and television used as interlocutors of the messages. Finally, in the last years, responders had to learn that spontaneous volunteers (T36.2, T43.3) are not only individually acting in disaster sites, but organizing themselves by using social media. It is thus important to use communication channels to reach and instruct them how to help in the most suitable way for CM. In DRIVER WP36, we experiment with bi-directional communication tools such as the crowd tasker app, which is used to inform citizens on preventive measures before a crisis and organize and mobilise online volunteers in the aftermath of a crisis (36.3, 44.3). In our experiments, we test different messages with the aim of target group sensitive communication from the crisis managers to the public. Here the issue of trust is central, thus for the experiments in Austria, an organisation well trusted by the population was selected as operator of the solution, the Red Cross. In a society with large groups of foreign language speakers, if the communication from the crisis managers to the public only targets certain parts of the population, for example by failing to communicate the message on the most relevant languages, this can be seen as a discriminatory practice.

### Assessments

#### Suspicion-Trust, Unease-Calmness, Transparency:

One main issue connected with the provision of information to the public is trustworthiness. If the information is false, or if the message is targeted in a way that discriminates or leaves out certain groups in society, the communication from crisis managers to the public can create unease and suspicion. When the population (or any other key stakeholder in the communication process) gets the impression that CM tries to retain information, this will lead to the loss of trust and might compromise the appropriate response of sectors of the population to a hazard. Trust may also have an influence on the communication habits as well as on the communication channels the public prefer to use [4]. With social media, the role of the authorities as main providers of alerts or information for situational assessment, starts to get more and more contested and changes depending on information from multiple actors and sources. This implication has another dimension for CM- the one of media and information literacy, meaning that the population needs to have the capacities to interpret the information they receive, so they can filter wrong or misleading information from other information such as the one of the authorities<sup>5</sup>. Also, the very act of communicating a message can make the public concerned, leading to unnecessary unease. For example, during the Kathmandu earthquakes in Nepal in April 2015, the Kathmandu's cellular network went down, overloaded by the volume of calls, and applications based on this technology (such as the free communication application "Line") stopped working [5].

<sup>&</sup>lt;sup>5</sup> Initiatives such as the Media and Information Literacy campaign run by UNESCO aim at increasing population's media literacy.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	22 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



• **Recommendation:** As solution developer, ensure that your tools function in a way which creates a trustful relationship between the crisis managers and the crisis population, if not this can seriously reduce the applicability of the tool and even create suspicion and unease in the population. Decision makers and crisis communicators shall not communicate false information or provide "quick fixes" to challenging questions that may arise from the public during a crisis, even if it might seem what the public wants to hear.

#### **Open- control society:**

Communication tools for crisis and preparedness communication with the population might contribute to the feeling of a centralised control mechanism. Any information provided by the public is centralised in one place and might therefore easily be searchable and used for controlling groups or the population.

• **Recommendation:** In cases, where openness of the communication process cannot be put into practice because, e.g., it affects other core values such as data protection, crisis communicators shall make sure to explain the need and benefit of such tools, helping the public to decide whether they want to use this tool.

#### Participation, Diversity:

The results of a content analysis of general disaster preparedness websites indicated that the information on these websites was quite difficult to read and that there was need for easy to read and visually adapted content [6]. This criticism of disaster preparedness material applies to the communication of preparedness measures in general, as many resources are electronic versions of printed guidelines. Regarding information – the content – what to communicate is quite stable and there is a common understanding on preparedness measures, guidelines and tips. The means – the how to communicate differs and may be the key to a better-prepared community, which is to be evolved together between disaster management professionals and media experts.

• **Recommendation:** Technical solution providers for communication tools from CM to population shall ensure that the amount of information that is shared is scalable but very clear and understandable so the population doesn't have the feeling of lacking information about the "bigger picture" or that some population groups are locked out of the communication process. The means – the how to communicate - differs and may be the key to a better-prepared community, which is to be evolved together between disaster management professionals and media experts.

#### Privacy & Data Protection, Suspicion-Trust, Misuse-Calmness:

According to the experience of some DRIVER end- users, people often do fear the misuse of their private data [82], which can lead to suspicion, a bad reputation or a loss of trust to an organization managing the volunteers and giving information to the public.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	23 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



• **Recommendation:** When using web- or app based solutions for informing the public and organizing and mobilizing their willingness to help- CM operators shall take measures to guarantee the legality and conformity of the communication tools with national and European data protection regulations.

#### **Political reputation**:

Communication itself, but also trust from the population, can influence the political reputation of an organization involved in CM. In case of bad communication or lack of communication, the opinion of the population towards an organization may change drastically. The organisation or institution that is sending the message can risk its political reputation, should the communication process be opaque or contain wrong information.

• **Recommendation**: Strive for the highest ethical standards when communicating with the public during or after a crisis. Any damage to the political reputation of the CM organization can be hard to restore.

#### Diversity, Dignity & Autonomy, Cultural & Gender Sensitivity:

If the communicated message does not consider e.g. cultural differences and e.g. the needs of woman versus men in a crisis situation, there is a risk that it can be seen as discriminatory practice [141].

• **Recommendation**: Ensure that the communication to the public takes account of cultural and gender differences, and that e.g. crucial messages are given in the most relevant languages. Take account of all societal groups when communicating.

#### 2.2.1.1 Media & Policy communication

#### Related WP and Tasks: WP35

For crisis managers, media contact during a crisis is highly probable. Therefore, having a crisis communication strategy for CM professionals, public policy makers and media stakeholders (35.2) enables a more effective use of media channels and through trainings the appropriate framing of messages to reach the various groups within the population can be learned. During a cross- border or cross-sectoral crisis, the need for coordination is critical, and badly coordinated messages can have devastating consequences [143]. The application of non-inclusive communication tools and cultural-and gender insensitive framed messages [141] can undermine any previous efforts leading to negative societal impacts. Media professionals and high level policy makers exposed to media coverage in crisis have little time for studying strategies and guidance before the occurrence of a disaster, why here short trainings are a good method to convey the messages. In DRIVER WP35, training sessions for high-level decision makers and media representatives are conducted in order to give guidance on how to enhance resilience and crisis communication with the population. However,

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	24 of 159	
Reference:	D840.21	D840.21         Dissemination:         PU         Version:         3.0						



the wrong application of communication tools and messages (e.g. when not framed culturally sensitive) can undermine any previous efforts leading to negative societal impacts. There is also a difficult and sensitive balance between including the population in the crisis management activities (e.g. by giving them advice on how to act, prepare and respond to a crisis- and maybe also by encouraging them to sign up as volunteers, donate blood etc.) and making sure that the population feels protected and taken care of by the responsible (national) authorities. The media plays a very important role in striking this balance, as it is for many people the main channel for information.

### Assessments

#### Social cohesion & Solidarity, Participation:

If the information communicated to the population during a crisis is not experienced as trustworthy or thorough, it can seriously influence the solidarity within the population, as they could feel that they cannot trust getting the information they need. If crisis managers do not inform well about the crisis situation, it is a risk that the population does not know on what terms they are e.g. being requested to participate in the response on [142]. Alerted but not affected population will strive to get additional information on the hazard, especially when they are emotionalised by mass media coverage, and some will even act and try to help [144]. Experiences from the 2013 floods in Austria and Germany support this thesis as social media groups formed rapidly, gathering several thousand followers grasping to know more about the flood situation, posting pictures of the floods and even trying to organize citizen-to-citizen help largely independently and often uncoordinated with the response [63].

• **Recommendation:** When communicating, decision makers should adhere to the principles of openness and honesty, in order to stimulate trust in the population and not represent a breach of solidarity. Strive for a transparent and open communication process, and if information needs to be withheld from the public, clearly state so. Ensure that all the volunteers are fully informed of what kind of activity they are signing up for. Crisis managers should inform well about the crisis situation, in order for volunteers to decide if they want to participate in the activity.

#### Unease-Calmness, Suspicion-Trust:

Poor communication practices, such as sending mixed or conflicting messages from multiple sources, late release of critical information or the exclusive use of communication channels that are perceived as less trustworthy, can lead to unease or can raise mistrust on the side of the population. Panic is less likely to arise when being honest instead of sending mixed messages. Mistrust can express itself, for example, by avoiding public health recommendations. Leaving myths and arising rumours uncorrected in crisis communication may reinforce existing perceptions that certain social groups are responsible for the disaster or may even get preferential treatment [142].

• **Recommendations:** It is important that official warning messages include recommended protective actions when the disaster strikes and raises the awareness and preparedness of

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	25 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



the population before the occurrence of disasters. Media trainings should therefore prepare the sender of the message to frame the messages in an appropriate way to reach various target groups within the population, triggering the most appropriate proactive actions while avoiding panic and unease on the side of the population.

#### State-Citizen Relationship, Participation, Social Cohesion & Solidarity:

The feelings of solidarity with the crisis population and the participation of society in citizen-tocitizen help can be jeopardized if the messages by the media only stresses the efforts undertaken by the professional response community, disregarding the role of the population in preparedness and response.

• **Recommendation:** Highlighting and valuing the effort by the respective local community during a crisis in the media can help support and build solidarity and encourage participation in the community. This can also have positive spill-over effects to other communities, and strengthen bonds between members of the society.

#### Transparency:

Insufficient communications training can result in a bad or wrongful communication style both in terms of the content of the message and it's framing [145]. This can result in perceived (or real) feelings of lack of transparency and a bad visibility of important issues among the population and thus negatively influence the actions people may take in the aftermath of a disaster. For example, during the first case of Ebola outbreak in Spain in October 2014, the communication strategy of the Spanish central and local governments, including the information and messages sent by public officials, were highly criticized for the lack of transparency and openness which lead to confusion, social alert, and a strong discomfort with the way the crisis was managed by the Spanish authorities [7].

 Recommendation: Joint trainings between responsible crisis communicators and media stakeholders contribute to the openness and transparency of the communication process and a better mutual understanding. Ensure that functioning cross-organizational and cross-border coordination mechanisms are in place in order to avoid nonharmonized or even conflicting messages through different channels or in different countries.

#### Suspicion-Trust, Political Reputation:

Failure to communicating truthfully can jeopardize the trust of citizens in the official response. Especially, it will damage the political reputation of the involved authorities and organisations as was the case during the Spanish government response during the outbreak of the first case of Ebola in Spain (see also above) [8].

• **Recommendation:** Unless there are good reasons for it, withholding information from the media should be avoided – the best strategy for disaster managers is generally communicating and acting truthfully to avoid sending mixed messages. In a cross-

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	26 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



sectoral or cross-border crisis, a coordinated media communication strategy is important to avoid mixed messages, confusion and erosion of trust.

#### Cultural & Gender Sensitivity, Social Cohesion & Solidarity, Diversity:

If the policy production or media messages does not account for cultural and gender related differences, it can lead to the discrimination against certain societal groups over others and affect social cohesion in a negative way.

• **Recommendation:** Make sure that the messages that are being sent through the media or in policy related communication, take into account and respect the full diversity of the society, e.g. cultural groups and gender differences. Enable communicators to select media channels and frame messages considering socio-cultural factors such as language, language proficiency, gender, nationality, ethnicity, class, age and/or physical limitations.

#### **Privacy & Data Protection:**

For media stakeholders during a crisis, proper treatment of personal data should be assured to build trust and avoid the leakage of private or sensitive data.

• **Recommendation:** Respect the sources of information during a crisis as these could be particularly vulnerable, and follow the relevant data protection legislation when it comes to collecting or sharing personal data. Always ensure conformity with European data protection legislation and rights.

## 2.2.1.2 Summary of recommendations: Fostering positive societal impact when working with solutions for crisis communication from crisis managers to citizens (public)

Solution developers ensure that tools function in a way which creates a trustful relationship between the crisis managers and the crisis population. If not, this can seriously reduce the applicability of the tool and even create suspicion and unease in the population. Where openness of the communication process cannot be put into practice because, e.g., it affects other core values such as data protection, crisis communicators shall make sure to explain the need and benefit of such tools, helping the public to decide whether they want to use this tool.

Technical solution providers for communication tools from CM to population shall ensure that the amount of information that is shared is scalable but very clear and understandable so the population doesn't have the feeling of lacking information about the "bigger picture" or that some population groups are locked out of the communication process. The means – the how to communicate - differs and may be the key to a better-prepared community, which is to be evolved together between disaster management professionals and media experts. Media trainings should therefore prepare the sender of the message to frame the messages in an appropriate way to reach various target groups within the population, triggering the most appropriate proactive actions while avoiding panic and unease on the side of the population. When communicating, decision makers should adhere to the

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	27 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



principles of openness and honesty, in order to stimulate trust in the population and not represent a breach of solidarity. Strive for a transparent and open communication process.

#### 2.2.2 From the Citizens to Crisis Managers

#### Related WP and Tasks: WP35, T36.3, T43.4

Communication from the public to crisis managers is becoming an important function in CM especially for providing an additional back channel from the public to the crisis managers [146]. This can happen in several ways, e.g. through secondary sources such as pre-existing software solutions, social media (Facebook, Twitter etc.), through primary sources such as specifically developed mobile applications for crisis management and through a combination of both (as is the case in WP36). In both cases, the general public is valued as a good source of information [146], e.g. to improve the operational picture for the crisis managers (e.g. T43.4 uses social media to gather situation awareness information), and to tailor the aid as such. Self-reporting from the public in the field can be a valuable resource for crisis management, but there is also a risk that the content of the data may come into conflict with ruling principles of privacy and data protection. This might e.g. be a risk in T43.4 if the pictures that are meant to be reported through a social media site show inappropriate content- such as identifiable injured bodies on the ground. Using the citizens as sensors through software- based crowd- tasking solutions, such as in T36.3, may have the effect that the communicated information from the public to the crisis managers are prone to hacking or misuse, i.e. that other actors such as the media may try to capitalize on the situation.

### Assessments

#### Suitability, Necessity & Proportionality, Misuse-Protection:

Communication tools like cell-phone apps may gather more information on the users and their surroundings than originally necessary to overcome a CM situation – thus being not proportional and prone to misuse.

• **Recommendation:** Limit the amount of data that is being collected. Apply the principle of data-minimization to collect only necessary and suitable information- of a proportional size.

#### Privacy & Data Protection, Open- Control Society:

Using bi-directional communication tools in CM such as social media or mobile apps -where the population can feed back information- may enhance the situational picture of responders [147]. At the same time authorities may gather sensitive data from users such as movement profiles or information on infrastructure and surroundings. As a result, the right to privacy and data protection can be affected and perceptions of being "watched" and controlled spread among the population [80]. Also, the privacy of the individuals (the public) that the data is gathered from, can be infringed upon if the data protection principles are not built into the communication system in the first place.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	28 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



• **Recommendation**: When collecting personal data from the public, it is very important that the privacy of the individuals from whom the data is collected is being respected. And that safeguards (some sort of censorship or screening) are taken to prevent pictures being posted which are violating in one way or the other.

#### **Diversity, Dignity & non-discrimination:**

The public can be a good resource for crisis managers to get a good picture of the situation during a crisis [147]. However, if the information is only gathered from certain groups in society, it can be seen as a discriminatory practice.

• **Recommendation:** Make sure that data is used only for the intended purpose to stimulate trust in the population.

#### Integrity:

The tools for collecting data from the public can negatively influence the integrity of the individuals from whom the data is gathered, if they don't follow rules for data protection and don't protect privacy.

• **Recommendation:** In order to respect the integrity of the public, ensure that privacy and data protection is a foundation when developing/ deploying a communication solution between the public and the crisis managers.

#### **Diversity & Non-discrimination**

During a crisis, it can be very difficult to ensure that the sum of the information coming from the field takes into account different views and contexts such as religious and cultural. If only one group in society is sharing information, other considerations that might be valuable for the crisis managers may be overlooked.

• **Recommendation:** Encourage different societal groups to make use of the communication tool, or consider alternative measures to ensure diverse input from the public.

#### Transparency

The way data is gathered from the public on the field can make it difficult to trace where the data is coming from and if it is reliable etc. It may also make it difficult to assess the information or the information source post- crisis, as the data collection tools may not be very transparent.

• **Recommendation:** While protecting the privacy of the individuals, consider including a mechanism for quality assuring the reliability of the information that is gathered from the public.

#### New Vulnerabilities- Progress:

Informing the crisis management through data gathered from the public during a crisis may result in wrong assumptions (or in the crisis managers getting the wrong kind of data), either by the data

Document name:	D840.21 – A guid functions – Versic	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					
Reference:	D840.21	Dissemination: PU Version: 3.0 \$					Final



being imprecise or simply false. Such mishaps may leave the crisis managers vulnerable and be both expensive and unfortunate, as they could potentially result in e.g. deployment of resources to the wrong area. Also, there is always a risk that the technology stops working. During the Kathmandu earthquakes in Nepal in April/ May 2015, a private crisis- response firm, Global Rescue, tried to use Twitter feeds to get information about their clients in affected areas, but the Wi-Fi was down, cell phone serviced was sporadic and satellite phones went in and out [5].

• **Recommendation:** Be careful not to base the deployment of resources entirely on selfreported information from the field, but rather use it as a supplement to more traditional crisis management information channels such as information form first responders or volunteers.

## 2.2.2.1 Summary of recommendations: Fostering positive societal impact when working with solutions for crisis communication from the citizens to crisis managers

When organisations collect personal data from the public, it is very important that the privacy of the individuals from whom the data is collected is being respected. And that safeguards (some sort of censorship or screening) are taken to prevent pictures being posted which are violating in one way or the other. Data protection and privacy rules must at all times be respected. This practice needs to be transparent in order to be able to motivate people to use new communication technologies for swifter alerting.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	30 of 159
Reference:	D840.21	Dissemination: PU Version: 3.0					Final



## 3 Assessments, examples, recommendations for functions concerning strengthened responders

### 3.1 Identification & Awareness

#### 3.1.1 Gap Analysis for community resilience

#### Related WP and Tasks: WP34, WP44

In general, gap analysis is a method for resource management and assessment of management efforts, comparing actual with desired performance [68]. In CM this can include analysing where mistakes have been made in the past or where more attention is needed [69]. As such, this category is slightly different from needs assessment, because it refers more to strategic planning (i.e. what do we need for future operations?) as opposed to needs assessment in an ongoing crisis. The analysis of gaps is one aspect of different tasks and gaps to be addressed within DRIVER. This includes, for example, self-assessments conducted by organizations to understand gaps in crisis management (T34.1) or support tools that identify gaps and bottlenecks, for example in transportation and traffic (WP44). These tasks mainly concern interactions between professionals and volunteers, which is why societal impacts are likely to appear only indirectly. One example of a societal challenge for this kind of gap analysis is that if it is not designed carefully, systems for identifying gaps in crisis management may neglect the specific needs of particular societal groups, which again creates negative knock-on effects for participation, diversity, cultural- and gender-sensitivity [see for example 70]. In addition, defining the level of gap analysis for CM is a balancing act: While gap analyses generally aim to enhance CM by closing these gaps, some systems might end up producing the opposite of security and resilience, namely an over-identification of gaps, which heightens the overall level of control and unease within societies [see for example 71] [80].

### Assessments

#### Unease – Calmness:

While the identification of gaps is generally important to reduce vulnerabilities and enhance the effectiveness of CM, the difficulty is to determine at what point the most crucial gaps are identified. Since the amount of gaps in need of management can be boundless, part of a gap analysis method should be not to over-engineer crisis-management. Regulating any possible aspect of CM may cause unease as a side effect, especially when the identification of gaps is not followed up by transparent

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	31 of 159
Reference:	D840.21	.21 Dissemination: PU Version: 3.0 S					Final



and concrete strategies to close such gaps [9]. While an 'over-analysis' of gaps in CM may cause unease, a ranking and recognition of the most crucial gaps combined with a discussion of strategies to close these gaps [72], and a clear assignment of responsibilities can foster the public's trust in CM efforts and a sense of calm in society.

• **Recommendation**: From the various gaps you will reveal, identify and rank the *key gaps* to be covered in order to avoid over-engineering CM and creating unease. For any key gap, provide for a strategy to close such gaps with a clear assignment of responsibilities, as well as definitions and delimitations of related tasks. If you share knowledge about gaps publicly ensure that for any gap a related strategy to close this gap is communicated in a transparent manner.

#### Misuse – Protection, Transparency:

The identification of gaps is highly dependent on the focus and the variables chosen to conduct the analysis, meaning that they can also 'produce the results that you are looking for'. Even though gap analyses usually follow strict methodologies [69], they may also be misused for political or commercial agenda setting. This would be the case when key actors, for example, push analyses to cover specific gaps the closing of which would serve a particular political or commercial purpose [73]. Hidden, these agendas open up for misuse of gap analysis methodologies and thus a misuse of CM efforts in total. While political and commercial agendas can always overlap with or speak to existing gaps and strategies for closing such gaps, the influence of such agendas will have to be reflected upon and made transparent [74]. If gap analysis methodologies are designed to identify and disclose such agendas, for example through a set of indicators, gap analysis methodologies can in fact create an additional effect of protection against political or commercial misuse of CM efforts. The identification of agendas can in effect assist in avoiding CM strategies that address irrelevant gaps.

• **Recommendation**: Design gap analysis methodologies that rely on comprehensible and transparent parameters to ensure that they are reproducible. When putting gap analysis methodologies to use, ensure to have mechanisms in place that identify potentially hidden political or commercial agendas. For example, define a set of indicators that determine political and commercial influence on gap analysis to ensure protection against the misuse of gap analysis methods or a focus on irrelevant gaps. When conducting the analysis, use a broad variety of data sources to avoid producing skewed results. Ensure to repeat gap analyses regularly in order to take account of changes and assist in creating sustainable solutions. Include mechanisms to challenge each step in the gap analysis to check whether it speaks to the overall goal.

#### New Vulnerabilities - Progress:

Although gap analyses are generally aimed at reducing vulnerabilities, labelling a certain condition a "gap" also defines it as something vulnerable [75]. It is thus important to compare and contrast identified gaps with vulnerability analyses [76]. The communication of gaps also draws attention to potential vulnerabilities that can become targets for people with malevolent intentions [83]. The identification of a gap should thus always be communicated in terms of its merit to CM efforts in

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1						32 of 159
Reference:	D840.21	D840.21         Dissemination:         PU         Version:         3.0         S					Final



general. If presented with a corresponding strategy on how to address and close such gaps the effect of creating by naming new vulnerabilities is not only dampened, but can in effect be turned into a positive message about progress in CM.

• **Recommendation**: Communicate about gaps carefully as they also point to a vulnerability that can be exploited. Ideally, identify a strategy for closing gaps at the same time and communicate that strategy together with the identified gap in order to present the gap analysis as a value-added and progress for CM in general.

#### Accountability:

The identification of gaps comes with a big responsibility and it may also affect the accountability of the actor responsible for doing the analysis. Something similar happened in L'Aquila, Italy, where scientists conducting analyses were held accountable for issuing a statement reassuring people to stay within the city, which caused major negative impacts once the earthquake struck harder than expected [10] [11]. If the question about accountability after such incidents is left unresolved, it can become a major societal issue in which both, the victims of crises as well as those conducting gap analyses feel unfairly treated [10]. If responsibilities are defined and agreed upon before the actual gap analysis takes place, the overall value of accountability can in fact be strengthened [77].

• **Recommendation:** Before conducting a gap analysis, agree upon responsibilities and their limits, in order to regulate accountabilities for the identification of gaps and for potential misidentifications.

#### **International Relations:**

If the identification of gaps at cross-border level is not internationally comparable, gap analyses may not only lead to diverging results, but may also entail negative effects for international relations because of their potential for creating misunderstandings or coordination issues [78]. Gap analyses instruments can, however, further and foster international relations if the gaps are defined commonly and instruments as well as methodologies are synchronized, meaning that they follow the same standards and variables [79: 586]. This again presupposes a transparent and foresighted cooperation following the same goals, before gap analyses methods are put to use.

• **Recommendation**: Conduct gap analyses only at cross-border level if goals, instruments and methodologies have been synchronized before and both parties agree to the analysis. If international cooperation for gap analysis is needed due to specific cross-border scenarios, ensure to coordinate with the relevant partners beforehand, potentially during exercises. Create common standards, variables and methodologies for gap analyses [79: 586].

#### **Open- Control Society, State-Citizen-Relationship:**

Gap analyses often identify areas that need to be controlled better [68]. If such areas include the control of citizens, or public spaces and activities, the identification of gaps may heighten the overall level of control in societies, and enforce a certain culture of control [80]. Gap analysis then influences the relationship between those who control the situation and those people living in areas that are

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	33 of 159
Reference:	D840.21	D840.21         Dissemination:         PU         Version:         3.0         S					Final



being controlled. However, if the parameters for gap analysis, as well as the variables and the areas to be controlled are made public and transparent - opening up for a debate about the prioritization of CM effort - gap analyses can in fact countervail control efforts and foster an open society as well as a positive state-citizen relationship [81].

• **Recommendation:** Ensure that any analysis of gaps includes reflections about the importance of these gaps and their potential for unnecessary control-efforts [80]. If possible, ensure that areas, variables and goals for gap analysis are made transparent, and invite the opinion of those who will be subjected to the gap analysis effort in order to foster a positive state-citizen-relationship and an open society.

#### Participation, Diversity, Cultural & Gender Sensitivity:

Gap identification depends mostly on the perspective of those who identify and define gaps [84]. If those who define the parameters of the gap analysis do not know the relevant gaps well enough, the analysis will be skewed and potentially exclude important factors [85]. As a result, some relevant gaps run the risk of being unaddressed if not all affected groups are represented in the analysis process [85]. In specific, if cultural and gender dimensions of CM gaps are ignored, the gap analysis may be incomplete and parts of the population and their specific needs are left unaddressed (e.g. religious dietary requirements or specific sanitary needs for women) [86]. If the process of defining gaps is made participatory, opening up for the definition of gaps from different perspectives, gap analysis can in fact foster overall diversity and gender sensitivity.

• **Recommendation:** Make sure the team defining parameters for gap identification is diverse. This does not only refer to the inclusion of analysts with a cultural and gender-sensitive perspective, but also relates to any kind of professional diversity needed for a thorough gap analysis. Time permitting, run a pre-analysis identifying those players and representatives who know best about gaps in a specific area. Include them into the identification of gaps. Define the parameters of gaps under the participation of those groups for which the analysis' theme will be most relevant.

#### **Privacy & Data Protection:**

The identification of gaps is based on a vast variety of information and information sources [87]. In particular knowledge connected to infrastructures and private companies may be confidential or private. To include private or sensitive information in the gap analysis without permission infringes upon privacy and data protection regulations [88]. A clarification of the data needed to run gap analyses as well as an agreement with the concerned parties for running gap analyses on their domains or facilities, potentially with data concerning them or even provided by them, will foster data protection.

• **Recommendation:** Comply with data protection regulations when identifying gaps, including international regulations (if applicable) [88]. Ensure that those public and private players who may be concerned by the gap analysis are involved in the process, and that they agree to share relevant data or allow for gap analyses concerning their domain.

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					Page:	34 of 159
Reference:	D840.21	40.21 <b>Dissemination:</b> PU <b>Version:</b> 3.0					Final



#### In/equality:

Some societal groups, for example disabled people, might be forgotten in the design of gap analyses for CM, and in CM in general [89]. Gap analyses that do not take account of such groups may not only produce results that are detrimental for that specific group, but it may inspire decisions and solutions that perpetuate this inequality, in the sense that the samples/ data might not be representative to the real life situation [90]Depending on the kind of gap analysis to be conducted, the inclusion of experts from a variety of different backgrounds and potentially even of all affected groups can enhance the effectiveness of gap analyses for society as a whole. This point to the more general principle of valuing staff diversity, and can foster equal treatment of all societal groups during crises [91].

 Recommendation: If gap analyses concern society as a whole, spend some time mapping the different societal groups and ensure to take account of all parts of population to avoid unequal solutions. If possible, include experts from various backgrounds with a broad variety of perspectives into the design of gap analyses.

## 3.1.1.1 Summary of recommendations: Fostering positive societal impact when doing Gap Analysis for community resilience

In order to foster positive societal impact when doing gap analysis for community resilience, communication and strategic planning is key. To avoid a sort of over-engineering of crisis management that can potentially create unease, identify and rank the key gaps. For closing any key gap, having a strategy with a clear assignment of responsibilities, as well as definitions and delimitations of related tasks is likely to increase chances of positive impact. This also relates to the importance of communication, since gap analysis also point to a vulnerability that can potentially be exploited. Ideally, a strategy for closing the gaps that are being identified should be communicated at the same time as the gaps themselves, and if this is communicated to the public, it is worth considering the value of transparent communication to avoid speculations and suspicion. This openness can also positively influence the state- citizen relationship. Agreeing upon responsibilities and their limits beforehand, can also serve to regulate accountabilities and potential misidentifications of gaps. In a similar sense, in terms of planning the process of designing gap analysis methodologies, rely on comprehensible and transparent parameters to ensure that they are reproducible, and consider having mechanisms in place that can identify potentially hidden political or commercial agendas. For example, a set of indicators could be defined, that determine political and commercial influence on gap analysis to ensure protection against the misuse of gap analysis methods or a focus on irrelevant gaps. Many kinds of crisis do not relate to borders, and thus gap analyses might be necessary at cross-border level. If this is the case, instruments and methodologies for supporting the process should be synchronized beforehand (e.g. via common exercises). Creating common standards, variables and methodologies for gap analysis in a scientifically sound manner should include using a broad variety of data sources to avoid producing skewed results. It is also important to comply with data protection regulations and data sharing agreements when identifying

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1						35 of 159
Reference:	D840.21         Dissemination:         PU         Version:         3.0         1						Final



gaps, including international regulations (if applicable). Other precautions that could foster positive impact and support sustainable solutions is to repeat the gap analyses regularly (as well as to measure progress towards the goal) in order to take account of (societal) changes. Diversity is an important principle in many arenas, and also when working with gap analysis for CM, having a team that is both professionally diverse as well as consisting of professionals with various cultural backgrounds and gender, is worth taking into account especially when dealing with solutions that concern society as a whole. Furthermore, mapping the societal groups affected by the solution, and taking into account all parts of the population minimizes the risk of inequality. This could e.g. mean to include experts from various backgrounds with a broad variety of perspectives into the design of gap analyses.

#### 3.1.2 Situational Analysis & Impact Assessment

#### Related WP and Tasks: T43.1, T43.2, T43.4, T43.5, T44.4, WP34

Situational analysis and impact assessments are important tools to prepare CM decision-making and plan effective response [92] [93]. Within DRIVER, such assessments are conducted to identify damages and needs through mobile applications (T43.1), airborne sensors (T43.2), via social media and crowd-tasking (T43.4) and by integrating information from different agencies and dimensions (T43.5). This category also includes assessment methods that focus on supply chains and bottlenecks, for example in transport (T44.4). Most solutions are directed at both professionals and the population as such, which emphasizes the necessity for careful evaluation of secondary effects. One example of a societal challenge for situational analysis is that while UAVs can be used to get an overview and assist in situational analysis, however, without clarifying the purpose and scope of UAV data collection and without clearly branding or communicating about such tools first, their use can lead to unease for those who will witness their operation without having been briefed [42]. Another example is that when collecting information through mobile applications for situational analysis, it is important to, in some way, account for the fact that not every citizen has a mobile device (or is an experienced user), which influences the results and options of participation. In the larger context, this is often referred to as "the digital divide", referring to the divergence of internet access (or other digital resources) between information rich and information poor societies or groups [94: 4]. If not verified and contextualized, self-reported data may be biased, [95] and may potentially lead to societal distrust between individuals, because it can open up for the reporting of problems that are not verified and are the result of hasty conclusions. As such, crowd-tasked information is prone for misuse [82], or to be used for circulating deceptive information which can heighten the unease in society. It may also create distrust vis-à-vis the state or the institution running the operation, if data is collected without informed consent [96].

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1						36 of 159
Reference:	D840.21	Dissemination: PU Version: 3.0					Final


## Assessments

## Unease-Calmness, Suspicion-Trust, Transparency, Open - Control Society:

Since the use of unmanned aerial vehicles (UAV) is not yet the norm and mainly known from a military context, the deployment of airborne sensors mounted on UAVs, or other forms of surveillance aimed at large areas or crowds, may cause unease within the population [97], especially if the population does not know what the vehicles are being used for. The population may furthermore feel disproportionate unease by being watched – especially if UAVs are deployed in preparation of a crisis - which creates a climate of suspicion between the population and those who deploy airborne sensors.<sup>6</sup> If populations are not being informed about CM data collection via airborne sensors, these practices can signify distrust towards different societal groups amongst each other or vis-à-vis public authorities, and may negatively influence ethics and privacy rights [98]. It can raise the general level of suspicion because such data can also be used for surveillance purposes. A similar climate of unease and suspicion may occur if, for example, the usage of data from social media is not explained well enough by those who collect it [12]. This goes to show that any kind of situational awareness function and the way in which they are tied to specific tools and methods, should always be explained. If crisis management drones, for example, are branded clearly as such, if their area of operation has been announced in the media beforehand and if it is explained which information is collected for situational analysis, the societal acceptability of such tools is likely to be higher.<sup>7</sup> Equally, the integrity as well as reputations of the institutions using them can be positively impacted. A similar policy of transparency applies to the usage of social media or mobile phone app data for CM.

• **Recommendation:** Make sure to clearly define the scope of the data that is supposed to be collected via airborne sensors, social media or apps. Clearly mark these methods and tools as something that belongs to the crisis management context, for example by marking UAVs with

<sup>&</sup>lt;sup>7</sup> This aligns with the statement of ARTICLE 29 DATA PROTECTION WORKING PARTY, stating that "drones should only be used in strictly enumerated and justified purposes that could be listed in advance and, in any case, the use should be geographically confined and time-limited. With a view to the "chilling effect" the use of drones can have on the rights to freedom of expression and freedom of assembly, particular attention should be paid to the need to protect, as far as possible, public demonstrations and similar gatherings from any kind of surveillance." (THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA, 2015, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones. Pag e 11. Available at: <a href="http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231\_en.pdf">http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231\_en.pdf</a>

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	37 of 159	
Reference:	D840.21	Dissemination: PU Version: 3.0						

<sup>&</sup>lt;sup>6</sup> The Peace Research Institute Oslo and the Norwegian Board of Technology hosted a workshop on the 7<sup>th</sup> of March 2013, discussing whether drones could and should be used in search and rescue operations in Norway. This workshop, developed in cooperation with the Norwegian Red Cross, involved over 25 experts from fields such as military and defense, law, ethics and fundamental rights, technology and emergency management. It was part of the FP7-funded DESSI project (Decision Support on Security Investment). Gogarty and Hagger write that although UAVs "have begun to transition to the civilian sector they still retain many of their military characteristics." (2008: 144). Gogarty B, Hagger M (2008) The Laws of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air. Journal of Law, Information and Science 19 (1): 73-145. The same problem is touched upon by the OCHA report, pointing out that humanitarian organizations wish not be associated with military technology (OCHA 2014 : 9) OCHA (2014) Unmanned Aerial Vehicles in Response.

https://docs.unocha.org/sites/dms/Documents/Unmanned%20Aerial%20Vehicles%20in%20Humanitarian%20Response%2 00CHA%20July%202014.pdf (15.11.2015)



the logo of the organization that uses them. If possible, always contextualize the use of airborne sensors through brochures and information campaigns before usage. Organize information campaigns in advance about the why and how of data collection (e.g. how it will be used) and collect informed consent of populations wherever possible.

## Misuse – Protection, State-Citizen-Relationship:

Using social media and apps to collect data for situational awareness is prone to misuse by both those who collect data, by using it for purposes other than the intended [13] [14] [15], and those who provide data, for example by sending deceptive information. Efforts need to be spent on distinguishing deceptive from correct information that is circulated via apps or social media after crises. Data misuse can be counter-balanced by a clear description and delimitation of the kind of data collected, the reason for collecting data and the protection of the collected data [82]. Together with a rigorous verification regime, (for example through triangulation methods) [99] these actions will enhance the positive impact that situational awareness tools can have for crisis management and for the protection of data altogether.

• Recommendation: Clarify the kind of data to be collected for situational analysis long before related tools are being put to use. Describe the limits of the data that you collect. Devise a clear code of conduct for how this data is being used and protected from misuse. Dedicate resources to the identification of deceptive information. Share the code of conduct and all protective measures with the people whose data you are likely to collect. If you collect data for situational analysis via apps and mobile phones, devise a clear and easy-to-understand consent form that people will read before they provide data. Avoid implementing such consent forms directly on the phone because people give easily consent on the phone without reading the terms of conditions. If you do implement consent forms to be signed directly on the phone, provide for a step-by-step consent form rather than a very condensed text. Communicate the added value of crowd-tasking and clarify where the responsibilities to collect information lie.

## New Vulnerabilities - Progress:

Data collected via airborne sensors, social media or apps may not only create new vulnerabilities visa-vis the privacy [16] [17] of the data owners, but also the aggregated data that is used to identify vulnerabilities, needs and requirements can be hacked and misused by malevolent parties [18]. As such, the creation of datasets always implies its own vulnerabilities. The identification of such vulnerabilities need to be assessed against the progress such situational analysis tools can provide for CM [75] [76]. If clear guidelines and the highest technical standards for protecting aggregated information can be secured, the risk for creating new vulnerabilities through hacks can be minimized and progress secured<sup>8</sup>. However, the risk of new vulnerabilities can never be removed completely<sup>9</sup>.

<sup>&</sup>lt;sup>9</sup> For example, there will alsways be the risk that new technologies or approaches (that may not be known or implemented in CM yet) can have functions that pose new vulnerabilities. For example, it is likely that advancements in drone (UAV)

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	Page:	38 of 159				
Reference:	D840.21	340.21Dissemination:PUVersion:3.0						

<sup>&</sup>lt;sup>8</sup> As a minimum, the regulations provided in the European Data Protection Directive (Directive 95/46EC), should be followed. By doing this, many potential risks are already minimized.



 Recommendation: If you foresee the usage of social media and apps for reporting, avoid asking for information that may lead to the identification of the sharing person. Protect the networks and platforms that collect and aggregate information for situational analysis according to highest standards. Devise clear guidelines for sharing information about bottlenecks and vulnerabilities, and limit the amount of people who have access to aggregated information and results to those parties which are strictly necessary.

## **Technology Dependency – Flexible Solutions:**

In case data collected from airborne sensors or apps [100] become the norm, such measures and methods do create technology dependencies, which level of engagement are influenced for example by context specific factors [101], meaning that when they fail, little alternative options for doing situational assessments are available, which again impacts on CM efficiencies [102]. Such a risk can be counterbalanced by providing for various alternative solutions of accessing such data, which may also function when communication networks or power sources break down [103]. Through that, you create flexible solutions that can function in many different CM settings and scenarios<sup>10</sup>.

• **Recommendation:** Make sure that alternative methods for situational assessment are in place to avoid technology dependency. Ensure that such methods can replace other functions in case particular information channels fall out and to limit the overall dependency on technology in society as a whole.

## Function Creep – Controlled Use:

Any novel technology, such as airborne sensors, or any novel method to collect data from social media or via apps, which are originally developed for the context of situational analysis and crisis management, opens up for function creep [104]. This means that they can be used for purposes other than crisis management<sup>11</sup>, for example, commercial analysis, but also – especially in the context of UAVs –other political usage [19]. While some "function creeps" are in fact welcome as a versatile way of re-using technologies or information in a sensible manner [105], an appraisal of such different usages will help guiding the development of this technology and its future use. In the best

<sup>&</sup>lt;sup>11</sup> One example from the context of expansions of forensic DNB databases can be found in: Dahl, J. Y., & Sætnan, A. R. (2009). "It all happened so slowly"—On controlling function creep in forensic DNA databases. International journal of law, crime and justice, 37(3), 83-103. Here, the authors discuss e.g. what future function creep it is possible to envisage, and, as security enhancing technologies may contribute to insecurities, what safeguards should be in place to render function creep governable.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	39 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						

technology will imply that the common drone in the future may have different and more sophisticated functionalities, such as the ability to smell, communicate or have algorithms written into them that allow for a (more) autonomous operation. See for example: Kaufmann, M. (2016), «Drone/Body – The Drone's Power to Sense and Construct Emergencies», in: Sandvik, K. B. and Jumbert M. G. (eds.) The Rise of the Good Drone, London, Ashgate.

<sup>&</sup>lt;sup>10</sup> For example, after Hurricane Sandy, Nicolas Dubus, IT director for Florida-based eTailer <u>CableOrganizer.com</u>, was interviewed on disaster preparedness for IT leaders. Dubus explained how to overcome challenges with little or no business disruption when disasters strike in the future: "One of the very first things I would say is to create a list of contact information for IT and the whole company," he says. "For instance, how to contact your manager and the other people you need to contact. It should be on paper. You want to have all of the information for your phone system provider, web server hosting, Internet contact—all the contacts you can imagine. Have it on paper and keep it updated." This is an example of acknowledging the importance of analogue backup.



case scenario, additional usages of such technologies can be identified beforehand, via e.g. a plan that outlines the potential usages of situational analysis technologies, in order to provide for a controlled "re"-use of the solutions you design.

• **Recommendation:** Since many solutions open up for additional usages that are different from the original purpose, identify which of the different future usages of the developed solutions are desirable and which not in order to avoid function creep. Provide for concrete guidelines and technical specifications that limit undesirable use. Such a plan will in fact foster a positive form of controlled "re-"use of situational analysis technologies beyond their original purpose and thus create new opportunities for CM.

## Negative – Positive Standardization:

The general idea of crowd-tasking also enhances the expectation that the citizen is to play a more prominent role in CM [106] [108]<sup>12</sup>. Enhancing these general expectations can lead to negative standardization in case the citizens are increasingly being "made responsible" to care for their own safety and wellbeing and to join initiatives against their will [109]. In the long term, some citizens may find that overburdening. If crowd-tasked information is only collected from those who volunteer, a positive standard for the inclusion of citizens can be established [107].

• **Recommendation**: Crowd-task information for situational analysis only from volunteering parties, who have given their consent ahead of the operation.

## Social Cohesion & Solidarity:

Some crowd-tasking mechanisms foresee the self-reporting of unrests, damages, missing persons or other aspects of a crisis [110]. Especially in the case of reporting unrests, digital technologies can lead to unfounded suspicions towards specific societal groups, which entail social segregation and a general climate of societal distrust. This happened, for example, on social media after the 22<sup>nd</sup> of July attacks in 2011 in Norway, when premature conclusions were drawn on Twitter and Facebook about the attacker being Muslim [15]. A code of conduct for the use of crowd-tasking apps can limit such negative impacts and focus on the merit of such crowd-tasking functions for situational analysis [111]<sup>13</sup>. A code of conduct can even focus on the ethical principles about sharing information. Such codes of conduct can be used to foster a climate of social cohesion and care for each other, even when sharing information about damages, missing persons or societal unrests.

• **Recommendation:** When developing a crowd-tasking mechanism, include not only an informed consent form, but in the best case scenario also a code of conduct. This should outline the ethical principles relevant, when sharing information about situations and fellow

<sup>&</sup>lt;sup>13</sup> See for example: Havlik, D., Egly, M., Huber, H., Kutschera, P., Falgenhauer, M., & Cizek, M. (2013, October). Robust and trusted crowd-sourcing and crowd-tasking in the Future Internet. In International Symposium on Environmental Software Systems (pp. 164-176). Springer Berlin Heidelber, for a discussion also of the legal and ethical challenges for ad-hoc volunteer supported networks supported by smart phones.

Document name:	D840.21 – A guid functions – Versio	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	40 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>12</sup> See for example: Howell, A. (2015). Resilience as Enhancement: Governmentality and Political Economy beyond 'Responsibilisation'. Politics, 35(1), 67-71.



citizens, in order to inspire a culture of care and solidarity and avoid negative effects on social cohesion.

## Participation, Culture- and Gender Sensitivity:

Although a great majority of EU citizens own a cellular phone [111,]he collection of information from social media and apps is limited to those who are equipped with phones or those who are experienced social media- users, which may vary across culture, age and gender [see for example 112]. Not reflecting about such context factors in the analysis of data would lead to a skewed analysis. In addition, ensure that citizens not only feel invited to volunteer for sharing information for situational analysis [107], but ensure to include different channels for sharing information that speaks to both, culture, age and gender-related differences in technology use. As such, you can foster the voluntary participation in situational analysis.

• **Recommendation**: Ensure that crowd-tasking does not make crisis populations feel pressured to share information, but rather invites them to participate in crisis management. Provide for different communication channels for crowd-tasking to ensure the broadest possible participation in society across culture, age and gender.

## Suitability, Necessity & Proportionality:

Since airborne sensors and social media can produce deceptive information, it can be contested whether they are suitable and necessary means to collect information (they would be suitable and necessary if no other, better means to collect situational data exist) [see for example 113]<sup>14</sup>. It can be contested whether the potential for vulnerabilities in terms of collected personal data and infringements upon data protection regulations are proportional to the value of the information collected [114]<sup>15</sup>. Another problem is that proportionality can mainly be tested after the actual occurrence of a situation in which the technologies have been deployed<sup>16</sup>. Running such assessments about suitability, necessity and proportionality before, during and after exercises and actual crises, will add to the long-term analysis of such factors.

• **Recommendation:** Take into account whether other means and tools exist to collect information in a manner more suitable and proportional to the problem. Run regular suitability assessments in exercises and after technology has been put to use during emergency situations.

## Non-Discrimination:

<sup>&</sup>lt;sup>15</sup> A common example is the proportionality of internet surveillance for combatting terrorism. See for example: Brown, I., & Korff, D. (2009). Terrorism and the proportionality of internet surveillance. European Journal of Criminology, 6(2), 119-134. <sup>16</sup> See for example Harbo, T. I. (2010). The function of the proportionality principle in EU law. European Law Journal, 16(2), 158-185, for a discussion of the wider context of the proportionality principle in EU law.

Document name:	D840.21 – A guid functions – Versio	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	41 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>14</sup> See for example Oh, O., Kwon, K. H., & Rao, H. R. (2010, August). An Exploration of Social Media in Extreme Events: Rumor Theory and Twitter during the Haiti Earthquake 2010. In ICIS (p. 231), for a discussion on the rumors and Twitter during the Haiti Earthquake in 2010. This is an example of deceptive information harvested from societal media.



If airborne sensors for situational analysis can identify cultural, ethnic or gender-related features, their deployment can run the risk of discriminating against these parts of the population –especially if the data collected for situational analysis is used for other purposes than intended (i.e. function creep). Advanced UAVs are becoming cheaper, and more sophisticated, and allow image capturing at greater distances with higher resolution [115: 7]. Keeping the resolution of the UAV sensors at a high level and a clear definition of the use of the collected data strictly for crisis management purposes can support non-discrimination [47]<sup>17</sup>.

• **Recommendation:** Avoid sensors for situational analysis that can identify cultural, ethnic or gender features. If they do, ensure that these are not fed into the analysis, unless strictly necessary, e.g. for the identification of missing persons. Limit the storage of data collected by UAVs in order to avoid additional usage that can discriminate against specific societal groups.

## Privacy & Data Protection:

Privacy is often infringed upon if data is collected without real consent [88]<sup>18</sup>. Consents might be hard to collect for the deployment of airborne sensors and even if the data subjects agree to a consent form, they often do not know which of the collected information is actually traceable and storable. In sum, the use of UAVs poses unique privacy challenges, due to their information gathering qualities [115]<sup>19</sup>. Sensors of low resolution can avoid the collection of personal data in the first place and enhance the privacy of the screened population (low resolution is e.g. a requirement in Norway, see e.g. [47)].

• **Recommendation:** Collect consent from people sharing information for situational analysis. If you utilize UAVs, choose sensors that avoid the unnecessary collection of personal data. Ensure that effective ways for analysing big data are in place, which do not infringe upon the data provider's privacy or produce skewed results.

## Freedom:

If populations feel watched by airborne sensors and cannot contextualize what exactly they are being used for, the use of this kind of sensors potentially infringes upon the freedom of movement and trust in the CM operation<sup>20</sup>. A clear communication of the data collected by the UAVs, a branding of the actual technology and an information campaign that outlines and announces the use of UAVs in specific areas will maybe not foster people's freedoms, but will at least avoid the unnecessary infringement upon crisis population's freedom of movement.

<sup>&</sup>lt;sup>20</sup> One example of the use of drones used for control, leading to unease among the population, is the case in Germany to use drones to fight graffiti. See: <u>http://www.nytimes.com/2013/05/29/world/europe/in-germany-unease-at-plan-to-use-drones-to-fight-graffiti.html</u>

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	42 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>17</sup> While the UAV technology, and its regualtions, are not harmonized across Europe, the limits for resolutiosn etc. will vary across countries. See e.g. [47] for an updated guide for the Norwegian regulations and guides.

<sup>&</sup>lt;sup>18</sup> This is a general principle of European data protection legislation, as well as a central condition for good research ethics. <sup>19</sup> See for example: Cayoukian A (2012) Brivacy and droper: Upmanned aerial vehicles (pp. 1-20). Optaging Capada

<sup>&</sup>lt;sup>19</sup> See for example: Cavoukian, A. (2012). Privacy and drones: Unmanned aerial vehicles (pp. 1-30). Ontario, Canada: Information and Privacy Commissioner of Ontario, Canada.



• **Recommendation:** Communicate through information campaigns which kind of data is collected by UAVs, as well as when, where and how UAVs are being put to use. Brand the actual technologies with a clearly recognizable sign that signals the UAV's purpose.

## 3.1.2.1 Summary of recommendation: Fostering societal impact when working with Situational Analysis & Impact Assessment

In order to foster positive societal impact when working with situational analysis and impact assessments, the handling of the data that is the base of the assessments is important. This would e.g. mean to clearly define the scope of the data that is supposed to be collected via airborne sensors, social media or apps, and to make sure that collection of data relating to cultural, ethic or gender features are explicitly communicated and justified. The principle of data minimization means that more data than necessary should not be collected, and it should also be considered if better or more proportional tools for data collection already exists. These tools or technologies should furthermore be clearly marked, so that it is clear that the tools belong to the crisis management context, for example by marking UAVs with the logo of the organization that uses them. Making the relevant technologies (such as a UAV) known to the public before deploying them, can be especially important if the technology is new and unknown. To do this, brochures and information campaigns can be launched before usage. When communicating to the public about this, why data collection is happening and how it is happening should be part of the communication. This includes e.g. collecting informed consent from the population when possible, and these forms should be easy to understand for the public, and tailored to the context and to the devise they are given on (such as crowd tasking via use of a mobile phone). Furthermore, when having collected the data, the data should also be properly protected. This can be done by designing a clear code of conduct for how data, networks and platforms are being used and protected from misuse. By dedicating resources to the identification of deceptive information, the risk of misuse is limited. The technology that is used for collecting the data is also important, and should be paid particular attention to. For example, steps should be taken to avoid that personal data is reported or shared without being properly regulated. This is particularly relevant for social media and apps used for self-reporting. Furthermore, the number of people having access to aggregated information and results should be minimized. To minimize the risk of becoming too dependent on once certain technology, alternate methods for doing situational analysis and impact assessments should be considered, and the suitability of each solution should be assessed. By providing for different communication channels for e.g. crowdtasking purposes, this is likely to increase the broad participation in society across culture, age and gender. However, regardless of the solution or methods, defining limits for the use (both via guidelines and technical specifications), is important to avoid that the solution is used for an undesired purpose.

Document name:	D840.21 – A guid	e assessing unintende	assessing unintended societal impacts of different CM					
	functions – Versic	on 1	1					
Reference:	D840.21	Dissemination:	Status:	Final				



## 3.1.3 Early Warning, Risk Analysis & Forecasting

## Related WP and Tasks: 43.1, 43.3, 43.4, 44.1, WP34, (WP54)

Within CM, early warning, risk analysis and forecasting covers any technology, system or measure that has as its key functions to conduct situational analysis or impact assessment, to conduct early warning, risk analysis or forecasting. It can refer to solutions of raising alerts, risk mapping, situation assessment via airborne sensors as well as modelling bottlenecks in, for example, traffic. Within DRIVER, this is reflected e.g. in tasks 43.1 and 44.1. As part of DRIVER, risk analysis and early warning are integral aspects for assessing crisis dynamics and approaching hazards (T43.3). Because risk analyses and early warning systems have always been important technologies within crisis management, some of their secondary societal impacts are well documented, especially when it comes to their implementation [20] [21] [22]. This section focuses on the way in which risk analyses and public warnings may cause negative impacts on society, but also reflects about the opportunities they offer to foster societal values when implemented with societal acceptability in mind. An example of a challenge for early warning is the question of societal reception and acceptance, which is crucial for early warning and alert systems. This became apparent in summer 2014 in Oslo, Norway, when terror alerts about a potential Islamist attack were made public. Without concrete advice for the public, warnings can leave the general public with unease and a feeling of helplessness [27] [28] [29]. Disproportionate warnings can undermine trust of the society in public authorities and provide fertile ground for discussions about raised surveillance, and benefits and negative effects of this terror alert have been widely discussed and criticized by the public in Norway [23]. Another example shows how timing and clarity are crucial to early warning systems. If published too late or without clear instructions, early warning and risk analyses may lead to situations similar to the L'Aquila earthquake when populations did not leave the dangerous areas and premises. If warnings are spread too early and too often, they may cause unease and potentially distrust in society and undermine the reputation of the warning organizations. Balancing this question was at the heart of the discussion following the L'Aquila earthquakes [24] [25] [26].

## Assessments

## Unease - Calmness:

Issuing early warnings may cause unease, especially when media present such warnings from a sensationalistic angle. The 2014 terror-warnings in Norway caused a societal discussion about the way in which the warnings caused feelings of insecurity in the population [27] [28] [29]. Balancing the communication about early warnings and risk assessments is important: if the warning includes a concrete advice for the population, for example on how to behave in a specific situation, warnings can translate into a positive effect of CM and lead endangered populations out of dangerous situations [30]. Without concrete advice, early warnings and risk assessments may signal a constant feeling of insecurity or even panic in the population which they don't know how to react to [31].

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	44 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



• **Recommendation:** Contemplate the secondary effects that a public warning may generate, be as clear as you can in formulating the message. Include concrete advice for professionals, volunteers and citizens to avoid confusion or panic. Carefully plan the language of a risk communication. Give concrete advice for the situation so that people can react in line to the communicated risk.

## Suspicion – Trust, Social Cohesion:

Risk communication, such as early warning statements is always about announcing insecurity, and have both intended and unintended consequences [116]. If risk assessments are announced without concrete advice or without a strategy to counter such a risk, the mere communication of risk can impact trust in governments [117]. More importantly, if risk assessments are conducted about specific groups, for example extremists, the announcement of such risks may create distrust in society and towards those parts of society that are believed to pose a risk – even if they don't<sup>21</sup>. Not all risk assessments target a specific group or population. If they do, risk assessments can create a feeling of suspicion towards a broader societal group entailing various other negative consequences, as has become clear from more than a decade of risk assessments about Islamic extremism [32]. In order to counter such moments of suspicion and foster social cohesion, it is important that risk analyses reflect the wider impacts that they have on society [116]. Risk assessments and public warnings that clearly reflect upon the consequences that are to be drawn from them can counteract suspicion and foster social cohesion. Especially if assessments or warnings are conducted about specific societal groups, avoiding generalizations will limit the negative impact that such assessments have for the groups in question.

• **Recommendation:** Avoid generalizations vis-à-vis specific societal groups to lower the general level of suspicion that such assessments can cause. Have a clear policy on which risk assessments are supposed to be public. Before you communicate risk assessments or early warnings, reflect about the potential consequences that society can draw from such assessments. Give concrete advice in an easy language.

## New Vulnerabilities – Progress:

The public communication of risk assessments through early warnings can cause new vulnerabilities, if weaknesses are identified by individuals with malicious intentions [30]. These new vulnerabilities, which may be caused unintentionally [116], can be countered by thinking about risk assessments in relation to strategic interventions. The more concrete a risk, the easier it is to devise a standard procedure to counter such risks. These counter-strategies can be communicated together with identified risks in order to provide for progress in CM.

• **Recommendation**: Plan the wording of warnings carefully since they also point to a vulnerability that can be exploited. Ideally, identify a strategy for addressing the risk to be

<sup>&</sup>lt;sup>21</sup> See for example: Aftenposten, 2014, Kritiserer mediene for å skape angst etter terrortrussel. Aftenposten, 2014. Available at: <u>http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-terrortrussel-7650037.html</u>, for a discussion about the medias role in creating anxiety in the population when communicating about terror threaths.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	45 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



communicated and communicate that strategy together with the warning/risk in order to provide for maximum progress of your solutions.

## Sustainability, Political Reputation:

Disproportional amounts of warnings can infringe upon the reputation and integrity of those public authorities issuing and sending the warnings, as was the case during the Norway terror alerts in the summer of 2014 [27] [28] [29] [30] [33]. If public early warning messages are sent too frequently and without meaningful context information, they risk turning the 'state of exception'<sup>22</sup> or the 'state of crisis' into a rule. Thereby they would lose their early warning effect. If early warnings are sent with context information and concrete advice and only in situations in which clear indicators for an imminent crisis exist, they are more likely to support their credibility and the one of those sending the warning, their sustainability as well as effectiveness.

• **Recommendation:** Only send warnings when clear indicators for an imminent crisis exist. Even if the threshold for these indicators is low - to be on the safe side – ensure that the affected populations and recipients of the warning understand these indicators and take them seriously. Once you issue a warning, send as much context information as possible so that receivers of such warnings know how to react and take the warning seriously. Give concrete advice on how to react. Through that you ensure the sustainability of such systems.

## Accountability:

Since risk analysis and assessments are mostly conducted by scientific experts, it might be challenging to determine where ultimate responsibilities lie. It is difficult to identify who is to be held accountable when risk assessments have led to wrong conclusions, which can cause disastrous consequences. This was the case in L'Aquila, when scientific experts were held accountable for their risk assessments and were found guilty for some of the damages that occurred during the L'Aquila earthquake in Italy in 2009. This judgment was discussed broadly in the aftermath and would not be effective in all jurisdictions [34]. However, if the question about accountability for risk assessments is unresolved, it can become a major societal issue in which both the victims of crises, as well as those conducting risk analyses feel unfairly treated. Governing after the crisis includes questions of accountability<sup>23</sup>. If responsibilities are defined and agreed upon before actual risk assessment and early warning systems are put to use, the overall value of accountability can in fact be strengthened.

• **Recommendation:** Clarify the responsibilities and accountabilities concerning both the risk assessment procedure, the issuing of warnings and the actual response strategies before making any related public announcement. Identify who is responsible for which part of the

 <sup>&</sup>lt;sup>23</sup> For a discussion about the governing of post-crisis, see for example Boin, A., McConnell, A., & Hart, P. T. (Eds.). (2008).
Governing after crisis: the politics of investigation, accountability and learning. Cambridge University Press.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	46 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>22</sup> The notion of the «state of exception» is explored in research by e.g. the Italian philosopher Giorgio Agamben, and it fundamentally describes a process or a point in time when a government (or an organization) allows for the rule of law to be set aside in the name of a specific cause or issue. For example, in his book *State of Exception*, Agamben uses the example of the 9/11 attacks on the US, to describe how such circumstances has historically been a powerful strategy that has the potential to change democratic states (Agamben, G. (2008), *State of Exception*. University of Chicago Press, Chicago.



process. Clarify lines of communication. If you work with collective models of responsibility, ensure that they can be implemented fairly.

## **Transparency:**

If early warnings and risk analyses are not transparent, they will create suspicion, confusion and unease within society. This was the case during the Norway terror alerts in the summer of 2014 [27] [28] [29] [30] [33]. They also can affect the credibility of the warning or analysis itself, as well as that of the actor in charge of assessment and dissemination. Transparent communication of early warnings and risk means to provide for context information, to clarify what the procedures mean and what the communication of risks and warnings entail in terms of concrete actions for society. This is especially important when governments or governmental agencies are the sender of the message [118]<sup>24</sup>. If possible, include information about 'knowns' and 'unknowns' about the risk or danger in question, without sharing confidential information or information that would lead to panic [35]. The more context information you provide, the more can you foster transparency in crisis management.

• **Recommendation:** Communication strategies on risks and early warnings should be honest and transparent. They should include the most feasible extent of information about what is known and what is not known about the future. Risk analyses should furthermore include explanatory information about the solutions: why are specific solutions best suited to address a specific risk? Methodologies for conducting risk analysis and related communication standards need to be developed in a transparent manner, identifying the context information that is necessary for a recipient to know in order to react.

## International relations:

The communication or non-communication of risks, early warnings and forecasting can cause international domino-effects, especially when potential threats may spread across borders, since many of the threats and risks society is faced with are global [119]. As such, risk assessments should also take account of procedures for risk assessment and crisis management in neighbouring countries in order to avoid strains on their relations during crises (for example when it comes to the assignment of responsibilities). A clear identification and mutual understanding of fields of responsibility - in terms of territory and CM tasks - will ease international collaboration and relation during times of crises.

• **Recommendation:** Ensure that all international institutions that could have an interest in the spread of threats are properly and timely informed. For each kind of risk, develop a mutual understanding of territorial and task-related responsibilities per institution and establish communication rules for times of crises.

#### **State-Citizen Relationship:**

<sup>&</sup>lt;sup>24</sup> See for example Jenille Fairbanks, Kenneth D. Plowman and Brad L. Rawlins, "Transparency in government communication", Journal of Public Affairs, (February 2007) Volume 7, no. 1, 23–37.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	47 of 159	
Reference:	D840.21	840.21 Dissemination: PU Version: 3.0						



The assessment and communication of risk is always tied to a position of power as it defines what people should feel insecure about [120]<sup>25</sup>. Risk communicators may underestimate or not even be aware of this relation between risk and power. As a result, the communication of risks and warnings can alter the state-citizen relationship long-term, especially if risk assessments concern a specific group of people, as has become apparent from risk assessments about extremism [109]. Risk assessments that don't take their causes and definitions for granted, but reflect about the reasons for choosing specific risks over others will help building the legitimacy of such assessments and avoid a negative impact of risk assessments on state-citizenship in the first place. A positive state-citizen-relationship will furthermore be fostered if the wording of such assessments and warnings is clear and non-sensationalistic and if warnings are not over-or under-stated vis-à-vis the public [33] [28] [27].

• **Recommendation:** When devising new solutions for risk and early warning systems include reflections about choosing and defining specific risks over others. Ensure that warnings are formulated for the specific recipient and if that recipient is the general public, ensure that they are factual, easy-to-understand and not exaggerated or understated.

## Participation, Cultural & Gender Sensitivity, Non-Discrimination, In/equality:

Risk itself differs across society [122]. For example, if risk analyses are based on generalized assumptions about society at large, they may not address the needs of specific societal groups, for example homeless people. Such groups may - as a consequence of being left out of such analyses - experience unfair effects during crises [see for example 121]. In addition, risk perception also differs across societal groups, which may cause different reactions to risk assessments and early warnings, depending on culture, gender and age<sup>26</sup>. Risk assessment approaches that acknowledge the diversity of society can thus foster participation, cultural- and gender sensitivity as well as non-discrimination in society at large. For example, assessment methods could include the perspectives of different societal groups on the same danger and reflect the consequences of the risk for these specific groups. From that, conclusions can be drawn about best practices in risk communication towards different groups across society.

• **Recommendation:** If possible, make a thorough screening of all societal groups to ensure that risk assessment solutions take account of diverse risk perceptions and needs across society. Plan risk communication and early warnings while taking all potential audiences, their risk perceptions and the specific risks that they face into consideration. Organize communication and media strategies that allow for specific risk communication and early warnings for different groups. Reflect whether the formulation of the alert can have any negative impact on a particular group, area or activity.

 <sup>&</sup>lt;sup>25</sup> See for example chapter 4 "Power making by image making" in Castells, M. (2013). *Communication power*. OUP Oxford.
<sup>26</sup> For an examination of the gap between expert views of risk and public perceptions, see for example Slovic, P. E. (2000). The perception of risk. Earthscan publications.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	48 of 159	
Reference:	D840.21	340.21Dissemination:PUVersion:3.0						



## 3.1.3.1 Summary of recommendations: Fostering societal impact when working with solutions for Early Warning, Risk Analysis & Forecasting

When working with solutions aimed at doing early warning, risk analysis or forecasting activities, the potential for fostering positive societal impact can happen in a number of ways. Communication is a key element in this regard, and this is especially apparent when it comes to early warning systems and strategies. Since a public warning about a threat or a risk can create negative secondary effects, being as clear and constructive in the communication to the public (but also among professionals or volunteers) is key. This also includes carefully weighing the language used, and the way the warning is framed, e.g. to avoid generalizations vis-à-vis specific societal groups. This is also important since such warnings also point to a vulnerability that can be exploited. Ideally, identify a strategy for addressing the risk to be communicated and communicate that strategy together with the warning, and if no instructions can be given to the population, consider if the warning is really necessary. If the threat or risk is considered realistic enough, give as much context information as possible so that receivers of such warnings know how to react and take the warning seriously. In other words, communication strategies on risks and early warnings should be honest and transparent, and responsibilities and accountabilities concerning both the risk assessment procedure, the issuing of warnings and the actual response strategies, should be in place before making any public announcement. Transparent communication also includes information about the solutions, and it should be considered if information should be given about e.g. why a specific solution is seen as best suited to address a specific risk. When planning the communication chain, ensure that all international institutions that could have an interest in the spread of threats are properly and timely informed, and that there exists a mutual understanding of territorial and task-related responsibilities per institution. The communication should also be planned in a way that takes into account all potential audiences, to ensure that the solutions take account of diverse risk perceptions and needs across society, e.g. relating to different cultural or religious needs. Reflect whether the formulation of the alert can have any negative impact on a particular group, area or activity.

## 3.1.4 Identification of Critical Infrastructure

## Related WP and Tasks: WP34

In all phases of the crisis management cycle, it is critical to uphold (or restore) the core infrastructures in the city to avoid additional damage and negative effects [123]. Resilience logistics and contingency plans in DRIVER refer mainly to the resilience of local governments and related areas of mobility, energy, water, buildings, logistics and information technologies (34.1). This task includes the identification of core infrastructures within government and the development of indicators and plans for strengthening their resilience. Since the identification of core infrastructures and resilience indicators itself is unlikely to produce negative effects, potential secondary impacts are highly dependent on the methodologies that are chosen to conduct these identifications and which may influence the results. For identifying critical infrastructure, one challenge can be that resilience indicators and contingency plans for information infrastructure are often based on principles of

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	49 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



technical redundancies [see for example 124]. These redundancies may foster resilience, but they also add complexity and make the governance of information infrastructure less transparent, especially if these newly added redundancies follow their own set of security policies. A diversity of policies again increases the risk of security breaches and creates a need for more universal standards (domino-effect of governing resilience/contingency planning). Another example is that when contingency plans fail to include the key partners, as well as gender- and culture-sensitive perspectives into the developments of such plans, they risk ignoring important aspects of CM. If such plans do not set out who the responsible partner for implementing specific measures is, they will not be effective<sup>27</sup>. The influence of secondary political agendas on the devising of such plans should be carefully evaluated and made transparent in order to increase the acceptance and durability of contingency plans.

## Assessments

## Misuse/ Protection, Suitability:

The identification of key resilience indicators is always tied to the identification of measures that need to be implemented to address these indicators. The selection of resilience indicators must be meaningful in the sense that they a) really apply to the given domain and that they b) really strengthen resilience within the particular domain without causing too many practical issues [36]. One practical issue is, for example, a domino-effect in governance, meaning that the realization of one resilience indicator may cause effects that require further measures. The selection of indicators is on the one hand informed by specific strategies [37], on the other hand the selection can be influenced by either political or commercial interests [38] that foresee the implementation of a specific measure. This is not negative per se, and can certainly have a positive impact, but the selection of indicators needs to reflect whether they are prone to political or commercial misuse<sup>28</sup>. The careful selection of resilience indicators that are suitable to protect and empower the citizens can indeed have positive effects in both the long- and the short term.

• **Recommendations**: Choose resilience indicators and measures for contingency plans that strengthen resilience without causing too many follow-up measures. Reflect on the influence that commercial or political actors may have on the selection of resilience indicators.

#### New Vulnerabilities- Progress, Unease- Calmness:

Keeping track of key functions and resilience indicators is closely related to the identification of vulnerabilities [125]<sup>29</sup>. Documentation about this often collects and synthesizes this information to define vulnerabilities and gaps. This is in itself a new vulnerability, because if identified gaps become

<sup>&</sup>lt;sup>29</sup> See for example Glickman, T. S., & White, S. C. (2006). Security, visibility and resilience: the keys to mitigating supply chain vulnerabilities. International Journal of Logistics Systems and Management, 2(2), 107-119.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	50 of 159		
Reference:	D840.21	Dissemination:PUVersion:3.0							

<sup>&</sup>lt;sup>27</sup> Fundamentally, it is crucial to ask "resilience of what to what?". See for example: Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001). From metaphor to measurement: resilience of what to what?. Ecosystems, 4(8), 765-781.

<sup>&</sup>lt;sup>28</sup> See for example: Smith, A., & Stirling, A. (2010). The politics of social-ecological resilience and sustainable socio-technical transitions. Ecology and Society, 15(1), 11.



public they can be exploited by individuals with malevolent intentions. It is also possible to overanalyse vulnerabilities and create more unease about them than necessary. However, should the identification of vulnerabilities and areas of improvement reveal gaps that are more or less easy to fill in order to make the situation better, it will yield CM progress, and the risk that this creates unease is less pertaining. In fact, tending to such gaps can make the population calmer, because they experience that progress in the crisis management field has a direct impact on their protection during crises.

• **Recommendation:** Consider if the identification of vulnerabilities should be made public, or if this in fact will add to vulnerability. Capitalize on the progress in the CM field, by filling in potential gaps that can raise the level of resilience in the city. Reduce complexity of contingency plans wherever possible.

## **Technology Dependency- Flexible Solutions:**

If the measures that are installed to enhance resilience are technological solutions, they may cause new dependencies which, if they fail, create negative impacts [102]. However, should the solutions be flexible enough to handle e.g. the fallout of electricity, this can have a positive impact, and allow for a more flexible approach to raising resilience.

• **Recommendation:** Consider analogue supplements to technological solutions to enhancing resilience in the city in order to avoid technology dependency of new solutions.

## Suspicion/Trust, Participation:

If those institutions and companies working on core infrastructures in the city are not included (or are suspicious that they are not included sufficiently) in the process of identifying indicators, contingency plans may not reflect the actual needs and important companies may not feel the necessary commitment to implement them later. If left out, actors may not trust the accuracy of the contingency plans. Yet, including practitioners at multiple levels in the planning and identification of resilience indicators can create a stronger cohesion across organizations, and increase the feeling of participation and ownership of different CM actors.

• **Recommendation:** Make a screening of all relevant actors to CM. Ensure that the partners that are responsible for core infrastructures in the city are part of the process of identifying resilience indicators. Carrying this out as a democratic and inclusive process will create an ownership that can be beneficial also in the long run.

## Accountability:

Contingency plans often assume accountabilities and responsibilities for specific partners and officials to provide backup solutions<sup>30</sup>. If the accountability and responsibilities chains are not clearly

<sup>&</sup>lt;sup>30</sup> See for example: Zsidisin, G. A., Panelli, A., & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study. Supply Chain Management: An International Journal, 5(4), 187-198.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	51 of 159	
Reference:	D840.21	D840.21     Dissemination:     PU     Version:     3.0						



set out in advance, or set our unfairly, accountabilities are not likely to be assumed in times of crises, which might jeopardize the response<sup>31</sup>. However, a crisis management organization can enforce and strengthen their accountability and liability by clarifying such roles and responsibilities, for example through crisis management exercises.

• **Recommendation:** It should be verified whether, how and to what extent certain identified partners can actually be held responsible for contingency plans and backup solutions. Practicing the execution of the resilience logistics that are needed in a crisis, can enforce its effect and also strengthen the accountability of the organization.

## Cultural & Gender Sensitivity, Diversity, Dignity & Non-discrimination:

If the identification of core infrastructures and the development of contingency plans is not culturally and gender sensitive, it may neglect crucial aspects and rights of many members of society and specific societal groups<sup>32</sup>. If the plans and solutions are devised to take into account cultural and gender differences and does not discriminate about certain societal groups they are more likely to work and be accepted, and thus have a positive societal impact.

• **Recommendation:** Review your contingency plans to check whether all solutions are culturally, age- and gender-sensitive.

## Transparency:

Should the identification of core infrastructures, the development of contingency plans and related indicators not be transparent, it may lack the involved companies' trust and acceptance or may cause confusion once emergency strikes [118]. A clear and transparent crisis management organization however, with clear chains of command and responsibilities is more likely to work effectively and in a predictable way [123]. This can make it easier to implement the plan, and also for potentially justifying the actions taken, in the aftermath of the crisis.

• **Recommendation:** Devise transparent contingency plans that state responsibilities and first response actions clearly. Issue reports on actions taken, and log potential gaps or inconsistencies revealed during or after the crisis.

#### **Political Reputation:**

The identification and communication of societal key functions can be intertwined with political agendas [see for example 116]. If political influences on the contingency plans are disproportionately big, the plan may lack acceptance by those who are supposed to implement the plan or by the general population and result in negative political reputation. To a certain extent, the organization

<sup>&</sup>lt;sup>32</sup> See for example Lemish, D., & Cohen, A. A. (2005). On the gendered nature of mobile phone culture in Israel. Sex Roles, 52(7-8), 511-521., for a discussion about the role technologies used to facilitate such plans are influenced by aspects such as gender.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	52 of 159	
Reference:	D840.21	D840.21     Dissemination:     PU     Version:     3.0						

<sup>&</sup>lt;sup>31</sup> For a discussion about the information flow during crisis, see for example: Militello, L. G., Patterson, E. S., Bowman, L., & Wears, R. (2007). Information flow during crisis management: challenges to coordination in the emergency operations center. Cognition, Technology & Work, 9(1), 25-31.



and maintenance of societal key functions are hard to keep separate from current political agenda or agenda setting [126]. This is not in itself negative, but the selection of resilience indicators should clearly reflect upon whether they are prone to political or commercial misuse. A careful selection of core infrastructures and resilience indicators that are suitable to protect and empower the citizens can have positive effects on the political reputation of the crisis management organization or actor.

• **Recommendation:** Reflect upon and steer the influence of political agendas on contingency planning, keeping in mind the basic needs and principles that exist in society (almost) regardless of political or commercial influence. The selection of resilience indicators should reflect whether they are prone to political or commercial misuse.

## **International Relations:**

A crisis knows no geographical boundaries. Thus, many crisis management relevant infrastructures are of international dimensions because they include international providers and/or because they cross territories of different nations<sup>33</sup>. The complex web of organizational and institutional affiliations that this requires can challenge the efficiency of the crisis management solution [127]<sup>34</sup>. To improve international relations, the respective international regulations need to be taken into account for contingency plans to work.

• **Recommendation:** When designing a contingency plan, verify which core infrastructures are connected to international infrastructures and ensure the inclusion of necessary international partners and respective regulatory issues.

## Suitability, Necessity & Proportionality:

If the identified indicators for contingency plans are neither suitable nor necessary, meaning that other, potentially better indicators exist, they risk not being proportional to the aim [124]. If resilience indicators are suitable, necessary and proportional to the task however, they are more likely to be accepted and sustainable in the crisis management field and in the general society.

• **Recommendation:** Ensure indicators for contingency planning are suitable, necessary and proportional to the contingency plan's aim to avoid unnecessary negative secondary effects.

**Privacy & Data Protection:** Data and information about core infrastructures and infrastructures can be confidential or private. If this is the case, this data cannot be accessed without the respective approvals<sup>35</sup>. Overlooking security measures or data protection requirements when collecting and storing data can have negative consequences for the CM organization both in terms of potential fines from the Data Protection Authority or similar, but it can also damage reputation or accountability of the organization<sup>36</sup>. It may also hamper the implementation of a solution, and lead to lack of

<sup>&</sup>lt;sup>36</sup> A well-know example from the surveillance context is the NSAs bulk collection of data. See [44]

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	53 of 159		
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0							

<sup>&</sup>lt;sup>33</sup> This acknowledgement is part of the fundament of the DRIVER project.

<sup>&</sup>lt;sup>34</sup> See for example chapter 8 and 9 in Coppola, D. P. (2006). Introduction to international disaster management. Butterworth-Heinemann, for a description of such various actors in international crisis management.

<sup>&</sup>lt;sup>35</sup> Such data would be protected by European data protection regulations. See [88]



efficiency and effectiveness. While planning infrastructure protection treat confidential data with care and follow strictest data-protection rules in order to strengthen the sense of privacy of everyone involved in the process.

• **Recommendation:** Information about the vulnerability and resilience of logistical domains and infrastructure can be confidential. Those who assess key functions, vulnerabilities and indicators need to ensure that they do not infringe upon legality and only obtain information about (potentially private) infrastructures and processes with consent. Keep a clear overview of the relevant approvals and requirements to ensure compliance with relevant data protection regulations, in order to protect privacy in case there is personal data involved. For secret of confidential data, particular rules may apply, and the local Data Protection Authority should be consulted.

## 3.1.4.1 Summary of recommendations: Fostering societal impact when working with solutions aimed at identifying critical infrastructure

When working with CM solutions that aim at identifying critical infrastructure, the chosen methodologies are important to create societal impact. To ensure that the methods used for identification are producing positive impacts, the resilience indicators and contingency plans that are chosen should not cause too many follow-up measures, and should not be uncritically influenced by commercial or political actors. The partners that are responsible for core infrastructures in the city should be included as participants in the process of identifying resilience indicators. Carrying this out as a democratic and inclusive process (also taking into account cultural-, age and gender sensitive variables) will create an ownership that can be beneficial also in the long run. Rehearsing these processes, e.g. on resilience logistics, can have a positive impact also on the accountability of the organization. Concretely, this would mean to develop transparent contingency plans that state responsibilities and first response actions clearly, to issue reports on actions taken, and logging potential gaps or inconsistencies revealed. When designing a contingency plan, verify which core infrastructures are connected to international infrastructures and ensure the inclusion of necessary international partners and respective regulatory issues. To ensure legality, keep a clear overview of the relevant approvals and requirements to ensure compliance with relevant data protection regulations. In terms of communication, it should be considered if the identification of vulnerabilities should be made public, or if giving information about the vulnerability and resilience of logistical domains and infrastructure will in fact add to vulnerability, and should rather be kept confidential. Another vulnerability, technology dependency, can be reduced by considering analogue supplements to technological solutions. Avoiding this kind of dependency can enhance resilience, and ensuring that the indicators for contingency planning are suitable, necessary and proportional to the contingency plan's aim, can also avoid unnecessary negative secondary effects.

Document name:	D840.21 – A guid functions – Versic	e assessing unintender on 1	d societal im	pacts of diffe	erent CM	Page:	54 of 159	
Reference:	D840.21	840.21 Dissemination: PU Version: 3.0						



## 3.2 CM Coordination, Command & Control

## 3.2.1 Tasking and resource management

This assessment covers also aspects of the high-level function "**CM Logistics**" with the mid-level function "**Strategic transportation and Supply Chains**". In the next version of the assessments they may be disentangled.

## Related WP and Tasks: T44.1, T44.2, T44.4, T44.5

Distributing resources via well-functioning supply chains, and ensuring that contingency plans are in place, is crucial for successful crisis management [see for example 128]. Before a crisis occurs, contingency plans are prepared to deal with a potential future risk that could have very large consequences, and such a plan will explain the procedures that the relevant employees, populations, or crisis managers should follow if such an event occurs<sup>37</sup>. A supply chain can be characterized as the systematic organization of resources, information, people, activities or other assets where, in simple terms, a service or a product is moved from one actor to another, e.g. from the crisis managers to the population<sup>38</sup>. Here, the strategic planning of transportation is crucial for the distribution of resources. Within DRIVER, resources can be either human, they can be material- e.g. in terms of knowledge, deriving from cross-border cooperation (T44.2) or they can be material resources (such as a typically is the case in a disaster relief supply chain such as in T44.5). For example, T44.2 deals with solutions for tasking and capacity monitoring to improve the effective assignment of resources during crises. If these resources include human resources then these should be treated fairly, and the collection of their personal data should be regulated. Also, in T44.4, the efficiency and capacity of the storage and transport of resources is evaluated. If the scenarios for testing the efficiency and capacity of the supply chain do not account for different cultural or religious needs, even seemingly technical work with supply chains can infringe upon values of diversity<sup>39</sup>, non-discrimination, and dignity.

## Assessments

## Unease- Calmness, Suspicion- Trust:

<sup>&</sup>lt;sup>39</sup> Diversity refers to the condition of having or being composed of differing elements, especially, the inclusion of different types of people in a group, organization or country. As a core societal and democratic value diversity describes the wide range of racial, cultural, ethnic, linguistic, and religious variation that exists within and across societies. Cultural, religious and linguistic diversity is recognized and protected by the European Charter of Fundamental Rights (art. 22).

Document name:	D840.21 – A guid functions – Versio	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	55 of 159	
Reference:	D840.21	D840.21     Dissemination:     PU     Version:     3.0						

<sup>&</sup>lt;sup>37</sup> See for example Glickman, T. S., & White, S. C. (2006). Security, visibility and resilience: the keys to mitigating supply chain vulnerabilities. International Journal of Logistics Systems and Management, 2(2), 107-119.

<sup>&</sup>lt;sup>38</sup> For a description of common designs and managemens issues for supply chains, see for example. Simchi-Levi, D., Simchi-Levi, E., & Kaminsky, P. (1999). Designing and managing the supply chain: Concepts, strategies, and cases. New York: McGraw-Hill.



Especially when dealing with low-income countries, the distribution of human and financial costs and resources can create unease or suspicion if the shares are unequally distributed. Should the distribution of resources and/or preparation of contingency plans involve (personal) data collection, it is important to follow national legislation in order to protect personal data, which would otherwise create suspicion [88]. Communicating openly about the existence of contingency plans can be a contributing factor in keeping the population calm in case of a crisis, because they are reminded that governmental or non-governmental organizations are prepared to handle it [118]. Testing and rehearsing such plans, for example by carrying out national or regional crisis management exercises demonstrating that such plans and backup- procedures exist, work, or are being improved, can not only make the population calmer, but it may also contribute positively to a trustful relationship between the CM actors and the population- that is if the exercise is carried out in a proper and good manner [129].

• **Recommendation:** Make sure that the distribution of human and financial costs and resources are fairly distributed, especially when planning or developing solutions for resource management or contingency efforts with low-income countries. If the distribution of resources and/or preparation of contingency plans involve (personal) data collection, these data have to be protected according to relevant national legislation. Inform the public accordingly when contingency plans or similar are tested through CM exercises, and disseminate the achievements and lessons learnt from them.

## Misuse- Protection, Transparency:

If distribution and the use of resources do adhere to fundamental ethical principles and rights [5] <sup>40</sup>, and the process is not transparent for the relevant partners [see for example 118], this can be seen as a form of misuse of the resources. However, not only good logistical planning of the distribution of resources is important to achieve positive impact, but also the content and character of the material resources. For example, ensuring that emergency kits for distribution include hygiene articles for women [see for example 86], and that the distribution of food includes meals that are accepted in all the relevant religions can make the crisis population feel better protected and taken care of.

• **Recommendation:** To avoid misuse a certain level of transparency with regards to how the resources are distributed and spent is required. Ensure that the material resources distributed take care of and respect the different needs of men, women and children, for example in terms of food (with regards to religious and other dietary needs) and hygiene articles.

## **Technology Dependency- Flexible Solutions:**

Novel methods for the distribution of resources and crisis management [100] also hold the risk of increasing technology dependency if their innovation and performance depends greatly on a certain technology [102], making other alternative methods of filling that function difficult. For example,

<sup>&</sup>lt;sup>40</sup> Such as the The Universal Declaration of Human Rights (UDHR) and the European data protection regualtions.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	56 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



relying on a crisis information service that is based on the use of smart phones would be too limiting and not a very flexible solution [121]. However, contingency planning also includes a plan for alternative ways of coordinating the distribution of resources (such as information or materials) to a crisis area, e.g. if there is no WIFI or if the GSM technology falls out and thus increases the flexibility of the crisis management operation. If you cannot plan for such alternative ways of crisis information services, reflect about the limits and potentials inherent in your suggested solution.

• **Recommendation:** Avoid complete dependency on a certain technological solution, e.g. for coordinating the distribution of resources during a crisis. Make sure that the contingency plan takes account for the fact that certain technologies can fall out, and that there are alternative ways of e.g. informing both the population and the crisis managers in case of such an occurrence.

## Accountability, Suspicion- Trust:

Regularly including the full crisis management organization in the testing and developing of the contingency plans, demonstrates that the crisis management organizational leader is accountable and well prepared to take on this responsibility [129]. Without such an open communication about the existence of CM plans, the accountability of the responsible actors can't be questioned. Regular exercises can not only enforce trust within the organization, as it e.g. draws the responder community closer together, but it can also create trust in the general community and population, as it can be seen as a demonstration of accountable and responsible actor that are prepared for many eventualities.

• **Recommendation:** In order to be prepared and accountable in case of a crisis, make sure that appropriate contingency plans have been prepared and communicated. Regularly test and exercise with the plans, using the whole crisis management organization, and if relevant and possible, communicate the results of them both internally and externally, always paying attention not to create unease, but to foster the people's trust in crisis managers.

## International Relations:

When working together to set up a supply chain or plan for the distribution of resources, it is possible that certain legal or regulatory frameworks are not harmonized, especially at cross-border and international levels (e.g. the regulation of the use of airborne sensors/ UAV's) [see for example 49, for a description of the Norwegian preliminary guidelines]. This, among other factors, may make international cooperation difficult or even impossible. However, a constructive cooperation seeking to fill regulatory gaps and investigate innovative ways of working together across borders can have a positive effect on the relations and relationships between countries and states also on other domains. For example, a constructive and smooth cooperation in terms of "building back better" [130] can have positive spill-over effect in the larger picture of international relations and cooperation.

• **Recommendation:** Tools and measures to improve the distribution of resources and to manage the supply chain (whether human, material or financial) need to adhere to both

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	57 of 159	
Reference:	D840.21	D840.21     Dissemination:     PU     Version:     3.0						



national and international legislations, (for the UAV e.g. in terms of data protection). Pay attention to grey areas and legal vacuums, particularly when developing and deploying new solutions or tools to be used across borders. When organizing international solutions, seek to create positive spill over effects on international relations by harmonizing regulation.

## Gender & Cultural Sensitivity, Dignity & Non- Discrimination:

When setting up a supply chain or distributing resources during a crisis, there is a risk of discriminatory distribution of supplies and resources in terms of recipients (whom the supplies and resources reach) and content (what is included in the supply chain or what kind or resources are being distributed) of the supply chain<sup>41</sup>. For example, men and women, as well as culturally diverse societal groups, have different needs (e.g. different kind of hygiene articles; dietary restrictions for Muslims and Jews) [see for example 86], and not taking care of such needs may be seen as discriminatory practice. Another discriminatory practice can be that the supply chain is organized in a way that favours or overlooks some social groups over others (for example, if it treats homeless people, immigrants, marginalized people, etc., differently or does not target them at all) [89]. This can also be seen as denying peoples dignity [89]. For example, during the Kathmandu earthquakes in Nepal in April/ May 2015, part of the evacuation process was reportedly determined by personal relationships between operators and climbing guides, and the Sherpas - an ethic group in the mountainous region of Nepal that are often hired as guides- are usually the ones left off helicopter medical evacuations, because they cannot pay [5] for them. However, there are several opportunities for fostering positive impact in this regard. Enforcing the principles of non-discrimination and gender & cultural sensitivity would mean that the crisis management is organized in a way that does not overlook such needs as described above. Concretely, that would for example translate into reducing systematic biases about whom to rescue. This would mean that no societal groups should be systematically left behind when distributing resources and that everyone is respected and cared for in an equal manner, regardless of characteristics such as religion, age, gender, etc. It would also mean that particular needs related to such characteristics are taken into consideration e.g. when setting up the supply chain. Incorporating such considerations into the very fundament of the resilience logistics can positively impact inclusion and enforce the principle of non-discrimination by respecting cultural and gender differences in a practical manner. This can be particularly importantand have even more significant impact- in a time of crisis when people may be feeling particularly sensitive and fragile.

 Recommendation: Ensure that the resources and content of the supply chain respects the diversity of the target population by taking gender, religious and/or cultural needs and rights into consideration. This could e.g. mean to include hygiene articles suitable for females, and include food that is suitable for all relevant religions. Ensure that the distribution of resources does not discriminate against any social groups in a way that can be seen as denying the dignity of people.

<sup>&</sup>lt;sup>41</sup> In the larger picture, one can look at the underlying principles of aid allocation, and the balance of motivations between the needs of the recipient and the interests of the dodnor countries or organizations. See for example: Maizels, A., & Nissanke, M. K. (1984). Motivations for aid to developing countries. World Development, 12(9), 879-900.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	58 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



## Accountability, Political Reputation:

The overall coordinator for preparedness and response is usually a national governmental agency who carries the accountability and responsibility of the actual crisis management. If the management of the actual crisis –whether in terms of distribution of resources, functioning of supply chains, or contingency planning- fails or is mismanaged (e.g. by discriminating against ethnic groups, or ignoring gender considerations), logically, the political reputation of the local or central government itself will be massively affected. For example, in the aftermath of hurricane Katrina in 2005, the Federal Emergency Management Agency (FEMA) was heavily criticized for its slow and inadequate response as well as for its inability to coordinate efforts with other federal agencies and organizations. Criticism from politicians, activists, and journalists were directed at the local, state and federal governments [39]. However, if the organization and distribution of resources through the supply chain takes into account fundamental societal and ethical principles, and does not treat some societal groups in a less appropriate manner than others, this can have an effect also on the more long-term accountability and political reputation of the crisis managing organization. Furthermore, a crisis management organization can for example enforce accountability and liability by clarifying roles and responsibilities, and acknowledging and assuming sound actions and decisions.

 Recommendation: In general, although citizens are already to a large extent expected to help themselves during a crisis, remember and acknowledge that citizens do expect coordinated emergency help from their authorities. Be aware that citizens may feel overburdened with responsibility in such a situation, and make sure to demonstrate who is to be held accountable during crises. Regularly practice the procedures for resilience logistics to enforce their effect and to strengthen the accountability of the organization. Ensure that the supply chains and the distribution of resources are developed and deployed in a way that treats all societal groups equally, and that they do not discriminate against someone based on their ethnical or religious characteristics.

## 3.2.1.1 Summary of recommendations: Fostering positive societal impact when working with tasking and resource management

Distribution of resources, i.e. personnel and resources should happen fairly and be equal, especially when planning or developing solutions for resource management with low-income countries. A certain level of transparency should be kept. Also when not dealing with low-income countries, ensure that the material resources distributed take care of and respect the different needs of men, women and children, for example in terms of food (with regards to religious and other dietary needs) and hygiene articles. To avoid creating additional vulnerabilities, and to avoid complete dependency on a certain technological solution (e.g. for coordinating the distribution of resources during a crisis), make sure that the contingency plan takes account for the fact that certain technologies can fall out. Collection of data is often necessary when working with such solutions, and these data have to be protected according to relevant national legislation. Generally, tools and measures to improve the distribution of resources and to manage the supply chain (whether human, material or financial)

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	59 of 159	
Reference:	D840.21	D840.21     Dissemination:     PU     Version:     3.0						



need to adhere to both national and international legislations, (for the UAV e.g. in terms of data protection). Attention should be paid to grey areas and legal vacuums, particularly when developing and deploying new solutions or tools to be used across borders. Regularly practice the procedures for resilience logistics to enforce their effect and to strengthen the accountability of the organization. In terms of communication, it is important that the public are informed accordingly when contingency plans or similar are tested through CM exercises. With regards to the content of the resources and of the supply chains, the diversity of the target population should be respected, by taking gender, religious and/or cultural needs and rights into consideration. This could e.g. mean to include hygiene articles suitable for females, and include food that is suitable for all relevant religions. In terms of the actual distribution of resources, this should not discriminate against any social groups in a way that can be seen as denying the dignity of people. Furthermore, be aware that citizens may feel overburdened with responsibility in such a situation, and make sure to demonstrate who is to be held accountable during crises.

## 3.3 Information Management

## 3.3.1 Collection & Storage of Data

This assessment covers also aspects of the low-level function "**Crowd Sourcing**" with the mid-level function "**Information Management**". In the next version of the assessments they may be disentangled.

Related WP and Tasks: WP34, T35.2, T36.2, T36.3, T43.1, T43.2, T43.4, T43.5, WP53, WP54

Data collection is one of the most common functions that a CM solution can perform. To a large extent, data collection is unavoidable for the deployment of many CM solutions, since knowledge production and benefitting from lessons learnt requires a data record of previous actions [87]. Many of the DRIVER solutions and measures have various kinds of collection and storage of data as their functions, e.g. airborne sensors (T43.2). The collection and storage of data in DRIVER varies from e.g. solutions that collect data from professionals and from the field (T43.1) to collecting data through a crowd tasking solution for volunteers (T36.3). For crisis management, the introduction of new technologies and social media has provided new ways of doing data collection, for example by "harvesting" data from social media platforms [100] [113]. Collection and storage needs to fulfil certain requirements to avoid the creation of secondary insecurities, and other negative impacts upon societal values. The common aim of EU data regulation is to protect the values and interests of the subject that data is collected about, such as privacy [40]. Collected data can be stored on paper, electronically or computer-based e.g. through cloud computing solutions, hard drives or memory sticks. For example, one societal challenge can be that in T43.2 airborne sensors will be used during CM activities, which necessarily implies the collection and storage of data. If limitations are not set for the access to collected and stored data, there is a risk that the data can be misused through a

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	60 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



potential function creep. Another potential challenge can be that if it becomes public that a CM solution has collected and stored personal data without adhering to ethical and/or legal principles, the trust that individuals have towards those actors and CM solutions that failed to comply with data protection principles could be hampered. This could further result in "chilling effects", which e.g. means that the individual or group would change its behaviour in response to the revelation [48].

## Assessments

# Transparency, Privacy & Data Protection, Open- Control Society, Integrity, Suitability, Necessity & Proportionality:

Disproportional, hidden, or opaque data collections are traits of a culture or society with a high level of control [41] [80]. If bulk collection of data happens in the name of CM without a clear and communicated purpose, this goes against the principle of transparency. If data is stored without further processing the necessity for collecting data in the first place can be questioned, which again influences the concept of an open society or the concept of privacy [88]. Further, what is considered legal data collection varies across countries. For example, an increasing amount of data collection for CM is currently happening per UAV even though the regulative basis for the deployment of UAVs has not been fully developed yet and varies across different countries and legislations [see for example 49]. Infringements upon this regulation have become known, for example when the Federal Emergency Management Agency in the US grounded drones deployed by the company Falcon for damage assessments after the Colorado Floods [42]. Even though the society and Falcon could have considered this data collection as legitimate - given the crisis situation - the use of the UAV's were not legal, and the integrity of the data controllers could be questioned. Therefore, the so-called Working Party 29 in the European Commission recommends manufacturers and operators of UAV's to embed privacy friendly design choices and privacy friendly defaults as part of a "Privacy-by-Design"- approach [43]. The aim is to help industry stakeholders and operators to prevent infringements and to enhance the social acceptability of drones [43]. Furthermore, such data collection can be of positive impact if it happens transparently, respecting the privacy of the individuals from whom the data is collected by adhering to, and potentially stimulating the expansion and/ or refinement of, data protection legislation or practice<sup>42</sup>. Such advancement in data protection law can lead to a more open society, if it contributes to facilitating more transparent data collection. A focus on data protection policy and legislation caused by increased data collection, can also contribute to a sophistication of data collection methods by formally embedding such concerns

<sup>&</sup>lt;sup>42</sup> For example, one can say that the passing of the USA Freedom Act, limiting the NSA's power to collect phone data, can be seen as a vindication of Edward Snowden's revelations of NSA's bulk collection of data. 114th Congress (2015-2016). H.R.2048 - USA FREEDOM Act of 2015. Available at: <u>https://www.congress.gov/bill/114th-congress/house-bill/2048/text</u>

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	61 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



better into the data collection practice. Finally, data collection is more likely to be societally accepted if it is suitable to the cause, and proportional to the task<sup>43</sup>.

 Recommendation: The collection, storage and processing of data and information facilitated by the DRIVER solutions needs to uphold the data protection regulations to protect the privacy of those whose data may be collected. Data collection in a so-called open society adheres to the principles of privacy, data protection and integrity. It follows a process that is suitable to the cause and proportional to the task. This means that solution developers need to ask if the data collection is really necessary, and if those data are best suited to fulfil the given function. Are there alternatives to collecting personal data (in particular *sensitive* data), or can it be encrypted or anonymized? Seize opportunities to demonstrate best practice in terms of data protection, for example by consulting the local Data Protection Authority. To minimize potential infringements and to increase the social acceptability of the CM solution, consider embedding privacy friendly design choices and privacy friendly defaults in the data collecting tools, as part of a "Privacy-by –Design"- approach.

# Function Creep- Specialized and Controlled Use, Misuse- Protection, New Vulnerabilities- Progress, Privacy & Data Protection:

Not setting up limitations for the access and use of data (via encryption or password protection) increases the risk of function creep and also the potential misuse of the collected data. This means that the data is used for purposes other than the intended<sup>44</sup>. The (large scale) storage of digital data can also create new vulnerabilities, as the data risks being hacked or illegally accessed<sup>45</sup>. This vulnerability can happen by a breach of data protection law, which can lead to misuse of data or illegal access to data. On the other hand, developers of CM solutions can have the possibility to create innovative specialized solutions for data collection that better protects the collected data and thus enforces privacy. One example of such progress can be solutions for only drawing out the specific data that you need from a database, instead of automatically accessing the full database. This can minimize risks of misuse, by having better control of the data, thus a better opportunity to protect the data.

 Recommendation: The risk for misuse of collected data needs to be actively counteracted in all phases of the CM solution's development and deployment. To minimize the risk of misuse, make sure to only collect the data you need for the predefined purpose and adhere to central data protection principles such as not reusing collected data uncritically. Have mechanisms for secured storage of the collected data in place. This can include locks and

<sup>&</sup>lt;sup>45</sup> See for example Wu, X., Zhu, X., Wu, G. Q., & Ding, W. (2014). Data mining with big data. IEEE transactions on knowledge and data engineering, 26(1), 97-107, on how the enormous volumes of the data also make an application vulnerable to attacks.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	62 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						

<sup>&</sup>lt;sup>43</sup> As shown also in a study of judicial bodies' interpretation of security limitations to the right to privacy in the scope of the SurPRISE- project (FP7). SurPRISE (2013: 25) D 3.2 – Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy.

<sup>&</sup>lt;sup>44</sup> For one example on function creep in forensic DNA databases, see Dahl, J. Y., & Sætnan, A. R. (2009). "It all happened so slowly"–On controlling function creep in forensic DNA databases. International journal of law, crime and justice, 37(3), 83-103.



other physical security measures, but also password protection or encryption of data. Do not store data for longer than necessary. Regarding the application of new technology and unexplored legal fields (creating new vulnerabilities) for data collection, local Data Protection Authorities should be consulted when necessary.

## Unease- Calmness, Integrity, Suspicion- Trust:

Data collection can create unease or suspicion towards the integrity of the data collector, should the population experience that their personal data is being illegally accessed or unrightfully reused [82]. Not informing the affected individuals about the predefined purpose for the collection and storage of personal data can lead to suspicion or unease, which can even lead to a distrustful relationship with the population as they could feel unnecessarily controlled without clear reason [44]. One example of unlawful collection and storage of data is the NSA bulk collection of phone data in the USA [44] for security purposes. On the other hand, many of these risks can be minimized if the purpose and scope of the data collection is clearly communicated and socially accepted by the public<sup>46</sup>. Such transparency might also enforce the integrity of the data controller, by demonstrating accountability. Generally, data collection and storage can also create calmness and trust in the population. For example, research show that it is crucial that the collected and distributed information in a crisis is real and trustworthy, and that it doesn't feed rumours and misconceptions during the crisis [45]. If so, it may have a calming effect on the population, and establish or strengthen a trustful relationship between the crisis manager and the public.

• **Recommendation:** Generally, communicate the purpose of the data collection clearly to the public in order to stimulate long- and short term trust in the population. A trustful relationship between the population and the crisis mangers can have mutual advantages as it may foster certain calmness in the population, while it can enforce the integrity and reliability of the data collector at the same time. Don't base the data collection on dubious information or sources. Be transparent and clear about the method for the data collection when you eventually distribute the collected information, since having a general level of trust in society makes it easier for people to put their wellbeing in the hands of other people.

## **Technology Dependency- Flexible Solutions:**

There is a risk that the collected data can be biased or derive from imprecise or wrong variables or criteria [95] (for example that not all relevant societal groups are represented in a data set that is supposed to illustrate the population), or that other methods for data collection would be better fitted to the cause (for example that targeted survey can give more precise information than harvesting Big Data). Using imprecise variables can produce skewed results or data that is not appropriate for the task<sup>47</sup>. Skewed data sets can also be a result of technology dependency, i.e. that

<sup>&</sup>lt;sup>47</sup> E.g. The European Commission launched 'antitrust charges' against Google in spring 2015 claiming that Google uses their dominant position in search by systematically favoring its own products in general search results. See for example: http://www.siliconbeat.com/2015/04/15/google-hit-with-european-antitrust-charges/

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	63 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>46</sup> And by adhering to the general European Data Protection regulations, many of these risks are already minimized, since the collection of personal data are regulated in every European legislation. [88]



the technology we choose for a certain task in reality determines what kind of data it allows us to collect and sensibility say something about [132], hence representative samples are important [90]. However, adhering to the principle of data minimization, that means to collect as little data as necessary, is a good way of clarifying what the data can and cannot say something about<sup>48</sup>. If only relevant data is collected, this will result in a more focused and precise data set. Somewhat paradoxically, sets of data deriving from focused and precise data collection can actually contribute to flexibility in the crisis management context, for example because the scope and limitations of the data are clearly defined, and thus, the processing of the data can be more easily regulated and governed, making the potential utilization and coherence of the data more apparent and more flexible to be re-used in different CM contexts.

• **Recommendation:** Account for the data collection methodologies you choose, and reflect upon the fact that some technologies and collection processes can be limiting, as they influence what data can be collected. For example, data collection by a drone provides the crisis manager with visual images (which has its own advantages and imitations), while collecting data through a mobile phone application allows for the inclusion of other context factors (that you would not get from using a drone). Only collect the data you need. Reflect also upon whether the data collection generally contributes to more flexibility, by considering how more easily regulated and governed datasets can make the potential utilization and coherence of the data (in the future and in other parts of the CM organization) more flexible, and thus increase transferability in CM.

## **Suspicion- Trust:**

Collection and storage of data can influence trust if the data is not collected and stored for the right purpose and according to the agreed terms (risking function creep etc.). This could lead to suspicion or uncertainty, as individuals would not be made rightfully aware of how their data is being collected and stored [96]. On the other side, being open about the data collection can foster trust in the population, making it easier to rely on their self-reported data during a crisis, because a trustful relationship has been established [95]. This can make it easier for crisis managers to deploy resources to the most affected areas, because the data is collected from the public in an environment of general trust.

• **Recommendation:** In order to establish the population's trust in the CM solution, be as open as possible about the way the data is being collected, how it is being used and stored, with whom it will be shared, and when it will be deleted. To build trust, and especially when introducing new methods for data collection, make sure to inform the population in a sufficient manner. Integrating information about the data collection only in the fine prints of the "terms and conditions" does not build trust. Make sure that the consent given is *active* consent, meaning that the individual who is sharing his data actively (not just passively, by receiving a letter about it) agrees to the data collection. Depending on the scope and depth

<sup>&</sup>lt;sup>48</sup> For a suggested terminology for privacy by data minimization, see Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	64 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



of the data collection, consider other ways of informing the public about it, such as media information campaigns. As part of this, also pay attention to the fact that any individual from whom the data is collected from whom personal data is being collected has the right to launch a subject access request allowing her to access all the data that the data controller has stored about her. On EU level, the right to access is defined in Article 12 of the European Union Data Protection Directive (DPD) [46].

## In/justice & in/equalities, Social Cohesion, Proportionality:

Collecting data from a specific religious group can foster inequalities if the data collection is carried out in a way that makes members of the group feel suspected of something that they experience as irrelevant [47] (for example if the data collector gives more weight to the meaning of religion in their everyday life than they do themselves). However, (if done right) through the inclusion of data from minorities, crisis management has the opportunity to better the situation for these groups. This can happen by selecting participants in an equal and just manner, and by making sure that the different represented groups are proportional to reflect the real life situation [90]. By taking minorities into account, this can have a positive influence on the social cohesion, as it would demonstrate that marginal groups are an equally important part of society as other groups.

• Recommendation: Data collection and storage must happen in a way that does not infringe upon the social cohesion of the population. Avoiding the collection of data that can create suspicion (e.g. if it is seen as unjust or as fostering inequalities by focusing in particular on a certain ethic group without a clear reason), can happen by e.g. ensuring proportionality in the data collection, and by communicating this in an open and transparent manner to the individuals from whom the data is collected. The argumentation for the choices made should be as transparent as possible, and the data collected should be proportional to the case, e.g. not include more sensitive data than necessary. When relying on data collecting mechanism that require certain equipment (such as a cell phone or a computer), compensate for the fact that not all members of society have access to such equipment (for example due to low/ high age, loss of income, homelessness, etc.). Marginal groups should be equally included in the CM activity that includes the data collection as other groups.

## Solidarity, Diversity, Cultural & Gender Sensitivity:

Data collection can also influence solidarity and diversity if the population feels unfairly targeted by the data collection. The principle of solidarity includes sharing both benefits and burdens, and data collection from one particular group could negatively influence solidarity if the basis for the selection of the target group is controversial (for example, if the opinions of a controversial religious community are side-lined with more conventional religious communities). Cultural and gender sensitivity is a key point here, as the data collection could be skewed by not taking diversity (including gender, marginal groups and cultural variables) into account when planning/ implementing the data collection [96]. However, if implemented with care, data collection and storage can also provide opportunities to foster societal security and resilience. Solidarity can be fostered indirectly

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	65 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



by data collection through/ for CM activities, e.g. by setting up diverse teams and working groups for the CM activity, seeking to include the representation of data collected from all genders and different cultural backgrounds. Ensuring the inclusion of feedback from a diverse group of people not only provides you with more variables, but also makes the CM activity more applicable in real life [96].

• **Recommendation:** When planning the CM activity, make sure that those subjects you collect data from are diverse, and selected on an equal and fair basis. Accounting for diversity concretely means including variables such as language, ethnicity, gender, culture and religion in the selection of participants or volunteers for the CM activity. This will ensure a more broad and accurate feedback, in addition to fostering opportunities for enforcing solidarity and diversity.

## Participation:

Public participation could be negatively influenced, both in the short and long term, if the data collection and storage is not done or based upon consent and a notification to the individual from which the data is collected in advance [96]. Furthermore, this could result in a "chilling effect" [48] where individuals change their behaviour and willingness to participate in certain activities because of concerns about how the collected information can be processed or used at a later point in time. This is especially relevant for CM activities such as training exercises or simulations, where sensitive personal data is collected about the participants. However, in general, participatory approaches to the development of CM solutions are advisable, especially if the final CM tools are meant to be used by the general public<sup>49</sup>. A higher level of public participation necessitates trust (cf. *trust*) between the population and the crisis managers, and messages that are clear and easy to understand for the public participating [133].

• **Recommendation:** To create a sustainable environment for participation, make sure to collect informed consent and to notify the relevant individuals before collecting data. Limit especially the collection of sensitive data, such as health information or political information. Aim for participatory approaches to the development of CM solutions, especially if the final CM solutions are meant to be used by the general public. Pay attention to maintaining a trustful relationship between the population and the crisis managers, and give clear and easy messages to the public in order to stimulate a transparent (cf. *transparency*) way of participating in the CM activity.

## Diversity, Dignity & Non- discrimination:

If diversity is not reflected in the selection of the population serving as test-, focus- or target group etc. for the development of CM solutions, the result will not be generalizable and representative [90]. For example, the question could be asked if the focus group reflect the actual distribution of gender and age that is included in the target population. Also, not respecting individual privacy can

<sup>&</sup>lt;sup>49</sup> This can for example happen via crisis management exercises involving the public.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	66 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



be seen as not respecting individual dignity<sup>50</sup>. If the collected data that is the basis for the development of CM is diverse and representative and does not discriminate against certain groups in society (either by leaving them out or by excessively focusing on them), data collection can on the other hand be a useful and necessary method for getting a better picture of the (crisis) situation, and thus make it easier for crisis managers to make decisions that respect individual's dignity, and finally to create CM tools that are more applicable.

• **Recommendation:** Avoid CM solutions for data collection or storage unnecessarily targeting certain groups, as this could be seen as a discriminatory practice. Account for diversity in both the planning and deployment of the data based- CM solution, including general variables such as language, ethnicity, gender, culture and religion. Although these variables are considered sensitive data, this will make the data more fair and non-discriminatory, but only of the information is not used to make decisions that can have negative implications for the groups. Don't reuse sensitive data, and don't use that information to discriminate against the groups from which the information derived.

## Political Reputation, State-Citizen Relationship:

Disproportional and hidden data collection will very likely influence the political reputation of the state or state actors in charge of the data collection process vis-à-vis its citizens [44]. On the other hand, including the population into data collection in a clear and transparent manner, adhering to all relevant data protection legislation, can foster a sense of participation (cf. *participation*) in the population, creating a feeling that they are contributing to bettering the CM situation, and thus it can have a positive influence on both the political reputation of the relevant actors (if the data collection is done in a good manner) and it can similarly contribute to resolving potential boundaries between the state and the citizens, by having a more participatory approach to the development of crisis management solutions<sup>51</sup>.

• **Recommendation:** To avoid influencing the relationship between state and citizens in a negative way as well as to protect the political reputation of the CM actor (whether professional, tool developer, volunteer, etc.), open, clear and timely communication is paramount. A participatory approach to the development of CM solutions (involving the public) can, if done in a good and sensible way, positively influence the political reputation of the CM actor, also because it makes it easier for the CM actor to take the diversity (age, gender, culture etc.) of the population into account (cf. *diversity*).

## Negative- Positive Standardization, Freedom & Protest:

<sup>&</sup>lt;sup>51</sup> There are efforts to develop normative criteria for evaluating models of the participation process. E.g. via the concept of social learning, the authors discuss how communities of people with both diverse and common interests can reach agreement on collective action to solve a shared problem. Webler, T., Kastenholz, H., & Renn, O. (1995). Public participation in impact assessment: a social learning perspective. Environmental impact assessment review, 15(5), 443-463.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	67 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						

<sup>&</sup>lt;sup>50</sup> Privacy can indeed be seen as an aspect of human dignity. See for example Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. NYUL Rev., 39, 962.



Making the collection of digital data the norm for CM solutions can become a negative standard if it normalizes data collection as the solution to a CM problem, when other kinds of data or solutions are equally suited to reach the same goal (or even other forms of doing data collection better suited) (c.f. e.g. the principle of data minimization). Data collection could infringe upon freedom and the right to protest if data collection targets certain groups, making them feel uneasy or suspicious of being disproportionally surveyed [se for example 114]. Furthermore, the "chilling effect" [48], that someone changes their behaviour because they fear that their original behaviour can have negative implications for them, can be seen as a negative consequence of a lack of freedom and the right to protest. On the other side, data collection can positively influence the right to freedom and protest, e.g. by allowing participants in focus groups or interviews to share their opinions about CM-related problems with someone that actually has the possibility and decision-power to make it better. In addition, the mere concept of data collection, as it becomes more common, can lead the way for the adjustment or implementation of official standards that can stand as positive standardizations of a given practice (e.g. a new standard that better defines or improves the rights of the individuals to access their personal data).

Recommendation: In most cases data collection for CM is unavoidable (such as pooling of data in public registers), but the data collector should inform the relevant individuals prior to the data collection exercise and respect their right to object to their data being collected. Consider also if the data collection itself is necessary, especially when it comes to intrusive data collection. Including the diverse population in focus groups and interviews, and let them raise their concerns as far as possible. Ensuring a continuous high level of compliance with the abovementioned recommendations in the relevant CM solutions can contribute to making best practice data collecting solutions the standard procedure for CM.

## 3.3.1.1 Summary of recommendations: Fostering positive impact when working with collection and storage of data

When working with solutions that collect and store data, the main principle to keep in mind is legality. Specifically data protection regulations to protect the privacy of those whose data may be collected. Suitability and proportionality are two other key terms, and when working with such solutions, the question should be asked if the data collection is really necessary, and if those data are best suited to fulfil the given function (and can the data be encrypted or anonymized?). This is especially relevant for sensitive personal data. The relevant Data Protection Authority should be consulted, especially if there are grey legal areas for new technology etc. To minimize potential infringements and to increase the social acceptability of the CM solution, consider embedding privacy friendly design choices and privacy friendly defaults in the data collecting tools, as part of a "Privacy-by –Design"- approach. The principle of data minimization should be followed (do not collect more data than you need, and do not store it for longer than it's needed), and data should generally not be reused for other purposes. In terms of physical security, collected data must be stored securely (using e.g. locks, password protection or encryption). To enforce trust and limit the risk of suspicion, the collection of personal data from an individual should always happen on the

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	68 of 159		
Reference:	D840.21	Dissemination:	D840.21 Dissemination: PU Version: 3.0						



basis of informed consent, and be as transparent as possible. This can also enforce the integrity and reliability of the data collector. When choosing the data collection methodologies, reflect upon the fact that some technologies and collection processes can be limiting, as they influence what data can be collected. The variables regulating the data collection should also account for diversity. Reflect also upon whether the data collection generally contributes to more flexibility, by considering how more easily regulated and governed datasets can make the potential utilization and coherence of the data (in the future and in other parts of the CM organization) more flexible, and thus increase transferability in CM. In a practical sense, when relying on data collecting mechanism that require certain equipment (such as a cell phone), compensate for the fact that not all members of society have access to such equipment (for example due to homelessness). To avoid influencing the relationship between state and citizens in a negative way as well as to protect the political reputation of the CM actor, transparency in communication is paramount. A participatory approach to the development of CM solutions (involving the public) can, if done in a good and sensible way, positively influence the political reputation of the CM actor, also because it makes it easier for the CM actor to take the diversity (age, gender, culture etc.) of the population into account (cf. diversity).

## 3.3.2 Facilitating Data Processing (Incl. Operational Data Lift)

## Related WP and Tasks: T43.5, WP53, T36.2

Systems and solutions for the facilitation of data processing differ from the collection and- storage of data as the aim of data processing facilitation is to create, bridge or join systems of data processing. Here, the question is which impacts the processing can have on society. Furthermore, technology is most often the facilitator for data processing, i.e. digital systems which assist the progress of data processing. Within DRIVER, the facilitation of data processing refers to, for example, tools or methods facilitating interoperability, such as methods for improving the situational awareness by integrating information from different agencies and professionals (T43.5). The key question is here what makes the data processing possible, and how can this facilitation have negative or positive societal side effects? For example, in T43.5, the aim is to improve situational awareness by integrating and facilitating the processing of information from different sources (such as the use of mobile devices in the field) and on different levels. As the case is in T43.5, the merging of data from different sources can challenge the legality of the CM tools for example, if the regulative landscape is not up to speed with new data collection methods used (which, for example, is the case for the use of drones in Norway) [49], if the CM tools are challenged by the amount of data that is being processed, or if the facilitating mechanisms are not those best suited for the job. Another example of a potential societal challenge is when the facilitation of data processing refers to e.g. tools or methods facilitating interoperability between CM tools or measures. If DRIVER facilitates this data processing through a method that does not adhere to common ethical principles such as transparency, openness and legality, it can influence the integrity and the accountability of the data processor(s). Such a procedure further risks becoming a negative standardization for facilitation of data processing.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	69 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



## Assessments

# Technology Dependency- Flexible Solutions, Misuse- Protection, New Vulnerabilities- Progress, Function Creep- Specialized and Controlled Use:

New vulnerabilities can be caused by expansive databases,<sup>52</sup> as they are exposed to an increasing risk of hacking. For example, facilitating the conjoining of databases can influence the possibility of misuse or illegal use of data, simply because the quantity and quality of data changes once merged<sup>53</sup>. Also, because data collected for one purpose is transferred to another database that is used for a different purpose than the original collection (c.f. function creep). Facilitating the expansion of databases can also contribute to technology dependency, as, for example, merged databases require oversight and other forms of control that can be hard to manage manually, meaning without technological means (this is one of many definition of "big data"<sup>54</sup>). This can also increase the risk for function creep, as collected data could be used for new purposes. However, if certain conditions are met, facilitating data processing through digitalized solutions can have an added value and even foster protection and progress. For example, for countries facing recurrent crises, working with regional and international organizations to create platforms at country level for facilitating the exchange of information can be important to strengthen resilience [50]. Furthermore, by looking to find better ways of doing data processing can open up for more flexibility in CM operations. For example because this process may result in the crisis managers having more or alternative means of communicating during a crisis, something which could ultimately mean better protection of the crisis population or of the infrastructure in the affected area. A solution can actually be both flexible, and specialized and tailored to a particular problem at the same time. For example by making sure that safeguard towards the risk of function creep is better built into the solution. This can be done by making sure that the facilitation of data processing are implemented better vis-à-vis privacy (e.g. based upon the principle of 'privacy-by-design'<sup>55</sup>) or that it have been subject to a Privacy Impact Assessment (PIA) [51]. The result would be a solution that is as flexible as it needs to be, but that at the same time mitigates against known risks towards privacy.

• **Recommendation:** When planning CM measures, consider if there is a real need for facilitating the processing of data in the planned scale, and reflect upon whether the action is leaving you more vulnerable by creating more technology dependency. If this is hard to

<sup>&</sup>lt;sup>55</sup> The concept of «privacy-by-design» is an approach to ensuring that privacy and data protection are promoted in the early stages of a project or a development. Although this approach is not a requirement of the Data Protection Act, it might make it easier for the partners/ organizations to comply with their obligations under the legislation. For more information, and some description of benefits of « privacy- by-design », see for example : <u>https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/</u>

Document name:	D840.21 – A guid functions – Versio	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	70 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>52</sup> See for example Rosenblatt, A., & Attkinsson, C. C. (1992). Integrating systems of care in California for youth with severe emotional disturbance. I. A descriptive overview of the California AB377 evaluation project. Journal of Child and Family Studies, 1(1), 93-113. This article illustrates how the administration of databases and in particular the variables chosen to process the data in them, potentially can create vulnerabilities through facilitating e.g. discriminatory practises.

<sup>&</sup>lt;sup>53</sup> See for example Wu, X., Zhu, X., Wu, G. Q., & Ding, W. (2014). Data mining with big data. IEEE transactions on knowledge and data engineering, 26(1), 97-107, on how the enormous volumes of the data also make an application vulnerable to attacks.

<sup>&</sup>lt;sup>54</sup> See for example Ward, J. S., & Barker, A. (2013). Undefined by data: a survey of big data definitions. arXiv preprint arXiv:1309.5821.



avoid, have backup solutions available, e.g. alternative ways of ensuring that the collected data is being protected according to relevant regulations. The general principle is to minimize data processing wherever possible, and to only collect the data that is needed for the activity. When designing the measures that lead to the processing of data, and to ensure the efficiency of the procedure, Consider if a risk- or Privacy Impact Assessment (PIA) could be useful to tailor the solution (e.g. by minimizing the amount of personal data that is collected for processing). Minimize secondary insecurities and challenges like function creep, misuse and the creation of new vulnerabilities by making the limitation of data processing a (built-in) feature of the solution, for example through making a PIA mandatory. Working with regional and international organizations to create platforms for facilitating the exchange of information (or other means of data processing) can be important to strengthen resilience [50] and also push progress on the CM area.

## Suspicion- Trust, Transparency, Privacy & Data Protection:

Sharing data between two or more partners, can infringe upon trust in the professional environment [134]. This is the case when not all actors agreed upon data exchange, or when data sharing happened in the wrong way (for example when data protection principles were overlooked). On a long-term perspective, this could foreseeably lower trust within the cooperation. However, a solution that facilitates data processing and data sharing can also be an example of best practice in the area of data protection and the protection of privacy, if the legal principles are duly followed, and the process happens in a transparent manner<sup>56</sup>. Furthermore, adhering or contributing to such best practice standards can in itself influence trust positively, which again makes the implementation of the solution or the cooperation with the public less problematic.

• Recommendation: The facilitation of data processing largely falls under the general rules for data protection, and should adhere to the basic principle of legality. This includes acknowledging that although the data collection may be legal, the processing may not beand vice versa. Especially if the processed data are sensitive data, particular measures and requirements may apply (depending on national regulation). To avoid lowering trust between partners facilitating data exchange or other forms of data processing, ensure that the process is transparent, open, and adhering to all relevant legal data protection frameworks. Be clear and transparent when communicating with the individuals from whom the data is collected about the processing of data, stating why it is necessary, and why it is suitable for pursuing the given objective. When facilitating data processing, in terms of sharing data between two or more partners (or the public), ensure that involved actors have the opportunity to voice their questions and concerns. This can enforce trustful relationships both in the short and in the long term, and may even have positive spill-over effects onto other domains of the cooperation. Consider also if the data processing tools are disproportionate in relation to the interests affected. The facilitation should include

<sup>&</sup>lt;sup>56</sup> See for example Piwowar, H. A., Becich, M. J., Bilofsky, H., & Crowley, R. S. (2008). Towards a data sharing culture: recommendations for leadership from academic health centers. PLoS Med, 5(9), e183, for an example from the health sector.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	71 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



possibilities for encryption or anonymization of personal data whenever possible, even if this means that the possibility of the individual to withdraw (their data) from the activity or to access their data, disappears.

## Social Cohesion & Solidarity:

If data processing happens in a way that favours one social group over another, it can influence the social cohesion in the affected communities as some groups could feel discriminated. This is the case, for example, when data analysis gives more weight to the data collected from a certain group than from another without a sound reason. Impartiality is key<sup>57</sup>. This could also result in a breach in solidarity. However, if data processing tools are developed and deployed according to data protection legislation [88], they have the opportunity to positively influence social cohesion by ensuring equal and fair processing of data. This includes that the individual from whom the personal data was gathered, has the right to access her own data in a fair and just manner<sup>58</sup>. Furthermore, more indirectly, data processing solutions can positively influence solidarity if the result of the data processing turns out to contribute to creating better conditions for a social group that is usually overlooked or does not normally have a voice in the debate etc.

• **Recommendation**: Make sure that the data processing solution does not facilitate data processing that favours one social group over another, unless there is a good cause for it (such as adjusting for low- income countries). Such reasons should be communicated in a clear and transparent manner (cf. *transparency*). Ensure also that the data processing tools adhere to data protection legislation, and that they facilitate making claims of privacy such as exercising the data access right, which is a measure intended e.g. to create transparency in the data processing, and make it easier for the individual to know how their data is being processed. Developing and streamlining this practice can, especially in the long run, help fostering solidarity as it is an action that produces good standards in society.

## Accountability, Privacy & Data Protection, Negative- Positive Standardization:

The facilitation of data processing has to be based on an ethically acceptable method and take legal frameworks (data protection legislation for protecting individual privacy) [88] and other relevant guidelines into account in order to foster the accountability of the processor<sup>59</sup>. If not followed, data processing will negatively affect the public accountability of the data processor(s), because it could be seen as not valuing the core principle of responsibility and good governance [42]. Poor data processing also includes the risk of negative standardization<sup>60</sup> if an unacceptable procedure becomes

<sup>&</sup>lt;sup>60</sup> Standardization generally describes the process of developing a specific level of quality or attainment for materials, products and services in order to ensure that they are "safe, reliable and of good quality". Negative standardization then refers to the overarching social process of establishing a procedure as normal when in fact it has detrimental effects.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	72 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>57</sup> See for example Olsen, W. (2011: 14). Data collection: key debates and methods in social research. Sage.

<sup>&</sup>lt;sup>58</sup> This right, and other rights connected to individual privacy, can be found in Article 12 of the European Union Data Protection Directive (DPD). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050. The data access right is one of the most prominent individual rights here. <sup>59</sup> For example special regulations for new technologies such as drones.


the standard, furthering a society based on a high degree of control. However, adhering to legal regulations should be a given precondition for doing crisis management in all sectors and phases of the crisis. The positive standardization of procedures that helps the data processor in taking care of such requirements on an less complicated and manageable way, can not only make sure that legal regulations are more strictly followed. In addition, it has a positive impact on the accountability of the data processor and its partners.

• **Recommendation**: Make sure that the data processing is based on ethically acceptable methods, e.g. data protection regulations, in order to enforce the accountability of the data processor(s) by valuing core principles for good governance. The method or tool for facilitating data processing (such as data exchange), should include a mechanism for informing the individuals from whom the data is collected about how her personal data is taken care of in the process. To avoid negative standardization of data processing routines, planning- and impact assessments can verify whether the process. Following particularly good routines or mechanisms for ensuring legal compliance (and taking better care of individual privacy) contributes to a (positive) standardization or a normalization of best practice.

#### Integrity, Political Reputation:

If the facilitation of data processing does not adhere to common ethical principles (such as informed consent), it can influence the integrity of the data processor in a negative way, as the data processor can be regarded as inconsistent or insincere. Loss of integrity could also influence the political reputation of the data processor. However, following ethically 'best practice' regarding the data processing can in the same way influence the political reputation and the integrity of the CM actor in a positive way.

• **Recommendation**: The integrity and political reputation of the data processor(s), can be positively influenced if it is publicized that common ethical and legal principles are explicitly taken into account by the CM organization when developing and deploying the data processing tool. Communicate your compliance with such practice in a clear and transparent manner to the relevant parties.

#### 3.3.2.1 Summary of recommendations: Fostering positive societal impact when facilitating data processing

The facilitation of data processing is different from collection and storage of data, since the aim of these solutions is to create, bridge or join systems of data processing. The principle of data minimization is also relevant when working with solutions for facilitating of data processing, and this means that the question should be asked whether there is really a need for data processing in the scale requiring the facilitating solutions (proportionality), and that only data needed for the case should be processed (suitability). If new technologies are needed to process data of the relevant scale, this could foster a form of dependency upon technologies that can create vulnerability in case

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	73 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



this technology falls out. For example, a commonly known feature of digital "big data" is that it can only be processed using technologies. If the reliance on certain technologies is hard to avoid, have backup solutions available, e.g. alternative ways of ensuring that the data is being protected according to relevant regulations. In general, it is crucial that the systems adhere to data protection principles and regulations, and the process should be open and transparent, to foster trust between the relevant actors, and to foster accountability for the data processor. Especially if the processed data are sensitive data, particular (national) measures and requirements may apply. Following particularly good routines or mechanisms for ensuring legal compliance (and taking better care of individual privacy) contributes to a (positive) standardization or a normalization of best practice. The purpose and conditions for processing personal data should always be communicated to the data subjects. Minimize secondary insecurities and challenges like function creep, misuse and the creation of new vulnerabilities by making the limitation of data processing a (built-in) feature of the solution, for example through making a PIA mandatory or by including possibilities for encryption or anonymization. Developing and streamlining privacy- friendly practices can, especially in the long run, help foster solidarity as it is an action that produces good standards in society. Furthermore, data from different societal groups should be processed equally fair, and reasons for a potential weighing should be communicated in a transparent way.

### 3.3.3 Analysis & Evaluation

**Related WP and Tasks:** T33.1, WP34, WP35, T36.2, T36.3, T43.1, T43.2, T43.3, T43.4, T43.5, T44.4, WP53

Any CM activity includes the collection of data. This data can have several attributes, and the collection and storage of it may happen in various scales. But what happens with the data once it has been collected and stored? Data analysis and evaluation is a form of data processing that is crucial for CM, as it provides the very basis for learning, and for developing new solutions for CM. It is often a necessary precondition for innovation and progress in the CM field, however, limits e.g. needs to be set for the use of the data. To analyse data can mean to handle, alter, treat or refine data. Various kinds of data and information are being analysed and evaluated throughout DRIVER. This happens, for example, in relation to data collection such as through an airborne sensor suite that includes an on-board processing system and a direct data link from the airborne platform to ground (T43.2). For example, in T43.2, the aim is to improve airborne sensor capabilities, for example through testing the usage of mobile sensors within a flood scenario. The use of such technology will include the analysis of information deriving from geo-referencing. A challenge here can be that legislation regulating the potential use of such data is not equally well developed in all European countries, e.g. because the use of UAV technology does not have a long tradition within civil sector use [42] [49]. Another potential challenge is that when collecting personal data, it is crucial to let the individuals who contribute with their personal data know what the purpose for the data collection is, and how it will be analysed and used [88]. When collecting data for one purpose, e.g. gather information about the movement patters of residents in a certain area for CM logistics purposes, this data cannot be reused in order to analyse their health status (c.f. function creep).

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	74 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



## Assessments

#### Privacy & Data Protection, Unease- Calmness:

If the data processing and analysis tools do not uphold principles of legality, they can jeopardize the CM activity [42]. If they contain personal data, they can create unease particularly for the individuals from whom that data was collected, because their personal data risks being misused or not treated according to the agreement. In general, operating with analysis and processing tools that are in the grey area of legality (this may also happen unintended, e.g. if the legal landscape has gaps or are not yet developed) [42] can have damaging spill-over effects onto other domains. It can create unease, both for involved internal actors, the individuals from whom that data was collected and for cooperating partners. However, fulfilling legal requirements can be a calming factor in that situation [88]. If there is un-clarity or rumours spread regarding the implementation and legality of a new crisis management solution, the responsible CM actor should be able to demonstrate that such requirements are fulfilled, and point to the relevant regulations supporting this. Furthermore, if the tool or method is legal, and founded in legal practice, it means that it is more likely that oversight mechanisms are in place for making sure that they keep following the rules also in the future. This will have a calming effect.

Recommendation: Analysis and processing of data and information needs to have a predefined purpose and happen according to data protection legislation in the country where data Is collected. This needs to be done to make the output legally usable and to protect the data protection rights (such as informing the individuals from whom the data is collected in advance) of the individuals from whom the information is gathered. Stay updated on all relevant legal guidelines and regulations affecting the analysis method or evaluation tool (or similar) to be better prepared to ensure and "calm" potential actors inquiring about the data processing.

#### Suspicion-Trust, Political Reputation, Function Creep- Specialized and Controlled Use, Integrity:

Security in data processing (including analysis and evaluation) has a lot to do with trust [52]. If the data analysis or evaluation does not adhere to the predefined arrangements and rules, it can negatively influence the trust between whichever parties are involved (this can for example happen via a function creep). If an actor does not believe that another actor of the arrangement is reliable, good and honest, this can influence the political reputation of the actor at stake, and not be as willing to give his information [48]. The data analyst has an individual responsibility for maintaining information security with regard to confidentiality, integrity and accessibility.. This can influence the integrity and reputation of the data controller negatively, but data analysis may also have a positive societal impact. In addition to the fact that the results and lessons learnt deriving from a data analysis or evaluating data can also contribute in building a trustful relationship, e.g. with the individuals from whom that data was collected, if it happens transparently and according to

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	75 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



agreement. If the data is analysed and evaluated with a clear purpose, and not stored for longer than necessary, this can further have a positive impact on the integrity of the data analyst, e.g. because this kind of transparency may work as an indicator that the data is less prone to function creep and that the data analyst is trustworthy.

• **Recommendation**: Make sure that data analysis happens with a clear and predefined purpose, meaning that the use of it is controlled and specialized to the aim. Make sure that the data is only put to use for the purpose it was collected for, to uphold or strengthen the integrity and political reputation of the data controller, and to minimize the risk of function creep. To enforce trust, set rules that limit the role of the data controller or the legally responsible actor, e.g. to ensure that the data is secure with regards to confidentiality, integrity and accessibility.

#### Suspicion- Trust, Misuse- Protection:

If the data controller does not fulfil the legal responsibility to ensure that the data is treated according to the relevant data protection legislation<sup>61</sup>, the people from whom the data stems can feel suspicious or uneasy about their privacy rights (such as the right to be informed and to access your data). If limitations for unrightfully accessing a data set are not determined, the data risks being reused or misused by someone obtaining illegal access to it (e.g. via function creep). This can also create further unease among the affected individuals if it becomes known that the data processing was illegal or unrightful [48] [44]. However, analysing data can also foster a culture of trust in two ways: Firstly, the results or outputs of the analysis can actually improve the situation for a certain societal group, e.g. if research indicates potential for bettering the conditions concerning the level of trust in society<sup>62</sup>. Secondly, trust can be fostered by the very method of analysing or evaluating data, e.g. if the data are sufficiently protected by data protection regulations that takes good care of individual privacy, demonstrating good practice by the data controller, which could also foster a good and trustworthy reputation in other domains (i.e. adhering to general data protection rules and regulations).

• **Recommendation**: The purpose for data analysis or evaluation must be clearly communicated. When analysing personal data, the individuals from whom that data was collected must be made aware of the full use of the data, and their claims and comments should not be re-interpreted in a different context later. For example, when collecting data for one purpose, e.g. gather information about the movement patters of residents in a certain area for CM logistics purposes, this data cannot be reused in order to analyse their health status. To enforce trust, and to minimize the potential for misuse and suspicion, rules should be set to limit the role of the data controller or the legally responsible actor<sup>63</sup>.

<sup>&</sup>lt;sup>63</sup>FHG will provide legal and regulatory advice to the DRIVER project, and the ethical procedures, risks and safeguards for responsible research (including, but not limited to SC15), can be found in D91.3.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	76 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>61</sup> In Norway e.g., the relevant legislation is the Personal Data Act of 2000, but since regulations can vary from country to country, always consult the data protection regulations that are closest to the data collecting activity.

 <sup>&</sup>lt;sup>62</sup> For an example on trust towards electronic banking, see: Munoz-Leiva, F., Luque-Martínez, T., & Sánchez-Fernández, J. (2010). How to improve trust toward electronic banking. Online Information Review, 34(6), 907-934.



Consider setting goals like the authentication of system users, the use of encryption and decryption, deletion of data in case of system failure (especially for sensitive data), and other goals to ensure trustable and secure data processing. Such measures can foster trust in the more general sense, both from the user's perspective and from the perspective of the individuals from whom the data is collected.

#### Data Protection & Privacy:

If a data analyst has dramatically different standards than other comparable or cooperating actors, it can make data exchange and analysis more difficult, e.g. because the results may be incomparable due to such variations in starting points. This can happen e.g. if the common ethical principles for data collection vary between two data collecting states, while the data is being analysed or evaluated on the same basis afterwards (such as overlooking the importance of representative samples [90]). It should also be noted that although such differences in regulation may strictly speaking be legal, the use and evaluation of the data might have a negative impact, if the biased or different starting points are not taken into account in the evaluation. However, although data protection legislation differs also within the EU, the main principles are largely coherent. In the long term perspective, difficulties with differing standards may also contribute positively in society by pushing the agenda in terms of European data protection standards forwards, e.g. as it enforces changes in regulations and legislations as a consequence of the need for alignment of regulations managing new types of data processing needs (c.f. positive standardization).

• **Recommendation:** Reassure the individuals from whom the data is collected about the protection of their privacy according to established data protection rights. Up to a certain point in the process (usually until the data is anonymized or encrypted) allow the individual to withdraw their personal data. Establish and keep connections with the local or relevant Data Protection Authorities, and use this resource for directing questions or challenges to, as it may potentially benefit and lay the groundwork and for other data processing actors in the future. Seize opportunities to follow best- practice for data protection and privacy rights. When collaborating with international actors on data collection and analysis, follow the data protection rules of the country with the highest data protection standards.

#### **Open- Control Society, Accountability:**

If too much data and information is being analysed without a clear objective, it can contribute negatively towards a society of control, because the analysis and evaluation of data most likely also includes collection and storage of more data than necessary (c.f. data minimization principle). If the analysis process is opaque and poorly regulated, it can create the impression that the data controller is not accountable<sup>64</sup>. However, adhering to data protection rules and regulations [88], and even seizing the opportunities for doing best-practice in this regard, can be a step towards creating the impression of an accountable company or organization (or similar). In the more long-term

<sup>&</sup>lt;sup>64</sup> See for example Beeman, S. K. (1995). Maximizing credibility and accountability in qualitative data collection and data analysis: A social work research case example. J. Soc. & Soc. Welfare, 22, 99.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	77 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



perspective, analysing crisis management data can contribute to a more open society, if all relevant groups in society are contributing equally to the data that is subject to analysis.

• **Recommendation:** In addition to not collecting and analysing more data than you need for the particular purpose (and to not reuse this data uncritically), the process of doing data analysis and evaluation needs to be transparent and as open as possible in order for the involved actors to experience that their data is being processed in a rightful manner, and to ensure that the accountability of the data processor is maintained. When relevant, ensure that the analysed data is made up of contributions from a wide range of diverse societal groups, as equality and freedom of thought are examples of traits of an open society<sup>65</sup>.

#### International Relations, Political Reputation:

There is a possibility that the implementation of legal regulations for data protection [88] are different between partnering countries (e.g. between Schengen member states and non- Schengen member states). This might challenge the data analysis and evaluation or even encourage the actors to take legal or ethical shortcuts. Not regulating international cooperation between CM actors with established regulatory or legal frameworks (such as [88]) can negatively influence the political reputation of the actor(s), and might potentially cause further spill-over effects into other domains of international relations and cooperation such as trade. Considering the potential publicity and media interest, such developments are not only unfortunate for the area of CM, but also for the international political climate. However, international relations between states and actors is a precondition for CM cooperation across borders, and bears with it many opportunities that are advantageous for positive influence and positive impact on not only the relationship between two parties, but for society as a whole<sup>66</sup>. For example, when the analysis of collected data allows for the identification of (regulatory) gaps, this becomes an opportunity not only to close or minimize the actual gap, but also to foster better and more constructive working conditions and climate for future CM cooperation, which results could potentially be beneficial to society as a whole.

• **Recommendation:** Pay attention to opportunities for fostering a positive climate in the international relation(s), and if relevant, see how you can organize the cooperation in a way that can be made sustainable also beyond the specific issue at stake.

#### Accountability, Integrity, Privacy & Data Protection:

If the way in which data is being analysed or evaluated causes suspicion (c.f. suspicion) and unease (c.f. unease) among the population, it can be said to negatively impact the accountability of the data analyst<sup>67</sup>. This happens for example when poor analysis/evaluation procedures (e.g. such as not

<sup>&</sup>lt;sup>67</sup> A well-know example from the surveillance context is the NSAs bulk collection of data. See [44]

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	78 of 159	
Reference:	D840.21	B40.21         Dissemination:         PU         Version:         3.0						

<sup>&</sup>lt;sup>65</sup> The concept of the open society was originally brought forth by Henri Bergson. See for example Henri Bergson, Les Deux Sources de la morale et de la religion, Félix Alcan, 1937 [1932], pp. 287–343. Available at : <u>https://fr.wikisource.org/wiki/Les Deux Sources de la morale et de la religion/Chapitre IV.</u> The concept is now widely used in various academic disciplines, such as criminology, political science and sociology.

<sup>&</sup>lt;sup>66</sup> See for example chapter 8 and 9 in Coppola, D. P. (2006). Introduction to international disaster management. Butterworth-Heinemann, for a presentation of the diverse set of actors involved in international crisis management.



limiting access to collected personal data) are seen as a sign of the actor undervaluing core ethical and societal principles such as the protection of privacy. In a similar way, the integrity of the data analyst/evaluator can also be questioned. However, ways of analysing or evaluating data can also have positive effects, based on the fact that the opportunities for collecting data are (practically) bigger than ever, including sophisticated analytical tools that can make the evaluation and analysis of the data more precise and useful (e.g. because you can search for only the data you need for doing the analysis). This wide access to data collection due to progressing technological solutions can provide new opportunities for CM<sup>68</sup>. In addition it can actually be a way of taking better care of individual privacy, as the data can more easily be encrypted before the analysis. Setting best-practice standards for such processes can have a positive impact on the integrity and accountability of the data analyst actor, but also further societal impacts if the methods or considerations are adopted by other actors.

 Recommendation: Plan the analysis and evaluation process adhering to high ethical and societal principles (such as privacy) in data analysis to enforce the accountability and integrity of the actor(s). Aim for best practice in the data analysis, including the encryption of data when possible, and by only collecting or drawing out the data you need for doing the particular analysis.

#### Suitability, Freedom & Protest:

If the data analysis is not done in accordance with the predefined purpose for the data collection, this can be seen as a form of misuse of the collected data (a form of function creep), and there is a risk that the individuals from whom that data was collected wants to withdraw personal data. Should the data analysis and evaluation happen in such a way that it does not allow the individual to access or withdraw their personal data from the collection, as per data protection legislation, it can be seen as hindering or limiting individual's freedom or the right to protest against unwanted or unrightfully data analysis and evaluation<sup>69</sup>. However, by making sure that you are implementing and following the relevant data protection regulations for the activity, the collected data are better protected, and the individuals from whom that data was collected are made aware of their rights and their opportunities to disagree or withdraw (as found in [88]). When you adhere to such principles, you not only take better care of the individual from which the data derives, but you can also have a positive impact on future CM activities by directly or indirectly encouraging them to participate or contribute to similar activities in the future.

• **Recommendation:** Make sure that the collected data is analysed in a suitable way, for example by ensuring that the data is collected based on fair and just principles, and that the data are the best data to analyse in order to say something about the issue at stake. Establish clear procedures and mechanisms which allow the individuals from whom the data is

<sup>&</sup>lt;sup>69</sup> On EU level, the right to access is defined in Article 12 of the European Union Data Protection Directive (DPD) [46].

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	79 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>68</sup> There are many examples of technology/ new data based opportunities that are making crisis management less complicated, but one example on the case of so-called « Big data » can be found in Hay SI, George DB, Moyes CL, Brownstein JS (2013). Big Data Opportunities for Global Infectious Disease Surveillance. PLoS Med 10(4). Available at: http://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001413



collected to exercise and voice their data protection rights and claims, such as the right to withdraw and access their data according to the relevant data protection regulations. Make sure that the data analysis process is resulting in an analysis of data that are appropriate and applicable for the particular task.

## 3.3.3.1 Summary of recommendations: Fostering positive societal impact when working with information analysis & evaluation

When working with solutions for analysing and evaluating data and information, the key recommendations relate to issues of data protection and privacy, and it is advisable to keep contact with the local or relevant Data Protection Authorities. In order to uphold or strengthen the integrity and political reputation of the data controller, analysis and processing of data and information needs to have a predefined purpose (which would control the use of the data) and happen according to data protection legislation in the country where data is collected. This could also reduce the risk of function creep. When analysing personal data, the individuals from whom that data was collected must be made aware of the full use of the data, and their claims and comments should not be reinterpreted in a different context later. For example, when collecting data for one purpose, e.g. gather information about the movement patters of residents in a certain area for CM logistics purposes, this data cannot be reused in order to analyse their health status. To enforce trust, and to minimize the potential for misuse and suspicion, rules should be set to limit the role of the data controller or the legally responsible actor. When collaborating with international actors on data collection and analysis, aim for best practise and follow the data protection rules of the country with the highest data protection standards. Consider setting goals like the authentication of system users, the use of encryption and decryption, deletion of data in case of system failure (especially for sensitive data), and other goals to ensure trustable and secure data processing. Such measures can foster trust in the more general sense, both from the user's perspective and from the perspective of the individuals from whom the data is collected. Furthermore, when relevant, ensure that the analysed data is made up of contributions from a wide range of diverse societal groups, as equality and freedom of thought are examples of traits of an open society . Make sure that the collected data is analysed in a suitable way, for example by ensuring that the data is collected based on fair and just principles, and that the data are the best data to analyse in order to say something about the issue at stake.

#### 3.3.4 Communication between first responders

#### **Related WP and Tasks:** WP35, T43.3, T44.2, T44.3, WP45

It is fundamental for effective and sound crisis management that crisis management professionals are able to be in constant communication and exchange data and information through secured and

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	80 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



interoperable systems to ensure an appropriate and consistent response<sup>70</sup>. At this point it is also important to remember that "communication" can be understood in several ways, such as in terms of the content of what is being communicated or the process of communication. Technical research and development activities tend to focus more on how the technical process of communication can be improved to support the communication of the content<sup>71</sup>. For coordinating a CM activity, both, the strategies<sup>72</sup>, roles<sup>73</sup>, and technological solutions<sup>74</sup> are crucial. In an interconnected world, where a crisis often transcends geographical boundaries, it is important to set up a well- regulated form of inter/intra- CM communication to ensure both legal, ethical and societally friendly processes collaboration processes. For example, in large-scale cross-border response actions, multiple stakeholders from different organisations, levels of command and nations have to communicate. DRIVER WP45 tackles that issue by improving IT based collaboration tools and structured information exchange for the communication between CM professionals. An overreliance on one technology, such as relying too much on a web-based architecture without thinking about tried and tested fallback solutions such as conventional radio, may raise the vulnerability. Another example of a potential societal challenge can be found in DRIVER 44.2, where the aim is to improve the efficient and effective assignment of resources during a crisis, through monitoring the actions taken by responders and the allocation of resources. This task includes cross- border cooperation, reporting, assignment of resources prioritized per task, and other actions that makes it crucial to have good solutions for cooperation between crisis managers.

### Assessments

#### **Technology Dependency - Flexible Solutions:**

If entirely based on technology, that is vulnerable for failure and breakdown, there is a risk that the communication between crisis managers may be prone to technology dependency [102]. This happens when there are no alternative ways of communicating, and one over-relies on a certain technology that is used for communicating. For example, to rely only on smartphones makes a communication system vulnerable if the GSM technology fails during a crisis. Technology dependency does not only lead to vulnerability in case of outage [102] but also when based on closed technology provided by a single vendor, such as with proprietary software that may stop to be updated and supported when the vendor stops existing leading to security issues.

<sup>&</sup>lt;sup>74</sup> See for example Heath, C., & Luff, P. (1992). Collaboration and controlCrisis management and multimedia technology in London Underground Line Control Rooms. Computer Supported Cooperative Work (CSCW), 1(1-2), 69-94.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	81 of 159	
Reference:	D840.21	Dissemination:         PU         Version:         3.0						

<sup>&</sup>lt;sup>70</sup> See for example Akella, M. K. (2009). First responders and crisis map symbols: Clarifying communication. Cartography and Geographic Information Science, 36(1), 19-28.

<sup>&</sup>lt;sup>71</sup> Such as in Kumar, V., Rus, D., & Singh, S. (2004). Robot and sensor networks for first responders. IEEE Pervasive computing, 3(4), 24-33.

<sup>&</sup>lt;sup>72</sup> See for example Militello, L. G., Patterson, E. S., Bowman, L., & Wears, R. (2007). Information flow during crisis management: challenges to coordination in the emergency operations center. Cognition, Technology & Work, 9(1), 25-31.

<sup>&</sup>lt;sup>73</sup> See for example Wagner, T., Phelps, J., Guralnik, V., & VanRiper, R. (2004, July). COORDINATORS: Coordination managers for first responders. In Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems-Volume 3 (pp. 1140-1147). IEEE Computer Society.



• **Recommendations:** As developer of CM solutions, take into consideration, that web-based communication may be of great added value for enabling interoperability, but if possible, ensure that sufficient non-electricity/non-high-tech based ways of communicating is available as backup systems, in order to minimize vulnerabilities. As decision maker you should consider establishing regulations for foreseeing to keep backup procedures in the case of a failure of new technologies and to make sure to have alternative plans and redundancies for communication systems as part of your resilience plans to avoid complete dependency on one communication channel. Also when procuring for new solutions flexibility and openness of the system may be formulated as high level prerequisite.

# Function Creep- Specialized and Controlled Use, Unease-Calmness, Suitability, Necessity, Proportionality:

First responders are increasingly relying on digital solutions and infrastructure<sup>75</sup>.Prioritizing communication from population to crisis managers (emergency calls) or internal responder communication might indirectly contribute to saving more lives and thus be required by crisis management, but at the same time it may limit the communication possibilities within the population. In extreme situations when the population is desperately trying to get in contact with their relatives to know about their whereabouts, it may even cause unease<sup>76</sup>. However, ensuring solid communication channels for crisis managers will make it easier for CM personnel to give more suitable advice to the population, and thus (indirectly) make the population calmer. In the onset of a crisis, such advice may for example be to prepare for a lack of communication possibilities.

• **Recommendation**: As a decision maker you should closely examine the suitability and necessity of prioritizing data, and inform the public when establishing such measures. Additional awareness rising for the population, on how to prepare for communication outage (e.g. agree a meeting point with your family in case you are separated and can't reach each other) may be a good accompanying measure.

#### Function Creep- Specialized and Controlled Use, Misuse- Protection:

Data exchange can increase the risk of function creep, i.e. that the data is reused for different or additional purposes than it was collected for. This is a bigger risk if the data being exchanged consists of (partly) unnecessary data, which makes it easier for the receiver of the data to find new uses for the exchanged data or to use data that is "left over" from the original purpose to solve another problem. Generally, such reuse goes against the data protection principle of data minimization (only

<sup>&</sup>lt;sup>76</sup> See for example: Weiss, Todd R. 2007, In emergencies, can cell phone network overload be prevented? Available at: <u>http://www.computerworld.com/article/2539929/mobile-wireless/in-emergencies--can-cell-phone-network-overload-be-prevented-.html</u>

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	82 of 159	
Reference:	D840.21	D840.21         Dissemination:         PU         Version:         3.0						

<sup>&</sup>lt;sup>75</sup> Such as Guerrieri, J. R., Francis, M. H., Wilson, P. F., Kos, T., Miller, L. E., Bryner, N. P., ... & Klein-Berndt, L. (2006, November). RFID-assisted indoor localization and communication for first responders. In 2006 First European Conference on Antennas and Propagation (pp. 1-6). IEEE.



collecting the data that you need for a particular purpose<sup>77</sup>) and also privacy principles (such as obtaining consent to the use of the data from the individuals from whom the data is collected) [88]. In a similar way, misuse of the exchanged data can happen if the exchange diffuses the information and makes it more difficult to control and regulate (i.e. if the exchange is not regulated by relevant rules and regulations). However, if implemented with care, the exchange of data can be an excellent opportunity for innovation in crisis management, because it may result in progress that could not otherwise have been achieved by individual actors, and based on this knowledge exchange, better and more specialized solutions can be more easily identified. In general, exchanging data is crucial for finding better solutions for international crisis management, as the crisis often transcends national borders. Research show that exchanging knowledge and data about the CM systems in other countries is central for developing national crisis management concepts further<sup>78</sup>, indicating that information exchange raises the knowledge levels and leads to a better sense of protection- both of the information and the crisis population.

• **Recommendation:** Minimizing the amount of data that is being exchanged will automatically minimize the risk of misuse of the data. Unnecessary data exchange should be avoided, and the risks and threats should be evaluated, to minimize the risk of function creep. The rules for data protection need to be carefully upheld in order to limit or prevent potential misuse of the information. Ensure that the receiving partner has a satisfactory level of protection for the exchanged data, and if in doubt, aim for complying with the legislation or regulation with the highest requirements.

#### Misuse-Protection, Transparency, Privacy & Data Protection, New Vulnerabilities-Progress:

Communication between crisis managers might have sensitive data as its content, for example in case of exchange of medical data of the individuals that are affected by the crisis. When data and information is exchanged between one partner, system or database, to another, the risk of misuse arises if the exchange is not well regulated, for example by legally and practically regulating the access to the databases (c.f. information security). Implications of such a breach in information security in the data exchange could be that sensitive data (such as data allowing for linking identifiable personal data to for example geo-locations from UAV's) can be obtained by someone who does not have permission to do so, which would be a breach of data protection legislation [88]. Lack of such procedures makes the data more prone to misuse (such as re-use, unlawful exchange or storage). Especially in the absence of legal frameworks, new vulnerabilities can be created by relying on communication tools that can be hacked for information about vulnerable infrastructure, distribution of resources in a supply chain, etc. In general, exchanging data often means merging databases with another actor, and this can both represent challenges and opportunities. As the

<sup>&</sup>lt;sup>78</sup> The concept of working together in international fora to solve also national challenges is not particularly controversial, and one example of such cooperation on European crisis management is described in Syrstad, R. S. (2014): Samarbeid om krisehåndtering i Europa. <u>https://www.regjeringen.no/no/aktuelt/samarbeid-om-krisehandtering-i-europa/id750968/</u>. Retrieved 10 November 2015.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	83 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>77</sup> For a suggested terminology for privacy by data minimization, see Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.



technical infrastructure and the complexity of the database increases once exchanged or merged, handling it correctly and properly becomes increasingly important. A breach of some kind could have more substantial impact as the consequences would reach out to more people (e.g. the individuals from whom the data is collected whose data is contained in the databases). However, there are many opportunities for positive impacts of data exchange<sup>79</sup>. For example, the exchange of information can reveal gaps and possibilities for improving the CM organization, and thus increase the general protection of society. If the data exchange is protected by data protection law, it more easily can respect especially the privacy of the individuals from whom the data is derived, for example if the process of exchanging data is transparent, and happens in a way that allows all involved actors or subjects to be made aware of what is happening to the data they are contributing with.

Recommendations: Ensure conformity with European data protection regulations when • implementing communication tools for communication between crisis managers (both ICT – and non-electronic based) and relevant national regulations. As policy maker you shall clearly set out safeguards to protect personal data, such as setting limits for what the communication technology will be used for, to minimize the risk of misuse. Access to databases must be limited both practically and legally. Solutions for encryption should be considered. This means that the very process and principle of exchanging information and data needs to be deemed the best solution for the issues at stake, a reflection which would include evaluating the applicability of the data exchange. For sustainable data sharing, especially on the European level, creating a constructive culture of data sharing can include, for example, developing financial and legal frameworks by working together with relevant partners and organizations. In addition to that, developing sustainable funding solutions for such initiatives is crucial [53]. Ensure that the data exchange process is open and transparent (as far as it is possible and reasonable), i.e. let the individuals from whom the data is collected know in advance to what extent their data will be exchanged and shared.

#### Suspicion-Trust, Transparency, Open- Control Society, Unease- Calmness:

If the process of data exchange does not adhere to the principles of transparency, it can create feelings of suspicion or unease, for example, among individuals being made aware that their data is being shared without a good reason or as per predefined agreements (c.f. [88]). This is especially important in a social and political climate that is increasingly concerned with issues of privacy [54]. If the communication solution used between crisis managers during a crisis happens in completely closed channels that are not easily investigated post-crisis (e.g. in order to examine the line of communication in case something went wrong), it can be seen as a trait of a so-called control society<sup>80</sup>. However, adhering to the fundamental principles regulating the exchange of data

<sup>&</sup>lt;sup>80</sup> The opposite of this would be the concept of the open society, which was originally brought forth by Henri Bergson. See for example Henri Bergson, Les Deux Sources de la morale et de la religion, Félix Alcan, 1937 [1932], pp. 287–343. Available at : <u>https://fr.wikisource.org/wiki/Les\_Deux\_Sources\_de\_la\_morale\_et\_de\_la\_religion/Chapitre\_IV.</u> The concept is now widely used in various academic disciplines, such as criminology, political science and sociology.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	84 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>79</sup> One system is for example suggested in: Flesher, Kevin, et al. "System for enabling collaboration and protecting sensitive data." U.S. Patent Application No. 10/459,394.



according to data protection law [88] creates a foundation for a constructive exchange of knowledge and information that can be highly beneficial to foster trust and a sense of calm in the respective populations. This can happen for example when lessons learnt from a crisis<sup>81</sup> are shared from one CM actor in one country to another, and this transfer of knowledge is used to better handle a similar crisis situation in another country. One example of such a lesson can be the way the CM actors communicate the crisis (or the risk of a crisis) to the population, and how this can have a significant effect on both the trust the population has in the relevant actor, and the way in which they feel calm and reassured in the situation.

• Recommendation: Make sure that the data exchange happens in a way that is as transparent as possible, in order to minimize feelings of suspicion and unease as to how the process is carried out and why it is necessary. Also, as a general principle, do not share more data than necessary to further reduce this risk. Take account of the fact that more people are aware of and sensitized towards privacy and data protection issues in light of recent global events such as the Snowden revelations [55] and the Right to be Forgotten- case [56]. Explore the opportunities for exchanging relevant knowledge and experience from actors in different contexts, sectors and countries, especially if you know that similar crisis situations have been previously tackled elsewhere and that the exchange could contribute in calming the situation. While ensuring the privacy of the individuals from whom the data is collected, as solution provider you should assure that the communication solution used by crisis managers is designed to support documentation so that it can be analysed and evaluated post- crisis. As part of an open society, transparency can enforce trust between the population and the crisis managers.

#### International Relations, Social Cohesion & Solidarity, Dignity, Non-discrimination:

Communication between crisis managers is often necessarily cross- border, as crisis (such as natural disasters) can easily happen across borders<sup>82</sup>. As is the core of the DRIVER project, this necessitates cooperation between crisis managers in several countries. If a cross-border measure or tool does not take international treaties and regulations (including, but not limited to data protection, such as [88]) into account, it can create large difficulties, not only for the implementation of the tool, but for the relationship between states. E.g. if international treaties or data protection regulations are overlooked when crisis managers are setting up communication systems, resulting in the system functioning differently in the different countries, this could even negatively influence solidarity and be seen as a discriminating practice by the system owner<sup>83</sup>.

• **Recommendation:** As CM solution provider you shall ensure that your solutions are in line with international treaties or regulations, in order to ease implementation and minimize

<sup>&</sup>lt;sup>83</sup> See for example Mahler, S. J. (2001). Transnational relationships: The struggle to communicate across borders. Identities Global Studies in Culture and Power, 7(4), 583-619, for a description of some struggels in such communication.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	85 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>81</sup> See for example: Farazmand, A. (2007). Learning from the Katrina crisis: A global and international perspective with implications for future crisis management. Public Administration Review, 67(s1), 149-159.

<sup>&</sup>lt;sup>82</sup> See for example Lai, A. Y. H. (2012). Towards a collaborative cross-border disaster management: A comparative analysis of voluntary organizations in Taiwan and Singapore. Journal of Comparative Policy Analysis: Research and Practice, 14(3), 217-233, for a comparison of the success of such collaboration across borders.



potential negative effects. Also when implementing a communication solution intended for international cooperation, it is important that the communication tool functions equally well in all the countries and takes into account, as much as possible and sensible, cultural and historical contexts in the relevant countries.

#### Suspicion-Trust, Integrity, Social Cohesion- Solidarity, Diversity, Cultural & Gender Sensitivity:

If a partner engaged in a process of data exchange does not adhere to the common principles of data protection [88], it can infringe upon the trust between the partner at stake and the other partner(s). This is a particularly sensitive risk also because it is commonly said that trust and a sense of integrity are easier to break down or destroy than to create. In addition, such a breach can have spill-over/ knock on effects onto other domains. Once the damage is done, and there has been a breach in trust, it can have several unfortunate consequences, and take time to rebuild- if ever<sup>84</sup>. Trust can also be influenced if the population or professionals feel that the data should not be exchanged with a certain partner for one reason or another (e.g. political reasons or if the topic is controversial). If the data exchange still happens, it could further negatively influence the feelings of solidarity in the community, as common principles, interests, objectives or standards are being questioned or overlooked. However, trust and integrity can also be strengthened in the context of data exchange, for example by demonstrating best practice, i.e. by making sure that it happens in a transparent and regulated manner [88]. In terms of solidarity, data- or information exchange with partners that do not share fundamental principles, interests, objectives or standards (for example that they have a substandard or inferior sensitivity in terms of cultural- and gender aspects), can negatively influence such principles. Nonetheless, the careful and considerate crafting of such an exchange process can have an effect in two ways. First, it can have a direct practical effect, e.g. by making available data that can contribute to solving a societal challenge related to solidarity or similar. Second, it can have an indirect effect, e.g. by signalling that the exchanging actors have included all social groups. Both effects can strengthen social cohesion and solidarity.

• **Recommendation:** Data exchange should happen only after a critical evaluation of the integrity of the receiver and after ensuring that the receiver upholds standard routines and regulations for processing the exchanged data. Be aware of this risk when exchanging data with third countries outside the Schengen- or EEA area. For CM professionals, avoid exchanging data with partners that fundamentally conflict with society's common principles, interests, objectives or standards. Ensure that the process happen in a transparent manner, in order to better overlook that the interests of the different partners are accounted for. Make sure the data being exchanged are representative of the cause, i.e. that it takes, for example, diversity, cultural and gender differences into account.

**Open- Control Society, Suitability, Necessity & Proportionality:** Relying heavily on data exchange to organize CM, can have negative impacts on the concept of the open society, i.e. if this exchange is

<sup>&</sup>lt;sup>84</sup> See for example Lyon, L., & Cameron, G. T. (2004). A Relational Approach Examining the Interplay of Prior Reputation and Immediate Response to a Crisis. Journal of public relations research.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	86 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



not executed well (for example if exchange of sensitive data is not encrypted or otherwise protected). Furthermore, this potential negative influence on the open society can be even stronger if the data exchange happens illegally, or through an opaque process, or if the data that is being exchanged is regarded as not suitable for the cause, or as particularly necessary or proportional to the cause<sup>85</sup>. However, information exchange is often necessary and bears with it also opportunities for improving the current conditions. In addition to filling the actual gap that the data exchange is the solution to, such exchange can also have the side effect that it establishes or enforces e.g. professional communities across borders or sectors, and creates networks of people that maybe otherwise wouldn't have met (e.g. via the coordination of volunteers). A positive societal side effect regulatory framework (i.e. for data protection, information security etc.), and that the overall conditions for doing data exchange and data processing at large, in fact can be improved.

Recommendation: Make sure that the data exchanging process happens according to relevant legal frames. Ensure that the data exchange is proportional to the case at stake, that it is suitable to solve the issue, and that it is necessary. The latter is important because the exchange can increase the risk of misuse [82] or function creep. Make sure that the exchange happens in a transparent manner. This includes making sure that all relevant data protection regulations and laws are being followed. Especially when exchanging personal data with other actors, clearly state the limitations of the data processing already before the data collected are subject to unjust control. If possible, seize opportunities to establish best-practice rules for data exchange in your company or organization, and investigate how your local Data Protection Authority can be of assistance in such a process. Consider building on networks that might emerge from the data exchange process. These can be beneficial in other areas of the crisis management operation as well.

## 3.3.4.1 Summary of recommendations: Fostering positive societal impact when working with solutions for communication between first responders

When working with solutions that are aimed at improving of facilitating communication between first responders, technology is an important factor to consider. For example, web-based communication may be of great added value for enabling interoperability between first responders, but it can also be advisable to ensure that sufficient non-electricity/non-high-tech based ways of communicating is available as backup systems, in order to minimize vulnerabilities. This should also be kept in mind when procuring for new solutions, in the sense that flexibility and openness of the system may be formulated as high level prerequisite. Data minimization (i.e. no unnecessary collection and storage of data) is a key principle, and will automatically minimize the risk of misuse of the data as well as function creep. In terms of legality and the regulations of the communication, the

<sup>&</sup>lt;sup>85</sup> One example of a set-up for exchange of data that was not considered as being proportional and suitable can be found in Størbu, M. K. (2015) EU- domstolen sier nei til datautveksling. <u>http://itavisen.no/2015/10/06/eu-domstolen-sier-nei-til-datautveksling/</u>. Retrieved 12 November 2015.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	87 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



rules for data protection (of both ICT- and non- electronic communication) need to be carefully upheld (on EU- and national level). This could e.g. mean to take precautions to ensure that the receiving partner has a satisfactory level of protection for the exchanged data. If in doubt; aim for complying with the legislation or regulation with the highest requirements. When implementing a communication solution intended for international cooperation, it is important that the communication tool functions equally well in all the countries and takes into account, as much as possible and sensible, cultural and historical contexts in the relevant countries. Explore the opportunities for exchanging relevant knowledge and experience from actors in different contexts, sectors and countries, especially if you know that similar crisis situations have been previously tackled elsewhere and that the exchange could contribute in calming the situation. With regards to security, access to databases must be limited, and solutions for encryption should be considered. This means that the very process and principle of exchanging information and data needs to be deemed the best solution for the issues at stake, a reflection which would include evaluating the applicability of the data exchange. Data exchange should happen only after a critical evaluation of the integrity of the receiver and after ensuring that the receiver upholds standard routines and regulations for processing the exchanged data. Be aware of this risk when exchanging data with third countries outside the Schengen- or EEA area. Consider building on networks that might emerge from the data exchange process. These can be beneficial in other areas of the crisis management operation as well.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	88 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



## 4 Assessments, examples, recommendations for functions concerning learning across borders

## 4.1 Competence- building for decision- makers and organizations

Related WP and Tasks: WP52, WP54, WP53, WP35, WP44

In CM, decisions usually have to be taken under circumstances of urgency<sup>86</sup>. A real merit thus lies in the preparation of decision-making and regulations for decision-making in CM need to be in place. Supporting decision-making during crisis management and developing competence in the field is a key activity within DRIVER. WP52 will develop a competence framework for crisis management that is applicable across the EU through the integration of different learning and competence approaches. Within WP54, models are being developed to enhance high level decision-making processes "Competence" is a highly dynamic concept and influenced by fast scientific, organizational and technological progress as well as socio-economic criteria and assumptions<sup>87</sup>. Logically, such a competence framework and related decision-making processes thus require constant updating in order to stay relevant, which might be especially true for crisis management. Since the relevant DRIVER tasks look at the overarching and harmonized CM frameworks, the assessments and recommendations below will focus on the way in which the modelling inherent in these solutions can cause secondary effects, both positive and negative, for society. Findings about impacts should be modelled into the frameworks.<sup>88</sup> Since the respective DRIVER work packages will develop high-level frameworks, the assessments will accordingly apply to the abstract level. An example of a potential societal challenge, has to do with the image of society that underlies decision-making and lessons learnt frameworks, and how these influences how such frameworks will produce effects on society. For example, if decision-makers base their decisions and lessons learnt on the fact that society is homogeneous, gender-, culture- and age-specific effects will not be taken into account and create long-term impacts of side-lining such specific needs and issues during crises<sup>89</sup>.

<sup>&</sup>lt;sup>89</sup> See for example Lustig, M. W., & Koester, J. (2003). Intercultural competence. Interpersonal communication across cultures.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	89 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>86</sup> This is a well-known fact, but is analysed in more detail here: Rosenthal, U., & Hart, P. T. (1991). Experts and decision makers in crisis situations. Science communication, 12(4), 350-372.

<sup>&</sup>lt;sup>87</sup> See for example: LaDuca, A., Engel, J. D., & Risley, M. E. (1977). Progress toward development of a general model for competence definition in health professions. Journal of allied health, 7(2), 149-156.

<sup>&</sup>lt;sup>88</sup> Two examples of this being done can be found in the ValueSec Project, where cost-benefit analysis of current and future security measures in Europe happens (http://www.valuesec.eu/) and also in the PACT project, *Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action* (<u>http://www.projectpact.eu/)</u>.



## Assessments

#### Unease – Calmness, Suspicion - Trust:

The process of identifying competences and gaps in competences (WP52) can be influenced by organizational or institutional agendas. Especially if competences and gaps are defined cross-border, organizations from low-income countries or smaller players might feel unease if they perceive that a culturally biased understanding of competence and competence gaps is imposed on them that, for example, benefit certain economic and employment interests of other countries or organizations<sup>90</sup>. Not listening to all players in such a process can thus cause an atmosphere of suspicion. A process of identifying existing competences and gaps in competences thus needs to be preceded by a thorough identification of relevant stakeholders or players before competence frameworks are designed. A democratic process of including both bigger and smaller players and reflecting on their positions, interests and stakes is thus a step to foster calm, trust and a progressive way of discussing competence-building.

 Recommendation: When putting a competence-development framework to use, ensure to identify all relevant stakeholders first. Reflect on their respective positions and stakes and ensure that everyone's position is taken account of when identifying and discussing competences, gaps in competences and new ways of building competences to foster a culture of trust.

#### Misuse - Protection:

Since many decision-making strategies translate different aspects of decisions into numeric values<sup>91</sup>, the outcome of the decision-making methodologies is dependent on the method chosen to convert real-world phenomena, dynamics or political priorities into such numeric values. Numeric values, however, may not be applicable to any kind of decision-making problem, or they may skew the process of decision-making, because they cannot accurately represent the factors influencing a decision. This also means that decision-making models, even if they are based on numeric assessments, can also be prone to misuse. If these priorities are not well-reflected, they can be misused for political agenda setting [57] [58]. If you design decision-making models that are based on numeric values, reflect about the best way to translate parameters into values and how these values may be open for manipulation in order to limit misuse and ensure the best possible outcome of decision-making models.

• **Recommendation:** When designing quantitative decision-making models, evaluate carefully which decision-making parameters can be translated into numeric values and how. Design decision-making models in which each parameter is clearly defined and its users will have a clear understanding of the results presented to them. Through that, you can control the

<sup>&</sup>lt;sup>90</sup> See for example Johnson, R. L., Saha, S., Arbelaez, J. J., Beach, M. C., & Cooper, L. A. (2004). Racial and ethnic differences in patient perceptions of bias and cultural competence in health care. Journal of general internal medicine, 19(2), 101-110. <sup>91</sup> This is for example the case in Bryson, N., & Mobolurin, A. (1997). An action learning evaluation procedure for multiple criteria decision making problems. European Journal of Operational Research, 96(2), 379-386.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	90 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



misuse of decision-making methodologies for unintended political or institutional agendasetting.

#### Sustainability:

Generally, one can say that it is possible to devise frameworks for very specific kinds of competences, which will ensure that a specific gap in competences is closed. This approach, however, could be weighed against frameworks that are broader, speaking to several kinds of competences and which are thus potentially more sustainable. In addition, it has to be taken into account that standards and legal regulation for specific situations may change rapidly on national and international level (e.g. because new technologies emerge that are not yet formally regulated). A sustainable framework then develops procedures that can be updated over the following years.

• **Recommendation:** The design of a decision-making methodology should clearly define the goal of the framework and then devise a method that addresses this goal concretely. Here, a broad framework may be more sustainable, but also less precise in its outcomes. When designing frameworks, ensure that it is possible to update the methodology over time and across different contexts.

#### Accountability:

Decision-making models do more than just identifying the best possible decision. They also produce a rationale for decision-makers according to which they choose to implement specific decisions [135]. As such, decision-making methodologies also assume and create accountabilities for those who take decisions. A rationale as to why a specific decision is taken is thus always inherent in the decision-making framework or methodology [135], but it is not always obvious to the decision-maker [59]. Reflecting upon these rationales and making them known to the decision-maker will also strengthen the sense of accountability that comes with taking decisions.

 Recommendation: Clarify where and how a decision-making methodology provides for rationales to take specific decisions. Make these rationales explicit and allow the decisionmaker to reflect about the effect that these decision-rationales have on their own accountability when taking such decisions.

#### **Transparency:**

if competence frameworks are hard to follow and understand, they become less actionable, which not only might hamper effectiveness<sup>92</sup>, but may also infringe negatively on the accountability (c.f. accountability) of those who take and implement decisions and opens up for covert agenda-setting<sup>93</sup>. In designing frameworks, acknowledge this complexity and try to reduce it by providing a clear

<sup>&</sup>lt;sup>93</sup> In a similar manner, difficult language or complex terminology, is a key element of improvement in the new EU General Data Protection Reform (article 12, 13, 14), where demands of understandability and simplification might contribute to reducing the potential for covert actions by the data controller.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	91 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>92</sup> For example in organization theory, "complexity theory" seeks to explain e.g. how complex adaptive system models represent a new way of simplifying the complex. See for example Anderson, P. (1999). Perspective: Complexity theory and organization science. Organization science, 10(3), 216-232.



definition of goals (i.e. the gaps to be closed), strategies and context descriptions that can influence competence-building and decision-making processes [60].

• **Recommendation:** Devise frameworks as transparent as possible so that they are actionable. Identify the concrete problems to be solved or gaps to be closed and reflect about the different context-factors that influence the respective decision-makers position. At best, decision-making frameworks document and make comprehensible any step of decision-making in order to make decision-making as transparent as possible. Make sure that political agenda-setting is not covertly integrated into decision-making processes by including methodologies that overtly address political agenda setting and priorities.

#### **International Relations:**

Especially if competence frameworks are harmonized across international borders<sup>94</sup>, they might potentially run the risk of being too general for the specific national situations. If a decision-making tool or methodology does, in turn, not take account of the international effects of the decision, it may produce risks for international collaboration and eventually infringe upon international treaty obligations<sup>95</sup>. Thus, planning with international dimensions of decision-making is always a balancing-act. If this is acknowledged and reflected in the design of the framework, international relations can in fact be fostered.

• **Recommendation:** Once you have defined for which concrete target group or problem the framework is supposed to be used, make sure all relevant partners are involved in devising or at least in reviewing competence-building models. Base competence building models on international consensus. Even if you develop national frameworks, reflect on potential international impacts. If you develop internationally relevant frameworks, ensure that the framework does not collide with each participant countries' specific legal, political, social and economic situation.

#### **Negative - Positive Standardization:**

International and high-level frameworks for decision-making can have the potential to create new standards (in the sense that the procedures are implemented as a formal standard, or a standard for certain domains or regions etc.), since they contribute to a normalization of the suggested decision-making process<sup>96</sup>. As such, the developers of that framework carry a certain responsibility to ensure that the suggested competence frameworks can in fact be followed by every country (i.e. adhering to

 <sup>&</sup>lt;sup>96</sup> For the crisis recovery phase, establishing criteria for decision making and standardization of requirements with regards to soil clean-up is one example of seeking to normalize a procedure. See for example: Moen, J. E. T., Cornet, J. P., & Evers, C. W. A. (1986). Soil protection and remedial actions: criteria for decision making and standardization of requirements. In Contaminated soil (pp. 441-448). Springer Netherlands.

Document name:	D840.21 – A guid functions – Versio	e assessing unintende on 1	d societal im	pacts of diff	erent CM	Page:	92 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>94</sup> This might be referred to as a "politics of harmonization". See for example Simmons, B. A. (2001). The international politics of harmonization: the case of capital market regulation. International Organization, 55(03), 589-620.

<sup>&</sup>lt;sup>95</sup> For an example of a framework for crisis management based on both regional and global disasters, and the different stakeholders involved, see Pearson, C. M., & Mitroff, I. I. (1993). From crisis prone to crisis prepared: A framework for crisis management. The academy of management executive, 7(1), 48-59.



relevant legal requirements) and that they take account of relevant context-factors for each country in order to assure positive over negative standardization<sup>97</sup>.

• **Recommendation:** Take into account how a new framework also creates new standards in decision-making. Can these standards be fulfilled by every participating country? Are they actionable and effective standards for every country? What are the accountabilities that the framework requires? While reflecting on answers to such questions already at the design-stage of competence and decision-making frameworks, you can ensure a positive new standard has the chance to materialize.

#### Diversity, Cultural & Gender Sensitivity, Non-Discrimination:

The degree of attention generally given to public participation in the policy process, highlights the importance of looking at how such processes may and will have an effect on both the relevant policy and the people who participate in the process [136: iii]. Similarly, the participation of relevant societal groups (as applicable), in the process of designing competence frameworks, can influence the final outcome, e.g. if they do not represent and reflect upon the different societal needs. This may potentially cause detrimental or discriminatory effects for the neglected groups. This concern, for example, cultural and gender- bias or related insensitivities in decision-making<sup>98</sup>. Decision-making based on biased parameters may then evoke distrust from the population vis-à-vis decision-makers (c.f. trust). An inclusive development of decision-making frameworks with the relevant stakeholders consulted and respective societal needs reflected can foster diversity, non-discrimination as well as cultural- and gender-sensitive crisis management that address society at large.

• **Recommendation:** Fair, proportional and non-discriminatory crisis management starts at the decision-makers level. When designing decision-making frameworks for crisis management, take local contexts into account. Geography, ethnicity, socio-economic indicators, age, gender and culture are important influence factors in identifying the best possible decisions in CM and to make them acceptable across society. These factors already play a role at high-level decision-making, which is why decision-making frameworks should include respective representatives of each group. This participation can help taking account of diversity and gender-, age- and culture-sensitive competences and solutions needed in European crisis management.

#### **Open- Control Society:**

<sup>&</sup>lt;sup>98</sup> For a discussion on the experiences of women and people of colour in decicion making process requiring all group memebers participation, see for example: Elsass, P. M., & Graves, L. M. (1997). Demographic diversity in decision-making groups: The experiences of women and people of color. Academy of Management Review, 22(4), 946-973.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	93 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>97</sup> Such context relevant factors could for example be the implementation of the concept/ framework in less developed countries. E.g. Lundvall et. al. present a theoretical deepening of a fairly narrow version of the concept "national systems of innovation", and in the movement toward the broader approach, in order to adapt the concept for the analysis of poor countries. See: Lundvall, B. Å., Johnson, B., Andersen, E. S., & Dalum, B. (2002). National systems of production, innovation and competence building. Research policy, 31(2), 213-231.



Technology plays an important role in decision-making frameworks, such as data processing capabilities<sup>99</sup>, but also, the frameworks might ask which kind of technology should be implemented to address a specific problem in crisis management. With the increased focus on technology in decision making<sup>100</sup>, such frameworks might not always take non-technological solutions into consideration, although a wide range of reliable qualitative tools<sup>101</sup> for decision making are known<sup>102</sup>. Thus, the design of decision-making frameworks can influence the level of technology dependency (c.f. technology dependency), surveillance and control within a society – even if not intended<sup>103</sup>. It is already at the level of designing decision-making frameworks that such influences can be steered. Utilizing frameworks to remind decision-makers about non-technological alternatives and the ways in which specific solutions foster open societies is thus a great opportunity to create a positive longterm impact.

**Recommendation:** Utilize the full potential of the frameworks you design for decisionmakers, for example by reminding them about the possibility not only to assess and take account of technological or other standard solutions, but a broad range of crisis management solutions.

#### 4.1.1.1 Summary of recommendations: Fostering positive societal impact when working with competencebuilding for decision- makers and organizations

When working with solutions for competence- building for decision- makers and organizations, the design of the plans and the methodology is important. For example, the respective stakeholder's positions should be reflected upon, and taken into account when identifying and discussing competences, gaps in competences and new ways of building competences to foster a culture of trust. The design of a methodology should also clearly define the goal of the framework and then devise a method that addresses this goal concretely. Here, a broad framework may be more sustainable, but also less precise in its outcomes. When designing frameworks, ensure that it is possible to update the methodology over time and across different contexts. When designing quantitative decision-making models, evaluate carefully which decision-making parameters can be translated into numeric values and how, and in general: clarify where and how a decision-making methodology provides for rationales to take specific decisions. Make these rationales explicit and allow the decision-maker to reflect about the effect that these decision-rationales have on their own accountability when taking such decisions. (Local) context-factors that might influence the decisionsmaker should be taken into account as well. Devise frameworks as transparent as possible so that they are actionable. Identify the concrete problems to be solved or gaps to be closed and reflect about the different context-factors that influence the respective decision-makers position. Make sure that political agenda-setting is not covertly integrated into decision-making processes by including

making<sup>103</sup> As for example can be found in the outputs of the DESSI Project (http://securitydecisions.org/about-dessi/).

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	94 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final

<sup>&</sup>lt;sup>99</sup> See for example: <u>http://www.useoftechnology.com/role-technology-decision-making/</u> <sup>100</sup> ibid

<sup>&</sup>lt;sup>101</sup> For example "Six thinking hats", as described in: de Bono, Edward, 1999, *Six Thinking Hats*. Little, Brown and Company.

<sup>&</sup>lt;sup>102</sup> Some are listed in this article. Available at: <u>http://www.43folders.com/2005/09/01/eight-tools-for-streamlined-decision-</u>



methodologies that overtly address political agenda setting and priorities. With regards to innovation, take into account how a new framework also creates new standards in decision-making. Such new standards should be careful to foster fair, proportional and non-discriminatory crisis management. Similarly, geography, ethnicity, socio-economic indicators, age, gender and culture are important influence factors in identifying the best possible decisions in CM and to make them acceptable across society. These factors already play a role at high-level decision-making, which is why decision-making frameworks should include respective representatives of each group.

Document name:	D840.21 – A guid functions – Versic	e assessing unintende on 1	d societal im	pacts of diffe	erent CM	Page:	95 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



## 5 Overview of relevant Criteria per Function

	SEC	ON	DARY	IN/ SE	CURITI	ES		POL	POLITICAL & ADMINISTRATIVE PRINCIPLES				ICIPLES	S LEGITIMACY CORE SOCIETAL & ETHICAL PRINCIPLES LE				LEGAL VALUES FUNDAMENTAL RIGHTS									
Subcategory	Unease - Calmness	Suspicion - Trust	Misuse - Protection	New Vulnerabilities - Progress	Technology Dependency - Flexible Solutions	Function Creep - Specialized and Controlled Use	Sustainability	Accountability	Transparency	Integrity	Negative - Positive Standardization	International Relations	International Cooperation	State- Citizenship- Relationship	Political Reputation	Social Cohesion & Solidarity	Participation	Diversity	Open-Control Society	Cultural & Gender Sensitivity	Suitability, Necessity & Proportionality	In/justice & In/equality	Dignity & Autonomy	Non-Discrimination	Privacy & Data Protection	Freedoms & Protest	Measures as of WP/Tasks
												Funct	ions cor	nceri	ning Civil S	ociety Re	esilien	ce									
													Catego	ry: Co	ommunity E	ngagemei	nt										
Training Communities for Psychosocial Support		×	x													x	x	x		x		x		x	x		
Building & Measuring Community Resilience	x	x	x						×														x	x	x		
Volunteer Management (Incl. Crowd Tasking)	x	x	×				×							×		×	x	x		x					x		
	-			1	1								Categ	ory: (	Crisis Comm	unication		1	1		1		1	1			
From Crisis Managers to Citizens (public)	×	×	x						×						х		×	×	×	×			x		×		
Low-level: Media & Policy communication	×	×												x	×	x	×	×		×					x		
From the Citizens to Crisis Managers			x	x					×	×								x	×		x		x	×	x		

Document name:	D840.21 – A guide asses	sing unintended societal impac	cts of different CN	1 functions – Versi	on 1	Page:	96 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



												Functio	ons conc	erni	ng Strengt	hened Re	espon	ders									
													Category	: Ide	ntification &	& Awaren	ess										
Gap analysis for community resilience	x		x	x				x	x			x		x			x	x		x		x			x		
Situational Analysis & Impact Assessment	x	x	x	x	x	x			x		x			x		x	x		x	x	x			x	x	x	
Early warning, Risk Analysis, Forecasting	x	x		x			x	x	x			x		x	x	x	x			х		x		x			
Identification of Critical Infrastructures	x	x	x	x	х			x	x			x			x			x		х	х		x	x	x		
												Categ	ory: CM	Coor	dination, Co	mmand 8	Conti	ol					-	-			
Tasking and resource management	x	x	x		х			x	x			х			x					х			х	х			
					L						:		0	ateg	orv: CM Log	istics					i				:		
Strategic Transportation & Supply Chains													Catagori														
	1	1 1		· · · · ·		r		1		-			Categor	y: Inf	ormation iv	lanageme	nt				1	-			1		
Collection & Storage of data	x	x	x	x	х	x			x	x	x			x	x	x	x	x	x	x	х	x	x		x	x	
Low- level: Crowd Sourcing																											
Facilitating Data Processing (Incl.		x	x	x	х	×		x	x	x	x				x	x									x		
Analysis & Evaluation	x	x	x			x		x		x		x			x				х		x				x		
Communicatio n between First Responders	x	x	x	x	(X)	x			x	x		x	x			x		x	х	х	x		x	x	x		

Document name:	D840.21 – A guide asses	sing unintended societal impac	cts of different CN	1 functions – Versi	on 1	Page:	97 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



												Funct	ions con	cern	ing Learniı	ng Across	Bord	ers						
	Category: Competence- Building for Decision- Makers and Organizations																							
Competence-																								
<b>Building for</b>																								
Decision-	х	х	х				х	х	х		х	х						х	х	х		х		
Makers and																								
Organizations																								

Figure 2: SIA Framework

Document name:	D840.21 – A guide asses	sing unintended societal impac	cts of different CM	1 functions – Versi	on 1	Page:	98 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



## 6 Overview of all recommendations

Below is the full catalogue of all the assessments, grouped per function.

## 6.1 Recommendations for community engagement

#### 6.1.1 Training Communities for Psychosocial Support

- **Recommendation:** When engaging with communities as a trainer you should ensure that all participants can speak or contribute in an equal way, promoting a climate of openness. Also think of power relations between members of the community which may not be visible and hinder certain members to speak freely. Also reflect about the power imbalance between trainer (CM professional) and trainee (lay public). Thus, foresee both a joint discussion and anonymous written feedback mechanism so that people are able to articulate their views.
- Recommendation: When designing training curriculums and selecting participants, ensure that socio-cultural diversity is taken into account. The curriculum and the profile of trainees has to also be as inclusive as possible, especially since members of specific groups, such as migrant communities and social minorities, are often underrepresented within CM professionals and volunteers. Because of increased diversity in the population [64], trainers have to be able to deliver training activities to various societal target groups and take into account their different cultures.
- Recommendation: As CM organisation providing PSS (psychosocial support training) training, select PSS-Trainers carefully to guarantee that confrontation techniques and methods of selfawareness are applied rightly and that trainers do not overestimate their skills. Also, think about regular external evaluation of your trainers. Having a qualified psychologist in the host organisation overseeing the development of PSS training programmes and monitoring their application can assure the proper application of the former points.
- **Recommendation**: Ensure conformity with European data protection legislation and rights and cultural customs related to privacy. Also when collecting and processing private data at trainings, the informed consent of participants is mandatory.
- **Recommendation:** Training curriculums should also pay special attention to how to establish a sphere of trust among trainers and trainees and include adequate evaluation and feedback mechanisms.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	99 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



### 6.1.2 Building & Measuring Community Resilience

- **Recommendation:** Explain in easy terms what you are doing and what is the expected added value for the participant. An added value at the individual level may promote further motivation.
- Recommendation: Solution developers shall be careful with sharing a quantitative visualisation of the resilience assessment. Such graphical representations might be appropriate for decision makers to get a quick overview, making them available to the public might trigger stigmatisation, which is especially problematic, when the assessments rely on very small samples.

### 6.1.3 Volunteer Management (Incl. Crowd Tasking)

- **Recommendations:** Operators should ensure and actively communicate that security measures were taken and that the users data is safe and only used in case of crisis to facilitate rescue missions. It will help building up a trust relationship with the population. When designing registration procedures ensure that privacy relevant information is represented in a transparent, understandable and user friendly way.
- **Recommendation:** In order to not create suspicion regarding the effort from the population or to misuse volunteers for other tasks than originally indented, a four-eye principle<sup>104</sup> should be put into place, ideally separating the level that a) requests b) alerts and deploys the volunteers and c) the level which gives clearance to the deployment.
- Recommendation: Before officially launching unaffiliated volunteer management programs, potential host organisations shall commission an independent survey to find out whether it would be accepted as host organisation by the envisioned target groups. In any case it might be advisable to partner with civil society organisations used to work in community engagement and use trusted and appropriate communication channels for reaching out to the target groups.
- **Recommendation**: Crisis Managers responsible for applying organisation and mobilisation concepts shall see the willingness to help as chance to foster social cohesion and shall provide the organisational (e.g. safe procedures) and legal framework (e.g. insurance coverage for time on mission) for individual spontaneous volunteers as well as for grassroots initiatives to assist.
- **Recommendation**: When selecting the target group for the organisation and mobilisation concept, operators shall not only think in "hard" operational efficiency parameters easy to be benchmarked (e.g. time to shovel 100 sandbags) but also "soft" parameters such as interpersonal skills relevant for cultural mediation.

<sup>&</sup>lt;sup>104</sup> This principle is described as following by United Nations Industrial Development Organisation: « The four-eyes principle means that a certain activity, i.e. a decision, transaction, etc., must be approved by at least two people. This controlling mechanism is used to facilitate delegation of authority and increase transparency ». Available at: <a href="http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html">http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html</a>

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	100 of 159
Reference:	D840.21	3.0	Status:	Final			



• **Recommendations**: Even if the willingness to help is temporarily restricted to the aftermath of a disaster, where it is needed most, people who spontaneously volunteered once may want to help again. Thus CM organisations can establish pools of "potential" spontaneous volunteers. This function works best when pre-registering and asking them what kind of contributions they could imagine making. When establishing structures for managing spontaneous volunteers don't mix up these activities with your recruitment activities for regular CM volunteers. Better see spontaneous volunteers as additional flexible "time donation". If you proactively try to persuade them to become regular volunteers this can lead to unease on side of the volunteers.

## 6.2 Recommendations for crisis communication

### 6.2.1 From Crisis Managers to Citizens (public)

- **Recommendation:** As solution developer, ensure that your tools function in a way which creates a trustful relationship between the crisis managers and the crisis population, if not this can seriously reduce the applicability of the tool and even create suspicion and unease in the population. Decision makers and crisis communicators shall not communicate false information or provide "quick fixes" to challenging questions that may arise from the public during a crisis, even if it might seem what the public wants to hear.
- **Recommendation:** In cases, where openness of the communication process cannot be put into practice because, e.g., it affects other core values such as data protection, crisis communicators shall make sure to explain the need and benefit of such tools, helping the public to decide whether they want to use this tool.
- Recommendation: Technical solution providers for communication tools from CM to population shall ensure that the amount of information that is shared is scalable but very clear and understandable so the population doesn't have the feeling of lacking information about the "bigger picture" or that some population groups are locked out of the communication process. The means – the how to communicate - differs and may be the key to a better-prepared community, which is to be evolved together between disaster management professionals and media experts.
- **Recommendation:** When using web- or app based solutions for informing the public and organizing and mobilizing their willingness to help- CM operators shall take measures to guarantee the legality and conformity of the communication tools with national and European data protection regulations.
- **Recommendation**: Strive for the highest ethical standards when communicating with the public during or after a crisis. Any damage to the political reputation of the CM organization can be hard to restore.
- **Recommendation**: Ensure that the communication to the public takes account of cultural and gender differences, and that e.g. crucial messages are given in the most relevant languages. Take account of all societal groups when communicating.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	101 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- **Recommendation:** When communicating, decision makers should adhere to the principles of openness and honesty, in order to stimulate trust in the population and not represent a breach of solidarity. Strive for a transparent and open communication process, and if information needs to be withheld from the public, clearly state so. Ensure that all the volunteers are fully informed of what kind of activity they are signing up for. Crisis managers should inform well about the crisis situation, in order for volunteers to decide if they want to participate in the activity.
- **Recommendations:** It is important that official warning messages include recommended protective actions when the disaster strikes and raises the awareness and preparedness of the population before the occurrence of disasters. Media trainings should therefore prepare the sender of the message to frame the messages in an appropriate way to reach various target groups within the population, triggering the most appropriate proactive actions while avoiding panic and unease on the side of the population.
- **Recommendation:** Highlighting and valuing the effort by the respective local community during a crisis in the media can help support and build solidarity and encourage participation in the community. This can also have positive spill-over effects to other communities, and strengthen bonds between members of the society.
- Recommendation: Joint trainings between responsible crisis communicators and media stakeholders contribute to the openness and transparency of the communication process and a better mutual understanding. Ensure that functioning cross-organizational and crossborder coordination mechanisms are in place in order to avoid non-harmonized or even conflicting messages through different channels or in different countries.
- Recommendation: Unless there are good reasons for it, withholding information from the media should be avoided – the best strategy for disaster managers is generally communicating and acting truthfully to avoid sending mixed messages. In a cross-sectoral or cross-border crisis, a coordinated media communication strategy is important to avoid mixed messages, confusion and erosion of trust.
- **Recommendation:** Make sure that the messages that are being sent through the media or in policy related communication, take into account and respect the full diversity of the society, e.g. cultural groups and gender differences. Enable communicators to select media channels and frame messages considering socio-cultural factors such as language, language proficiency, gender, nationality, ethnicity, class, age and/or physical limitations.
- Recommendation: Respect the sources of information during a crisis as these could be particularly vulnerable, and follow the relevant data protection legislation when it comes to collecting or sharing personal data. Always ensure conformity with European data protection legislation and rights.

### 6.2.2 From the Citizens to Crisis Managers

• **Recommendation:** Limit the amount of data that is being collected. Apply the principle of data-minimization to collect only necessary and suitable information- of a proportional size.

Document name:	D840.21 – A gui functions – Vers	ide assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	102 of 159
Reference:	D840.21	3.0	Status:	Final			



- **Recommendation**: When collecting personal data from the public, it is very important that the privacy of the individuals from whom the data is collected is being respected. And that safeguards (some sort of censorship or screening) are taken to prevent pictures being posted which are violating in one way or the other.
- **Recommendation:** Make sure that data is used only for the intended purpose to stimulate trust in the population.
- **Recommendation:** In order to respect the integrity of the public, ensure that privacy and data protection is a foundation when developing/ deploying a communication solution between the public and the crisis managers.
- **Recommendation:** Encourage different societal groups to make use of the communication tool, or consider alternative measures to ensure diverse input from the public.
- **Recommendation:** While protecting the privacy of the individuals, consider including a mechanism for quality assuring the reliability of the information that is gathered from the public.
- **Recommendation:** Be careful not to base the deployment of resources entirely on selfreported information from the field, but rather use it as a supplement to more traditional crisis management information channels such as information form first responders or volunteers.

## 6.3 Recommendations for Identification & Awareness

### 6.3.1 Gap Analysis for community resilience

- **Recommendation**: From the various gaps you will reveal, identify and rank the *key gaps* to be covered in order to avoid over-engineering CM and creating unease. For any key gap, provide for a strategy to close such gaps with a clear assignment of responsibilities, as well as definitions and delimitations of related tasks. If you share knowledge about gaps publicly ensure that for any gap a related strategy to close this gap is communicated in a transparent manner.
- **Recommendation**: Design gap analysis methodologies that rely on comprehensible and transparent parameters to ensure that they are reproducible. When putting gap analysis methodologies to use, ensure to have mechanisms in place that identify potentially hidden political or commercial agendas. For example, define a set of indicators that determine political and commercial influence on gap analysis to ensure protection against the misuse of gap analysis methods or a focus on irrelevant gaps. When conducting the analysis, use a broad variety of data sources to avoid producing skewed results. Ensure to repeat gap analyses regularly in order to take account of changes and assist in creating sustainable solutions. Include mechanisms to challenge each step in the gap analysis to check whether it speaks to the overall goal.
- **Recommendation**: Communicate about gaps carefully as they also point to a vulnerability that can be exploited. Ideally, identify a strategy for closing gaps at the same time and

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	103 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



communicate that strategy together with the identified gap in order to present the gap analysis as a value-added and progress for CM in general.

- **Recommendation:** Before conducting a gap analysis, agree upon responsibilities and their limits, in order to regulate accountabilities for the identification of gaps and for potential misidentifications.
- **Recommendation**: Conduct gap analyses only at cross-border level if goals, instruments and methodologies have been synchronized before and both parties agree to the analysis. If international cooperation for gap analysis is needed due to specific cross-border scenarios, ensure to coordinate with the relevant partners beforehand, potentially during exercises. Create common standards, variables and methodologies for gap analyses.
- **Recommendation:** Ensure that any analysis of gaps includes reflections about the importance of these gaps and their potential for unnecessary control-efforts. If possible, ensure that areas, variables and goals for gap analysis are made transparent, and invite the opinion of those who will be subjected to the gap analysis effort in order to foster a positive state-citizen-relationship and an open society.
- **Recommendation:** Make sure the team defining parameters for gap identification is diverse. This does not only refer to the inclusion of analysts with a cultural and gender-sensitive perspective, but also relates to any kind of professional diversity needed for a thorough gap analysis. Time permitting, run a pre-analysis identifying those players and representatives who know best about gaps in a specific area. Include them into the identification of gaps. Define the parameters of gaps under the participation of those groups for which the analysis' theme will be most relevant.
- **Recommendation:** Comply with data protection regulations when identifying gaps, including international regulations (if applicable). Ensure that those public and private players who may be concerned by the gap analysis are involved in the process, and that they agree to share relevant data or allow for gap analyses concerning their domain.
- Recommendation: If gap analyses concern society as a whole, spend some time mapping the different societal groups and ensure to take account of all parts of population to avoid unequal solutions. If possible, include experts from various backgrounds with a broad variety of perspectives into the design of gap analyses.

#### 6.3.2 Situational Analysis & Impact Assessment

• **Recommendation:** Make sure to clearly define the scope of the data that is supposed to be collected via airborne sensors, social media or apps. Clearly mark these methods and tools as something that belongs to the crisis management context, for example by marking UAVs with the logo of the organization that uses them. If possible, always contextualize the use of airborne sensors through brochures and information campaigns before usage. Organize information campaigns in advance about the why and how of data collection (e.g. how it will be used) and collect informed consent of populations wherever possible.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	104 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- Recommendation: Clarify the kind of data to be collected for situational analysis long before related tools are being put to use. Describe the limits of the data that you collect. Devise a clear code of conduct for how this data is being used and protected from misuse. Dedicate resources to the identification of deceptive information. Share the code of conduct and all protective measures with the people whose data you are likely to collect. If you collect data for situational analysis via apps and mobile phones, devise a clear and easy-to-understand consent form that people will read before they provide data. Avoid implementing such consent forms directly on the phone because people give easily consent on the phone without reading the terms of conditions. If you do implement consent forms to be signed directly on the phone, provide for a step-by-step consent form rather than a very condensed text. Communicate the added value of crowd-tasking and clarify where the responsibilities to collect information lie.
- **Recommendation:** If you foresee the usage of social media and apps for reporting, avoid asking for information that may lead to the identification of the sharing person. Protect the networks and platforms that collect and aggregate information for situational analysis according to highest standards. Devise clear guidelines for sharing information about bottlenecks and vulnerabilities, and limit the amount of people who have access to aggregated information and results to those parties which are strictly necessary.
- **Recommendation:** Make sure that alternative methods for situational assessment are in place to avoid technology dependency. Ensure that such methods can replace other functions in case particular information channels fall out and to limit the overall dependency on technology in society as a whole.
- Recommendation: Since many solutions open up for additional usages that are different from the original purpose, identify which of the different future usages of the developed solutions are desirable and which not in order to avoid function creep. Provide for concrete guidelines and technical specifications that limit undesirable use. Such a plan will in fact foster a positive form of controlled "re-"use of situational analysis technologies beyond their original purpose and thus create new opportunities for CM.
- **Recommendation**: Crowd-task information for situational analysis only from volunteering parties, who have given their consent ahead of the operation.
- Recommendation: When developing a crowd-tasking mechanism, include not only an informed consent form, but in the best case scenario also a code of conduct. This should outline the ethical principles relevant, when sharing information about situations and fellow citizens, in order to inspire a culture of care and solidarity and avoid negative effects on social cohesion.
- **Recommendation**: Ensure that crowd-tasking does not make crisis populations feel pressured to share information, but rather invites them to participate in crisis management. Provide for different communication channels for crowd-tasking to ensure the broadest possible participation in society across culture, age and gender.
- **Recommendation:** Take into account whether other means and tools exist to collect information in a manner more suitable and proportional to the problem. Run regular

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	105 of 159
Reference:	D840.21	3.0	Status:	Final			



suitability assessments in exercises and after technology has been put to use during emergency situations.

- **Recommendation:** Avoid sensors for situational analysis that can identify cultural, ethnic or gender features. If they do, ensure that these are not fed into the analysis, unless strictly necessary, e.g. for the identification of missing persons. Limit the storage of data collected by UAVs in order to avoid additional usage that can discriminate against specific societal groups.
- **Recommendation:** Collect consent from people sharing information for situational analysis. If you utilize UAVs, choose sensors that avoid the unnecessary collection of personal data. Ensure that effective ways for analysing big data are in place, which do not infringe upon the data provider's privacy or produce skewed results.
- **Recommendation:** Communicate through information campaigns which kind of data is collected by UAVs, as well as when, where and how UAVs are being put to use. Brand the actual technologies with a clearly recognizable sign that signals the UAV's purpose.

#### 6.3.3 Early Warning, Risk Analysis & Forecasting

- **Recommendation:** Contemplate the secondary effects that a public warning may generate, be as clear as you can in formulating the message. Include concrete advice for professionals, volunteers and citizens to avoid confusion or panic. Carefully plan the language of a risk communication. Give concrete advice for the situation so that people can react in line to the communicated risk.
- **Recommendation:** Avoid generalizations vis-à-vis specific societal groups to lower the general level of suspicion that such assessments can cause. Have a clear policy on which risk assessments are supposed to be public. Before you communicate risk assessments or early warnings, reflect about the potential consequences that society can draw from such assessments. Give concrete advice in an easy language.
- **Recommendation**: Plan the wording of warnings carefully since they also point to a vulnerability that can be exploited. Ideally, identify a strategy for addressing the risk to be communicated and communicate that strategy together with the warning/risk in order to provide for maximum progress of your solutions.
- **Recommendation:** Only send warnings when clear indicators for an imminent crisis exist. Even if the threshold for these indicators is low - to be on the safe side – ensure that the affected populations and recipients of the warning understand these indicators and take them seriously. Once you issue a warning, send as much context information as possible so that receivers of such warnings know how to react and take the warning seriously. Give concrete advice on how to react. Through that you ensure the sustainability of such systems.
- Recommendation: Clarify the responsibilities and accountabilities concerning both the risk
  assessment procedure, the issuing of warnings and the actual response strategies before
  making any related public announcement. Identify who is responsible for which part of the
  process. Clarify lines of communication. If you work with collective models of responsibility,
  ensure that they can be implemented fairly.

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1						106 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- **Recommendation:** Communication strategies on risks and early warnings should be honest and transparent. They should include the most feasible extent of information about what is known and what is not known about the future. Risk analyses should furthermore include explanatory information about the solutions: why are specific solutions best suited to address a specific risk? Methodologies for conducting risk analysis and related communication standards need to be developed in a transparent manner, identifying the context information that is necessary for a recipient to know in order to react.
- **Recommendation:** Ensure that all international institutions that could have an interest in the spread of threats are properly and timely informed. For each kind of risk, develop a mutual understanding of territorial and task-related responsibilities per institution and establish communication rules for times of crises.
- **Recommendation:** When devising new solutions for risk and early warning systems include reflections about choosing and defining specific risks over others. Ensure that warnings are formulated for the specific recipient and if that recipient is the general public, ensure that they are factual, easy-to-understand and not exaggerated or understated.
- **Recommendation:** If possible, make a thorough screening of all societal groups to ensure that risk assessment solutions take account of diverse risk perceptions and needs across society. Plan risk communication and early warnings while taking all potential audiences, their risk perceptions and the specific risks that they face into consideration. Organize communication and media strategies that allow for specific risk communication and early warnings for different groups. Reflect whether the formulation of the alert can have any negative impact on a particular group, area or activity.

### 6.3.4 Identification of Critical Infrastructure

- **Recommendations**: Choose resilience indicators and measures for contingency plans that strengthen resilience without causing too many follow-up measures. Reflect on the influence that commercial or political actors may have on the selection of resilience indicators.
- **Recommendation:** Consider if the identification of vulnerabilities should be made public, or if this in fact will add to vulnerability. Capitalize on the progress in the CM field, by filling in potential gaps that can raise the level of resilience in the city. Reduce complexity of contingency plans wherever possible.
- **Recommendation:** Consider analogue supplements to technological solutions to enhancing resilience in the city in order to avoid technology dependency of new solutions.
- **Recommendation:** Make a screening of all relevant actors to CM. Ensure that the partners that are responsible for core infrastructures in the city are part of the process of identifying resilience indicators. Carrying this out as a democratic and inclusive process will create an ownership that can be beneficial also in the long run.
- **Recommendation:** It should be verified whether, how and to what extent certain identified partners can actually be held responsible for contingency plans and backup solutions.

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1						107 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



Practicing the execution of the resilience logistics that are needed in a crisis, can enforce its effect and also strengthen the accountability of the organization.

- **Recommendation:** Review your contingency plans to check whether all solutions are culturally, age- and gender-sensitive.
- **Recommendation:** Devise transparent contingency plans that state responsibilities and first response actions clearly. Issue reports on actions taken, and log potential gaps or inconsistencies revealed during or after the crisis.
- **Recommendation:** Reflect upon and steer the influence of political agendas on contingency planning, keeping in mind the basic needs and principles that exist in society (almost) regardless of political or commercial influence. The selection of resilience indicators should reflect whether they are prone to political or commercial misuse.
- **Recommendation:** When designing a contingency plan, verify which core infrastructures are connected to international infrastructures and ensure the inclusion of necessary international partners and respective regulatory issues.
- **Recommendation:** Ensure indicators for contingency planning are suitable, necessary and proportional to the contingency plan's aim to avoid unnecessary negative secondary effects.
- **Recommendation:** Information about the vulnerability and resilience of logistical domains and infrastructure can be confidential. Those who assess key functions, vulnerabilities and indicators need to ensure that they do not infringe upon legality and only obtain information about (potentially private) infrastructures and processes with consent. Keep a clear overview of the relevant approvals and requirements to ensure compliance with relevant data protection regulations, in order to protect privacy in case there is personal data involved. For secret of confidential data, particular rules may apply, and the local Data Protection Authority should be consulted.

## 6.4 Recommendations for CM Coordination, Command & Control

#### 6.4.1 Tasking and resource management

- **Recommendation:** Make sure that the distribution of human and financial costs and resources are fairly distributed, especially when planning or developing solutions for resource management or contingency efforts with low-income countries. If the distribution of resources and/or preparation of contingency plans involve (personal) data collection, these data have to be protected according to relevant national legislation. Inform the public accordingly when contingency plans or similar are tested through CM exercises, and disseminate the achievements and lessons learnt from them.
- **Recommendation:** To avoid misuse a certain level of transparency with regards to how the resources are distributed and spent is required. Ensure that the material resources distributed take care of and respect the different needs of men, women and children, for example in terms of food (with regards to religious and other dietary needs) and hygiene articles.

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					Page:	108 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final


- **Recommendation:** Avoid complete dependency on a certain technological solution, e.g. for coordinating the distribution of resources during a crisis. Make sure that the contingency plan takes account for the fact that certain technologies can fall out, and that there are alternative ways of e.g. informing both the population and the crisis managers in case of such an occurrence.
- **Recommendation:** In order to be prepared and accountable in case of a crisis, make sure that appropriate contingency plans have been prepared and communicated. Regularly test and exercise with the plans, using the whole crisis management organization, and if relevant and possible, communicate the results of them both internally and externally, always paying attention not to create unease, but to foster the people's trust in crisis managers.
- **Recommendation:** Tools and measures to improve the distribution of resources and to manage the supply chain (whether human, material or financial) need to adhere to both national and international legislations, (for the UAV e.g. in terms of data protection). Pay attention to grey areas and legal vacuums, particularly when developing and deploying new solutions or tools to be used across borders. When organizing international solutions, seek to create positive spill over effects on international relations by harmonizing regulation.
- **Recommendation:** Ensure that the resources and content of the supply chain respects the diversity of the target population by taking gender, religious and/or cultural needs and rights into consideration. This could e.g. mean to include hygiene articles suitable for females, and include food that is suitable for all relevant religions. Ensure that the distribution of resources does not discriminate against any social groups in a way that can be seen as denying the dignity of people.
- **Recommendation:** In general, although citizens are already to a large extent expected to help themselves during a crisis, remember and acknowledge that citizens do expect coordinated emergency help from their authorities. Be aware that citizens may feel overburdened with responsibility in such a situation, and make sure to demonstrate who is to be held accountable during crises. Regularly practice the procedures for resilience logistics to enforce their effect and to strengthen the accountability of the organization. Ensure that the supply chains and the distribution of resources are developed and deployed in a way that treats all societal groups equally, and that they do not discriminate against someone based on their ethnical or religious characteristics.

# 6.5 Recommendations for Information Management

# 6.5.1 Collection & Storage of Data

• **Recommendation:** The collection, storage and processing of data and information facilitated by the DRIVER solutions needs to uphold the data protection regulations to protect the privacy of those whose data may be collected. Data collection in a so-called open society adheres to the principles of privacy, data protection and integrity. It follows a process that is suitable to the cause and proportional to the task. This means that solution developers need

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	109 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



to ask if the data collection is really necessary, and if those data are best suited to fulfil the given function. Are there alternatives to collecting personal data (in particular *sensitive* data), or can it be encrypted or anonymized? Seize opportunities to demonstrate best practice in terms of data protection, for example by consulting the local Data Protection Authority. To minimize potential infringements and to increase the social acceptability of the CM solution, consider embedding privacy friendly design choices and privacy friendly defaults in the data collecting tools, as part of a "Privacy-by –Design"- approach.

- Recommendation: The risk for misuse of collected data needs to be actively counteracted in all phases of the CM solution's development and deployment. To minimize the risk of misuse, make sure to only collect the data you need for the predefined purpose and adhere to central data protection principles such as not reusing collected data uncritically. Have mechanisms for secured storage of the collected data in place. This can include locks and other physical security measures, but also password protection or encryption of data. Do not store data for longer than necessary. Regarding the application of new technology and unexplored legal fields (creating new vulnerabilities) for data collection, local Data Protection Authorities should be consulted when necessary.
- **Recommendation:** Generally, communicate the purpose of the data collection clearly to the public in order to stimulate long- and short term trust in the population. A trustful relationship between the population and the crisis mangers can have mutual advantages as it may foster certain calmness in the population, while it can enforce the integrity and reliability of the data collector at the same time. Don't base the data collection on dubious information or sources. Be transparent and clear about the method for the data collection when you eventually distribute the collected information, since having a general level of trust in society makes it easier for people to put their wellbeing in the hands of other people.
- Recommendation: Account for the data collection methodologies you choose, and reflect upon the fact that some technologies and collection processes can be limiting, as they influence what data can be collected. For example, data collection by a drone provides the crisis manager with visual images (which has its own advantages and imitations), while collecting data through a mobile phone application allows for the inclusion of other context factors (that you would not get from using a drone). Only collect the data you need. Reflect also upon whether the data collection generally contributes to more flexibility, by considering how more easily regulated and governed datasets can make the potential utilization and coherence of the data (in the future and in other parts of the CM organization) more flexible, and thus increase transferability in CM.
- **Recommendation:** In order to establish the population's trust in the CM solution, be as open as possible about the way the data is being collected, how it is being used and stored, with whom it will be shared, and when it will be deleted. To build trust, and especially when introducing new methods for data collection, make sure to inform the population in a sufficient manner. Integrating information about the data collection only in the fine prints of the "terms and conditions" does not build trust. Make sure that the consent given is *active* consent, meaning that the individual who is sharing his data actively (not just passively, by receiving a letter about it) agrees to the data collection. Depending on the scope and depth

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	110 of 159	
Reference:	D840.21	V840.21 Dissemination: PU Version: 3.0 S						



of the data collection, consider other ways of informing the public about it, such as media information campaigns. As part of this, also pay attention to the fact that any individual from whom the data is collected from whom personal data is being collected has the right to launch a subject access request allowing her to access all the data that the data controller has stored about her. On EU level, the right to access is defined in Article 12 of the European Union Data Protection Directive (DPD) [46].

- Recommendation: Data collection and storage must happen in a way that does not infringe upon the social cohesion of the population. Avoiding the collection of data that can create suspicion (e.g. if it is seen as unjust or as fostering inequalities by focusing in particular on a certain ethic group without a clear reason), can happen by e.g. ensuring proportionality in the data collection, and by communicating this in an open and transparent manner to the individuals from whom the data is collected. The argumentation for the choices made should be as transparent as possible, and the data collected should be proportional to the case, e.g. not include more sensitive data than necessary. When relying on data collecting mechanism that require certain equipment (such as a cell phone or a computer), compensate for the fact that not all members of society have access to such equipment (for example due to low/ high age, loss of income, homelessness, etc.). Marginal groups should be equally included in the CM activity that includes the data collection as other groups.
- Recommendation: When planning the CM activity, make sure that those subjects you collect data from are diverse, and selected on an equal and fair basis. Accounting for diversity concretely means including variables such as language, ethnicity, gender, culture and religion in the selection of participants or volunteers for the CM activity. This will ensure a more broad and accurate feedback, in addition to fostering opportunities for enforcing solidarity and diversity.
- **Recommendation:** To create a sustainable environment for participation, make sure to collect informed consent and to notify the relevant individuals before collecting data. Limit especially the collection of sensitive data, such as health information or political information. Aim for participatory approaches to the development of CM solutions, especially if the final CM solutions are meant to be used by the general public. Pay attention to maintaining a trustful relationship between the population and the crisis managers, and give clear and easy messages to the public in order to stimulate a transparent (cf. *transparency*) way of participating in the CM activity.
- **Recommendation:** Avoid CM solutions for data collection or storage unnecessarily targeting certain groups, as this could be seen as a discriminatory practice. Account for diversity in both the planning and deployment of the data based- CM solution, including general variables such as language, ethnicity, gender, culture and religion. Although these variables are considered sensitive data, this will make the data more fair and non-discriminatory, but only of the information is not used to make decisions that can have negative implications for the groups. Don't reuse sensitive data, and don't use that information to discriminate against the groups from which the information derived.
- **Recommendation:** To avoid influencing the relationship between state and citizens in a negative way as well as to protect the political reputation of the CM actor (whether

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	111 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



professional, tool developer, volunteer, etc.), open, clear and timely communication is paramount. A participatory approach to the development of CM solutions (involving the public) can, if done in a good and sensible way, positively influence the political reputation of the CM actor, also because it makes it easier for the CM actor to take the diversity (age, gender, culture etc.) of the population into account (cf. *diversity*).

Recommendation: In most cases data collection for CM is unavoidable (such as pooling of data in public registers), but the data collector should inform the relevant individuals prior to the data collection exercise and respect their right to object to their data being collected. Consider also if the data collection itself is necessary, especially when it comes to intrusive data collection. Including the diverse population in focus groups and interviews, and let them raise their concerns as far as possible. Ensuring a continuous high level of compliance with the abovementioned recommendations in the relevant CM solutions can contribute to making best practice data collecting solutions the standard procedure for CM.

# 6.5.2 Facilitating Data Processing (Incl. Operational Data Lift)

- Recommendation: When planning CM measures, consider if there is a real need for facilitating the processing of data in the planned scale, and reflect upon whether the action is leaving you more vulnerable by creating more technology dependency. If this is hard to avoid, have backup solutions available, e.g. alternative ways of ensuring that the collected data is being protected according to relevant regulations. The general principle is to minimize data processing wherever possible, and to only collect the data that is needed for the activity. When designing the measures that lead to the processing of data, and to ensure the efficiency of the procedure, Consider if a risk- or Privacy Impact Assessment (PIA) could be useful to tailor the solution (e.g. by minimizing the amount of personal data that is collected for processing). Minimize secondary insecurities and challenges like function creep, misuse and the creation of new vulnerabilities by making the limitation of data processing a (built-in) feature of the solution, for example through making a PIA mandatory. Working with regional and international organizations to create platforms for facilitating the exchange of information (or other means of data processing) can be important to strengthen resilience [50] and also push progress on the CM area.
- **Recommendation:** The facilitation of data processing largely falls under the general rules for data protection, and should adhere to the basic principle of legality. This includes acknowledging that although the data collection may be legal, the processing may not be-and vice versa. Especially if the processed data are sensitive data, particular measures and requirements may apply (depending on national regulation). To avoid lowering trust between partners facilitating data exchange or other forms of data processing, ensure that the process is transparent, open, and adhering to all relevant legal data protection frameworks. Be clear and transparent when communicating with the individuals from whom the data is collected about the processing of data, stating why it is necessary, and why it is suitable for pursuing the given objective. When facilitating data processing, in terms of

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	112 of 159	
Reference:	D840.21	B40.21   Dissemination:   PU   Version:   3.0						



sharing data between two or more partners (or the public), ensure that involved actors have the opportunity to voice their questions and concerns. This can enforce trustful relationships both in the short and in the long term, and may even have positive spill-over effects onto other domains of the cooperation. Consider also if the data processing tools are disproportionate in relation to the interests affected. The facilitation should include possibilities for encryption or anonymisation of personal data whenever possible, even if this means that the possibility of the individual to withdraw (their data) from the activity or to access their data, disappears.

- Recommendation: Make sure that the data processing solution does not facilitate data processing that favours one social group over another, unless there is a good cause for it (such as adjusting for low- income countries). Such reasons should be communicated in a clear and transparent manner (cf. *transparency*). Ensure also that the data processing tools adhere to data protection legislation, and that they facilitate making claims of privacy such as exercising the data access right, which is a measure intended e.g. to create transparency in the data processing, and make it easier for the individual to know how their data is being processed. Developing and streamlining this practice can, especially in the long run, help fostering solidarity as it is an action that produces good standards in society.
- **Recommendation**: Make sure that the data processing is based on ethically acceptable methods, e.g. data protection regulations, in order to enforce the accountability of the data processor(s) by valuing core principles for good governance. The method or tool for facilitating data processing (such as data exchange), should include a mechanism for informing the individuals from whom the data is collected about how her personal data is taken care of in the process. To avoid negative standardization of data processing routines, planning- and impact assessments can verify whether the process. Following particularly good routines or mechanisms for ensuring legal compliance (and taking better care of individual privacy) contributes to a (positive) standardization or a normalization of best practice.
- Recommendation: The integrity and political reputation of the data processor(s), can be
  positively influenced if it is publicized that common ethical and legal principles are explicitly
  taken into account by the CM organization when developing and deploying the data
  processing tool. Communicate your compliance with such practice in a clear and transparent
  manner to the relevant parties.

# 6.5.3 Analysis & Evaluation

• **Recommendation:** Analysis and processing of data and information needs to have a predefined purpose and happen according to data protection legislation in the country where data Is collected. This needs to be done to make the output legally usable and to protect the data protection rights (such as informing the individuals from whom the data is collected in advance) of the individuals from whom the information is gathered. Stay updated on all relevant legal guidelines and regulations affecting the analysis method or

Document name:	D840.21 – A gui functions – Vers	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1						
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



evaluation tool (or similar) to be better prepared to ensure and "calm" potential actors inquiring about the data processing.

- **Recommendation**: Make sure that data analysis happens with a clear and predefined purpose, meaning that the use of it is controlled and specialized to the aim. Make sure that the data is only put to use for the purpose it was collected for, to uphold or strengthen the integrity and political reputation of the data controller, and to minimize the risk of function creep. To enforce trust, set rules that limit the role of the data controller or the legally responsible actor, e.g. to ensure that the data is secure with regards to confidentiality, integrity and accessibility.
- **Recommendation**: The purpose for data analysis or evaluation must be clearly communicated. When analysing personal data, the individuals from whom that data was collected must be made aware of the full use of the data, and their claims and comments should not be re-interpreted in a different context later. For example, when collecting data for one purpose, e.g. gather information about the movement patters of residents in a certain area for CM logistics purposes, this data cannot be reused in order to analyse their health status. To enforce trust, and to minimize the potential for misuse and suspicion, rules should be set to limit the role of the data controller or the legally responsible actor<sup>105</sup>. Consider setting goals like the authentication of system users, the use of encryption and decryption, deletion of data in case of system failure (especially for sensitive data), and other goals to ensure trustable and secure data processing. Such measures can foster trust in the more general sense, both from the user's perspective and from the perspective of the individuals from whom the data is collected.
- **Recommendation:** Reassure the individuals from whom the data is collected about the protection of their privacy according to established data protection rights. Up to a certain point in the process (usually until the data is anonymized or encrypted) allow the individual to withdraw their personal data. Establish and keep connections with the local or relevant Data Protection Authorities, and use this resource for directing questions or challenges to, as it may potentially benefit and lay the groundwork and for other data processing actors in the future. Seize opportunities to follow best- practice for data protection and privacy rights. When collaborating with international actors on data collection and analysis, follow the data protection rules of the country with the highest data protection standards.
- **Recommendation:** In addition to not collecting and analysing more data than you need for the particular purpose (and to not reuse this data uncritically), the process of doing data analysis and evaluation needs to be transparent and as open as possible in order for the involved actors to experience that their data is being processed in a rightful manner, and to ensure that the accountability of the data processor is maintained. When relevant, ensure that the analysed data is made up of contributions from a wide range of diverse societal groups, as equality and freedom of thought are examples of traits of an open society<sup>106</sup>.

<sup>105</sup>FHG will provide legal and regulatory advice to the DRIVER project, and the ethical procedures, risks and safeguards for responsible research (including, but not limited to SC15), can be found in D91.3. (new D14.3)

<sup>&</sup>lt;sup>106</sup> The concept of the open society was originally brought forth by Henri Bergson. See for example Henri Bergson, Les Deux Sources de la morale et de la religion, Félix Alcan, 1937 [1932], pp. 287–343. Available at :

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	114 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



- **Recommendation:** Pay attention to opportunities for fostering a positive climate in the international relation(s), and if relevant, see how you can organize the cooperation in a way that can be made sustainable also beyond the specific issue at stake.
- Recommendation: Plan the analysis and evaluation process adhering to high ethical and societal principles (such as privacy) in data analysis to enforce the accountability and integrity of the actor(s). Aim for best practice in the data analysis, including the encryption of data when possible, and by only collecting or drawing out the data you need for doing the particular analysis.
- **Recommendation:** Make sure that the collected data is analysed in a suitable way, for example by ensuring that the data is collected based on fair and just principles, and that the data are the best data to analyse in order to say something about the issue at stake. Establish clear procedures and mechanisms which allow the individuals from whom the data is collected to exercise and voice their data protection rights and claims, such as the right to withdraw and access their data according to the relevant data protection regulations. Make sure that the data analysis process is resulting in an analysis of data that are appropriate and applicable for the particular task.

# 6.5.4 Communication between first responders

- **Recommendations:** As developer of CM solutions, take into consideration, that web-based communication may be of great added value for enabling interoperability, but if possible, ensure that sufficient non-electricity/non-high-tech based ways of communicating is available as backup systems, in order to minimize vulnerabilities. As decision maker you should consider establishing regulations for foreseeing to keep backup procedures in the case of a failure of new technologies and to make sure to have alternative plans and redundancies for communication systems as part of your resilience plans to avoid complete dependency on one communication channel. Also when procuring for new solutions flexibility and openness of the system may be formulated as high level prerequisite.
- **Recommendation**: As a decision maker you should closely examine the suitability and necessity of prioritizing data, and inform the public when establishing such measures. Additional awareness rising for the population, on how to prepare for communication outage (e.g. agree a meeting point with your family in case you are separated and can't reach each other) may be a good accompanying measure.
- **Recommendation:** Minimizing the amount of data that is being exchanged will automatically minimize the risk of misuse of the data. Unnecessary data exchange should be avoided, and the risks and threats should be evaluated, to minimize the risk of function creep. The rules for data protection need to be carefully upheld in order to limit or prevent potential misuse of the information. Ensure that the receiving partner has a satisfactory level of protection for

https://fr.wikisource.org/wiki/Les\_Deux\_Sources\_de\_la\_morale\_et\_de\_la\_religion/Chapitre\_IV. The concept is now widely used in various academic disciplines, such as criminology, political science and sociology.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	115 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



the exchanged data, and if in doubt, aim for complying with the legislation or regulation with the highest requirements.

- Recommendations: Ensure conformity with European data protection regulations when implementing communication tools for communication between crisis managers (both ICT and non-electronic based) and relevant national regulations. As policy maker you shall clearly set out safeguards to protect personal data, such as setting limits for what the communication technology will be used for, to minimize the risk of misuse. Access to databases must be limited both practically and legally. Solutions for encryption should be considered. This means that the very process and principle of exchanging information and data needs to be deemed the best solution for the issues at stake, a reflection which would include evaluating the applicability of the data exchange. For sustainable data sharing, especially on the European level, creating a constructive culture of data sharing can include, for example, developing financial and legal frameworks by working together with relevant partners and organizations. In addition to that, developing sustainable funding solutions for such initiatives is crucial [53]. Ensure that the data exchange process is open and transparent (as far as it is possible and reasonable), i.e. let the individuals from whom the data is collected know in advance to what extent their data will be exchanged and shared.
- Recommendation: Make sure that the data exchange happens in a way that is as transparent as possible, in order to minimize feelings of suspicion and unease as to how the process is carried out and why it is necessary. Also, as a general principle, do not share more data than necessary to further reduce this risk. Take account of the fact that more people are aware of and sensitized towards privacy and data protection issues in light of recent global events such as the Snowden revelations [55] and the Right to be Forgotten- case [56]. Explore the opportunities for exchanging relevant knowledge and experience from actors in different contexts, sectors and countries, especially if you know that similar crisis situations have been previously tackled elsewhere and that the exchange could contribute in calming the situation. While ensuring the privacy of the individuals from whom the data is collected, as solution provider you should assure that the communication solution used by crisis managers is designed to support documentation so that it can be analysed and evaluated post- crisis. As part of an open society, transparency can enforce trust between the population and the crisis managers.
- Recommendation: As CM solution provider you shall ensure that your solutions are in line
  with international treaties or regulations, in order to ease implementation and minimize
  potential negative effects. Also when implementing a communication solution intended for
  international cooperation, it is important that the communication tool functions equally well
  in all the countries and takes into account, as much as possible and sensible, cultural and
  historical contexts in the relevant countries.
- Recommendation: Data exchange should happen only after a critical evaluation of the integrity of the receiver and after ensuring that the receiver upholds standard routines and regulations for processing the exchanged data. Be aware of this risk when exchanging data with third countries outside the Schengen- or EEA area. For CM professionals, avoid exchanging data with partners that fundamentally conflict with society's common principles,

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	116 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



interests, objectives or standards. Ensure that the process happen in a transparent manner, in order to better overlook that the interests of the different partners are accounted for. Make sure the data being exchanged are representative of the cause, i.e. that it takes, for example, diversity, cultural and gender differences into account.

Recommendation: Make sure that the data exchanging process happens according to relevant legal frames. Ensure that the data exchange is proportional to the case at stake, that it is suitable to solve the issue, and that it is necessary. The latter is important because the exchange can increase the risk of misuse or function creep. Make sure that the exchange happens in a transparent manner. This includes making sure that all relevant data protection regulations and laws are being followed. Especially when exchanging personal data with other actors, clearly state the limitations of the data processing already before the data collected are subject to unjust control. If possible, seize opportunities to establish best-practice rules for data exchange in your company or organization, and investigate how your local Data Protection Authority can be of assistance in such a process. Consider building on networks that might emerge from the data exchange process. These can be beneficial in other areas of the crisis management operation as well.

# 6.6 Recommendations for Competence- building for Decision- makers and organizations

- Recommendation: When putting a competence-development framework to use, ensure to
  identify all relevant stakeholders first. Reflect on their respective positions and stakes and
  ensure that everyone's position is taken account of when identifying and discussing
  competences, gaps in competences and new ways of building competences to foster a
  culture of trust.
- Recommendation: When designing quantitative decision-making models, evaluate carefully
  which decision-making parameters can be translated into numeric values and how. Design
  decision-making models in which each parameter is clearly defined and its users will have a
  clear understanding of the results presented to them. Through that, you can control the
  misuse of decision-making methodologies for unintended political or institutional agendasetting.
- **Recommendation:** The design of a decision-making methodology should clearly define the goal of the framework and then devise a method that addresses this goal concretely. Here, a broad framework may be more sustainable, but also less precise in its outcomes. When designing frameworks, ensure that it is possible to update the methodology over time and across different contexts.
- **Recommendation:** Clarify where and how a decision-making methodology provides for rationales to take specific decisions. Make these rationales explicit and allow the decision-

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	117 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



maker to reflect about the effect that these decision-rationales have on their own accountability when taking such decisions.

- **Recommendation:** Devise frameworks as transparent as possible so that they are actionable. Identify the concrete problems to be solved or gaps to be closed and reflect about the different context-factors that influence the respective decision-makers position. At best, decision-making frameworks document and make comprehensible any step of decision-making in order to make decision-making as transparent as possible. Make sure that political agenda-setting is not covertly integrated into decision-making processes by including methodologies that overtly address political agenda setting and priorities.
- **Recommendation:** Once you have defined for which concrete target group or problem the framework is supposed to be used, make sure all relevant partners are involved in devising or at least in reviewing competence-building models. Base competence building models on international consensus. Even if you develop national frameworks, reflect on potential international impacts. If you develop internationally relevant frameworks, ensure that the framework does not collide with each participant countries' specific legal, political, social and economic situation.
- Recommendation: Take into account how a new framework also creates new standards in decision-making. Can these standards be fulfilled by every participating country? Are they actionable and effective standards for every country? What are the accountabilities that the framework requires? While reflecting on answers to such questions already at the designstage of competence and decision-making frameworks, you can ensure a positive new standard has the chance to materialize.
- Recommendation: Fair, proportional and non-discriminatory crisis management starts at the decision-makers level. When designing decision-making frameworks for crisis management, take local contexts into account. Geography, ethnicity, socio-economic indicators, age, gender and culture are important influence factors in identifying the best possible decisions in CM and to make them acceptable across society. These factors already play a role at high-level decision-making, which is why decision-making frameworks should include respective representatives of each group. This participation can help taking account of diversity and gender-, age- and culture-sensitive competences and solutions needed in European crisis management.
- Recommendation: Utilize the full potential of the frameworks you design for decisionmakers, for example by reminding them about the possibility not only to assess and take account of technological or other standard solutions, but a broad range of crisis management solutions.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	118 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# 7 Conclusions & way ahead: utilizing SIA throughout the project and key recommendations

The assessments presented in this deliverable are examples of how the SIA framework may concretely produce useful and applicable assessments of various functions of CM solutions. The first set of assessments presented here, thus has two functions: 1) they are demonstrating the SIA framework and methodology in practise, and they are 2) already providing useful recommendations to crisis managers working with the respective solutions. The current version of the assessments includes the actual assessments, examples and recommendations based on the framework developed in D840.11. All of them have been presented, updated and revised several times.

As mentioned in the introduction, the next step is to enhance the usage of the framework and to distribute the assessments throughout the project. Several steps are foreseen to achieve this:

- 1. The training of the SIA framework and assessments to the consortium
- 2. The integration of SIA methodology into the overall DRIVER methodology for running trials (SP2)
- 3. The integration of the SIA framework and updated assessments as a complete approach to and methodology for integration of SIA into CM, into the PoS

The feedback collected from the usage of SIA in the training sessions and throughout the trials will contribute to the updating of the assessments. This means that the assessments presented in this deliverable – thus already useful and applicable via their concrete recommendations- will be further advanced, underpinned and concrete, as the feedback from the consortium partners working with the relevant functions contribute to their updating. For the implementation of SIA via training and in the trials, a feedback mechanism is incorporated (see D94.1), which ensures that the consortium's input, criticisms and comments about the framework *or* the assessments can be taken into account. The questionnaire presented in Chapter 8.5 of this deliverable is one such mechanism. The feedback collected through various channels will serve as a basis for the revisions and final versions of the framework and the assessments foreseen in M47.

# 7.1 SIA training for the DRIVER consortium

Specific training modules including concrete examples, work sheets and pedagogical material to teach the SIA framework itself and its deployment to the DRIVER consortium, have already been developed (D94.1), and will be delivered to the consortium via dedicated training sessions. The main

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	119 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



aim of the training sessions is to ensure that the consortium members know how to use the framework's method for their own purposes, and to be able to conduct assessments themselves. The training sessions will take place throughout 2017 and will address the different partners working with different solutions, with individualized modules tailored to their needs.

The contents of the framework and assessments will be used in trials, and feedback from the consortium will shape the final categorization of functions, the set of criteria, assessments, examples and recommendations, as well as the final training modules that will be part of the SIA component to be usable beyond DRIVER. Versions 2 of the framework and the assessments will be presented in a way that facilitates and prepares the integration of these into the DRIVER Portfolio of Solutions, and as such, it is an original and distinct separate methodology for SIA .There are additional ways in which the framework can be used in and feed into various parts of DRIVER. Some of these are described in Chapter 4 of D840.11 Societal Impact Assessment Framework.

# 7.2 Potential risks and challenges

One risk is that the examples that are chosen for this deliverable may be too DRIVER specific. While they clearly relate to the actual work going on in DRIVER at the moment, the examples could be formulated as more general in the final version of the deliverable. This will ensure sustainability, and make it possible to give more general advice to crisis managers on the different areas of potential impact. In contrast, some of the actual assessments can be too general at this point in time. Through the integration of the assessments in training sessions and experiments, feedback will be harvested to make the assessments more pointed and relevant to users also beyond the project.

# 7.3 SIA questionnaire, including key recommendations

The SIA questionnaire (in Annex 1) provides a summary or preliminary "conclusion" about the assessments. It lists the four key recommendations that each assessment generated and that could serve as a guideline for those working on a particular solution. In order to make them work in and throughout the different parts of the project, these recommendations are integrated into a questionnaire. This will also help making them more operable and to gain feedback and additional inputs from the DRIVER consortium on the different assessments and recommendations. The questionnaire will also assess how important the recommendations were (to explore priorities) and whether new impacts were identified that were not yet part of the assessments. It will also ask for feedback on the assessment criteria to identify those criteria that the solution providers considered the most relevant and important. At the same time, the questionnaire also serves as yet another pedagogical tool to make solution providers more familiar with societal impact assessments altogether. Concretely, the questionnaire will be integrated into the project in several ways, as part of the PoS, and potentially as part of training sessions (which, however, will also have additional

Document name:	D840.21 – A gui functions – Vers	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1						
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



feedback mechanisms in the training material). It is also designed in such a way that a step-by-step integration into a computer-based survey is possible (i.e. translating the text into software) to avoid having to print the complete set of pages. While the questionnaire appears massive, it is designed in several sections (aligned according to the functions), and the respondents are only supposed to fill out the sections relevant for the CM solutions they are working with.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	121 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# 8 References

- [1] Lee, D. and Newby H. (1983), *The Problem of Sociology. An introduction to the discipline*, London, Unwin Hyman.
- [2] United Nations Development Program (UNDP) (2014). *Disaster Resilience Measurements,* <u>http://www.preventionweb.net/files/37916\_disasterresiliencemeasurementsundpt.pdf</u>, retrieved November 26, 2015.
- [3] Anderson, B. (1991), *Imagined communities: reflections on the origin and spread of nationalism* London, Verso.
- [4] Swedish Civil Contingencies Agency (MSB) (2013), *Strategic challenges for societal security. Analysis of five future scenarios*, https://www.msb.se/RibData/Filer/pdf/27189.pdf, retrieved November 26, 2015.
- [5] Streep, A. (2015), *The Tricky Ethics of the Lucrative Disaster Rescue Business*, <u>http://www.wired.com/2015/08/search-and-rescue-for-sale/</u>, retrieved November 26, 2015.
- [6] Friedman, D.B., Tanwar, M., & Richter, J.V.E. (2008), An evaluation of online disaster and emergency preparedness resources. *Prehospital and Disaster Medicine*, 23(5), 438-446.
- [7] El Pais (2014), Los cinco errores de comunicación institucional en la crisis del Ebola, <u>http://politica.elpais.com/politica/2014/10/09/actualidad/1412872730\_989674.html</u>, retrieved November 26, 2015.
- [8] El Pais (2014), Ebola in Spain: Five days after Ebola case confirmed, Deputy PM takes control of crisis, <u>http://elpais.com/elpais/2014/10/10/inenglish/1412949468\_311967.html</u>, retrieved November 26, 2015.
- [9] Aradau C., & V. R. Munster (2011) *The Politics of Catastrophe. Genealogies of the Unknown.* London, Routledge
- [10] Radical Geography (2009), L'Aquila Earthquake, Italy 2009, A Case study of an Earthquake in an MEDC, http://www.radicalgeography.co.uk/laquilasum.pdf, retrieved November 26, 2015.
- [11] Ropeik D. (2012), *The L Aquila Verdict: A Judgment Not against Science, but against a Failure* of Science Communication, <u>http://news.yahoo.com/l-aquila-verdict-judgment-not-against-science-against-230100998.html</u>, retrieved November 26, 2015.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	122 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- [12] Kaufmann M. (2015), Resilience 2.0: Social media and (self-)care after 2011 Norway attacks, *Media, Culture and Society* 37(7): 972-987.
- [13] Andrejevic M. and K. Gates (2014), Big Data Surveillance: Introduction. *Surveillance and Society* 12(2): 185-196.
- [14] Boyd D. and K. Crawford (2012), Critical Questions for Big Data. *Information, Communication and Society* 15(5) : 662-679.
- [15] Morozov, E. (2013), *To save everything click here. Technology, solutionism and the urge to fix problems that don't exist*, Penguine Books, London.
- [16] Porter C. (2014), *Little Privacy in the Age of Big Data*. <u>http://www.theguardian.com/technology/2014/jun/20/little-privacy-in-the-age-of-big-data</u>, retrieved November 26, 2015.
- [17] Gonzalez F. G., Bellanova R. (2013), European Data Protection and the Haunting Presence of Privacy, *Privacy and New Technologies*, NovATIca, from 2012/2013 Annual Selection of Articles 17 22.
- [18] Rosenberg J.M. (2014), Hacking a big danger for small businesses. http://www.usatoday.com/story/money/business/2014/10/12/small-business-hackingdangers/17041613/, retrieved November 26, 2015.
- [19] Kaufmann, M. (2016), «Drone/Body The Drone's Power to Sense and Construct Emergencies», in: Sandvik, K. B. and Jumbert M. G. (eds.) *The Rise of the Good Drone*, London, Ashgate.
- [20] Furedi, F. (2006), *The Culture of Fear Revisited*. London, Continuum.
- [21] Jaeger, C., Renn, O., Eugene A. R., Webler, T. (2006), *Risk, Uncertainty and Rational Action.* London, Earthscan.
- [22] Baker, T. & Simon, J. (2002), *Embracing Risk. The Changing Culture of Insurance and Responsibility*. Chicago, The University of Chicago Press.
- [23] Lindholm O. (2014), Frykter Økt overvåking etter alarm, http://www.dagsavisen.no/innenriks/frykter-%C3%B8kt-overv%C3%A5king-etter-alarm-1.290816, retrieved November 26, 2015.
- [24] Amato A., Cerase A. and Galadini F. (2015), *Terremoti, comunicazione, diritto; Riflessioni sul processo alla "Commissione Grandi Rischi"/ (Earthquakes, communication, law; Reflections on the "High Risk Committee" trial),* Hoepli, Italy.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	123 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- [25] Pappas, S. (2012), Italian Scientists Get 6 Years for L'Aquila Earthquake Statements. <u>http://www.livescience.com/24164-italian-scientists-earthquake-verdict.html</u>, retrieved November 26, 2015.
- [26] Nadeau B. (2012), *Scientists Found Guilty in L'Aquila Earthquake Trial*, <u>http://www.thedailybeast.com/articles/2012/10/22/scientists-found-guilty-in-l-aquila-earthquake-trial.html</u>, retrieved November 26, 2015.
- [27] Stenvaagnes R. (2014), *Kritiserer mediene for å skape angst etter terrortrussel*, <u>http://www.aftenposten.no/nyheter/iriks/Kritiserer-mediene-for-a-skape-angst-etter-</u>terrortrussel-7650037.html, retrieved November 26, 2015.
- [28] Thorvaldsen L. (2014), Advarer mot fryktkultur http://klassekampen.no/article/20140728/ARTICLE/140729963, retrieved November 26, 2015.
- [29] Morgenbladet (2014), Et glimt av USA, http://morgenbladet.no/samfunn/2014/et\_glimt\_av\_usa#.VCLQI\_mSx8E, retrieved November 26, 2015.
- [30] Stewart D.W. and Martin I.M. (1994), Intended and Unintended Consequences of Warning Messages: A Review and Synthesis of Empirical Research, *Journal of Public Policy & Marketing* 13 (1): 1-19.
- [31] Hagmann J. and Cavelty, M. D. (2012), National risk registers: Security scientism and the propagation of permanent insecurity. *Security Dialogue* 43(1) 79–96.
- [32] Kaufmann M. (2010), Ethic Profiling and Counter-Terrorism. Berlin: LIT Verlag.
- [33] Solem T.P. (2014), Advarer mot overdreven frykt, http://www.dagsavisen.no/samfunn/krisepsykolog-advarer-mot-overdreven-frykt/, retrieved November 26, 2015.
- [34] BBC (2011), Italy Scientists on Trial over L'Aquila Earthquake. http://www.bbc.co.uk/news/world-europe-14981921, retrieved November 26, 2015.
- [35] International Federation of the Red Cross and Red Crescent Societies (2008:8), Bridging the Gap. Integrating Climate Change in Disaster Risk Reduction, <u>http://www.ifrc.org/Global/Case%20studies/Disasters/cs-climate-change-drr-en.pdf</u>, retrieved November 26, 2015.
- [36] Briguglio, L. (2014: 27), A vulnerability and resilience framework for small states. Malta, University of Malta. <u>http://www.um.edu.mt/\_data/assets/pdf\_file/0007/215692/Briguglio\_The\_Vulnerability\_R</u> <u>esilience\_Framework, 23\_Mar\_2014.pdf</u>., retrieved November 26, 2015.
- [37] Cutter, S. L., Burton C. G. & Emrich C. T (2010), Disaster Resilience Indicators for Benchmarking Baseline Conditions. *Journal of Homeland Security and Emergency*

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	124 of 159	
Reference:	D840.21	840.21 Dissemination: PU Version: 3.0						



Management.

http://www.degruyter.com/view/j/jhsem.2010.7.1/jhsem.2010.7.1.1732/jhsem.2010.7.1.17 32.xml, retrieved November 26, 2015.

- [38] Kaufmann, M. (2013), Cyber-resiliens i EU. *Internasjonal Politikk* 71(2): 274-283.
- [39] Staff W. (2005), *Katrina day-by-day recap.* Palm Beach Post. September 1, 2005.
- [40] Bygrave, L. (2002), *Data protection law. Approaching its rationale, logic and limits.* Great Britain. Anthony Rowe Limited.
- [41] Garland, D. (2001), *The culture of control. Crime and Social Order in Contemporary Society.* The University of Chicago Press Books.
- [42] Miser, C. (2013), Falcon UAV Supports Colorado Flooding Until Grounded by FEMA. http://www.falconunmanned.com/falcon-uav-news/2013/9/14/-falcon-uav-supportscolorado-flooding-until-grounded-by-fem.html, retrieved November 26, 2015.
- [43] Article 29 Data Protection Working Party (2015), Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones. <u>http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231\_en.pdf</u>, retrieved November 26, 2015.
- [44] Ackerman, S. & Roberts, D. (2014), US government board says NSA bulk collection of phone data is illegal. <u>http://www.theguardian.com/world/2014/jan/23/nsa-barack-obama-phone-data-collection-illegal-privacy-board</u>, retrieved November 26, 2015.
- [45] Vieweg, S., Hughes, A. L., Starbird, K., & Palen, L. (2010), *Microblogging during two natural hazards events: What twitter may contribute to situational awareness.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, Georgia, USA.
- [46] European Parliament & The European Council (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal* L 281, 23/11/1995 P. 0031 0050.
- [47] Lyon, D. (2003), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*. London, Routledge.
- [48] Cohn, C. (2014), NSA Surveillance Chilling Effects: HRW and ACLU Gather More Evidence. The Electronic Frontier Foundation, <u>https://www.eff.org/deeplinks/2014/07/nsa-surveillance-chilling-effects,</u> retrieved November 26, 2015.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	125 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- [49] Datatilsynet (2014), *Dronar- kva er lov*? <u>http://www.datatilsynet.no/Teknologi/Dronar--kva-er-lov/,</u> retrieved November 26, 2015.
- [50] European Commission (2013), Disaster Risk Reduction. Increasing Resilience by Reducing Disaster Risk in Humanitarian Action. <u>http://ec.europa.eu/echo/files/policies/prevention\_preparedness/DRR\_thematic\_policy\_doc</u> .<u>pdf,</u>retrieved November 26, 2015.
- [51] Information Commissionaires Office (ICO), *What is privacy by design*? <u>https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/</u>, retrieved November 26, 2015.
- [52] Toshiba, Pålitelig databehandling: jakten på den sikre mobile plattformen, http://www.toshiba.no/Contents/Toshiba\_nd/ND-NO/WHITEPAPER/files/FEA-2005-04-Trustable-Computing-ND.pdf, retrieved November 26, 2015.
- [53] The Alfred Wegener Institute for Polar and Marine Research (ed.) (2011), *Ten Tales of Drivers & Barriers in Data Sharing. Setting Course for a Data Sharing Culture.* Brochure of the ODE project (Opportunities for Data Exchange), <u>http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2011/10/7782\_ODE\_Brochure\_v5.pdf</u>, retrieved November 26, 2015.
- [54] Tuunainen, V. K., Pitkänen, O., Hovi, M. (2009), Users' Awareness of Privacy on Online Social Networking Sites – Case Facebook (2009). <u>http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1000&context=bled2009</u>, retrieved November 26, 2015.
- [55] Thon, B. E. & T. Tennøe (2014), Personvernet etter Snowden, <u>http://www.personvernbloggen.no/2014/01/28/personvernet-etter-snowden/</u>, retrieved November 26, 2015.
- [56] Court of Justice of the Europen Union (2014), Case C-131/12. 2014. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014). Case C-131/12.
   http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d644d05bf64bd 7411e9133855057590c48.e34KaxiLc3qMb40Rch0SaxuOaxj0?text=&docid=152065&pageInde x=0&doclang=EN&mode=Ist&dir=&occ=first&part=1&cid=29115, retrieved November 26, 2015.
- [57] Bianco, D. P., *Decision Making*, Reference for Business, <u>http://www.referenceforbusiness.com/management/De-Ele/Decision-Making.html</u>, retrieved November 26, 2015.
- [58] Hammond, J. S., Keeney, R. L., and Raiffa, H. (1998), The Hidden Traps in Decision Making. *Harvard Business Review* 76, no. 5, 1-11.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	126 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



- [59] Edwards M. (2012), Decision Making and Accountability Deficits in Public Governance, CEPA Meeting, UN, 17 April 2012. Discussant. <u>http://unpan1.un.org/intradoc/groups/public/documents/unpan049018.pdf</u>, retrieved November 26, 2015.
- [60] Triad Business Journal (2009), *Decision-making process should be open, transparent*. <u>http://www.bizjournals.com/triad/stories/2009/10/12/smallb3.html?page=all</u>, retrieved November 26, 2015.
- [61] Windle, G., Bennett, K. M., Noyes, J. (2011), A methodological review of resilience measurement scales, Health Qual Life Outcomes. 2011; 9: 8. <a href="http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3042897/">http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3042897/</a>, retrieved December 15, 2015.
- [62] Seo, M., Sun, S., Merolla A. J., Zhang, S. (2012), Willingness to Help Following the Sichuan Earthquake. Modeling the Effects of Media Involvement, Stress, Trust, and Relational Resources, Communication Research vol. 39 no. 3-25. <u>http://crx.sagepub.com/content/39/1/3.abstract</u>, retrieved December 15, 2015.
- [63] Wünsch, S. (2013), #Floodwaters Social networks in the time of disaster, Deutsche Welle <u>http://www.dw.com/en/floodwaters-social-networks-in-the-time-of-disaster/a-16867078</u>, retrieved December 15, 2015.
- [64] Rodriguez, S. (1997), Diversity and Volunteerism: Deriving Advantage from Difference, Presentation at the 1996 International Conference on Volunteer Administration. Posted with permission of THE JOURNAL OF VOLUNTEER ADMINISTRATION from its Spring 1997 issue, Volume XV, No. 3, pp. 18-20, <u>https://www.energizeinc.com/art/diversity-and-volunteerismderiving-advantage-difference</u>, retrieved December 16, 2015.
- [65] Bishop, L. (2009), Ethical Sharing and Reuse of Qualitative Data, Australian Journal of Social Issues, Volume 44 Issue 3, <u>http://search.informit.com.au/documentSummary;dn=074756462301919;res=IELHSS</u>, retrieved December 16, 2015.
- [66] Levine, S. (2014), Assessing resilience: why quantification misses the point. HPG Working paper. <u>http://www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9049.pdf</u>, retrieved December 16, 2015
- [67] Kramer, R. M. & Tyler, T. R. (eds.) (1996), *Trust in Organizations. Frontiers of theory and research.* London, Sage Publications.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	127 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- [68] Business Dictionary, gap analysis. Available at: http://www.businessdictionary.com/definition/gap-analysis.html
- [69] Red 24 Assist, *Gap Analysis Tool- GAT*. Available at: <u>https://www.red24assist.com/gap-analysis-tool-gat</u>
- [70] Lopez-Claros, A., Zahidi S.,(2005), *Women's Empowerment: Measuring the Global Gender Gap. World Economic Forum,* <u>http://www.weforum.org/pdf/Global\_Competitiveness\_Reports/Reports/gender\_gap.pdf</u> retrieved November 20, 2015.
- [71] Cohn, C. (2014), *NSA Surveillance Chilling Effects: HRW and ACLU Gather More Evidence*. The Electronic Frontier Foundation. Available at: <u>https://www.eff.org/deeplinks/2014/07/nsa-surveillance-chilling-effects</u> retrieved November 20, 2015.
- [72] Van Breugel, P., Kindt, R., Lillesø, J.-P. B., & van Breugel, M. (2015). Environmental Gap Analysis to Prioritize Conservation Efforts in Eastern Africa. PLoS ONE, 10(4), e0121444. <u>http://doi.org/10.1371/journal.pone.0121444</u>
- [73] Beckfield, J., & Krieger, N. (2009). Epi+ demos+ cracy: linking political systems and priorities to the magnitude of health inequities—evidence, gaps, and a research agenda. Epidemiologic reviews, mxp002. Available at: http://epirev.oxfordjournals.org/content/early/2009/05/27/epirev.mxp002.short
- [74]
   Transparency international. The glaobal coalition against corruption. Politics and government.
   Available
   at:

   http://www.transparency.org/topic/detail/politics\_and\_government
   Available
   at:
- [75] Cloud Access. Vulnerability Assessment/Security Risk Gap Analysis. Available at: http://www.cloudaccess.com/solutions/business-solutions/vulnerabilityassessement/
- [76] Swedish Civil Contingencies Agency. *Guide to Risk and vulnerability analysis.* Available at: <u>https://www.msb.se/RibData/Filer/pdf/26267.pdf</u>
- [77] Brändstrøm, A. 2016, Crisis, Accountability and Blame Management Strategies and Survival of Political Office-Holders. Available at: <u>http://fhs.diva-portal.org/smash/get/diva2:896367/FULLTEXT01.pdf</u>
- [78] Mancuso M., Serge Desmarais, Kelly Parkinson and Brian Pettigrew. Disappointment, Misunderstanding and Expectations: A Gap Analysis of NSSE, BCSSE and FSSE. Higher Eductions Quality Council of Ontario. Available at: http://www.heqco.ca/SiteCollectionDocuments/WS%20NSSEBCSSEFSSE.pdf
- [79] Leivesley, S "Permanent Monitoring Panel- Mitigation of Terrorist Act, Report for the year 2010-2011". In Ragaini, R C International Seminar on Nuclear War and Planetary Emergencies: 44<sup>th</sup> session.
- [80] Garland, D. 2001, *The culture of control. Crime and social order in contemporary society.* Oxford. Oxford University press.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	128 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- [81] Harrison, K. *Learn the secrets of stakeholder communication during a crisis.* Cutting Edge PR. Available at: <u>http://www.cuttingedgepr.com/articles/crisiscomm\_learn\_the\_secrets.asp</u>
- [82] European Comission. *Misuse of your personal data redress.* Available at: http://ec.europa.eu/justice/data-protection/individuals/misuse-personal-data/index\_en.htm
- [83] United Nations Office on Drugs and Crime, 2013, Abuse of a position of vulnerability and other "means" within the definition of trafficking in persons. Issue paper. Available at: <u>https://www.unodc.org/documents/human-trafficking/2012/UNODC\_2012\_Issue\_Paper\_-</u> \_Abuse of a Position of Vulnerability.pdf
- [84] Value Forward group, 2016, *Market gap analysis.* Available at: <u>http://valueforward.com/market-gap-analysis/</u>
- [85] Kish, Leslie (1995) Survey Sampling, Wiley, ISBN 0-471-10949-5.
- [86] ShortTutorials.com, Sanitary Napkins for Woman. Emergency Disaster Survival Kit. Available at: <u>https://www.shorttutorials.com/basic-disaster-supplies-kit/sanitary-napkins.html</u>
- [87] Schorr, Lisbeth & Frank Darrow, 2011, Expanding the Evidence Universe. Doing Better by Knowing More.Center for the study of social policy. Available at: <u>http://www.cssp.org/publications/harold-richman-public-policy-symposium/Expanding-</u> Evidence-the-Evidence-Universe Doing-Better-by-Knowing-More December-2011.pdf
- [88] European Data Protection Directive (Directive 95/46EC). Available at: <u>http://eur-</u>lex.europa.eu/LexUriServ/LexUriServ. do?uri=CELEX:31995L0046:en:HTML
- [89] European Network for Psychosocial Crisis Management Assisting Disabled in Case of Disaster, EUNAD. Available at: <u>https://www.nkvts.no/prosjekt/european-network-for-psychosocial-crisis-management-assisting-disabled-in-case-of-disaster-eunad/</u>
- [90] Austin Research, *The importance of representative samples and how to get them*. Available at: <u>http://austinresearch.co.uk/the-importance-of-representative-samples-and-how-to-get-them/</u>
- [91] The Sydney Morning Herald, 2012, *Is your workplace blind to staff diversity*? Available at: <u>http://www.smh.com.au/small-business/the-venture/is-your-workplace-blind-to-staff-</u> <u>diversity-20120612-206up.html</u>
- [92] National Research Council. 1999, *The impacts of natural disasters: A framework for loss estimation*, National Academy Press, Washington, D. C.
- [93] Pelling, M., A. Özerdem, and S. Barakat. 2002. "The macro-economic impact of disasters". *Progress in Development Studies* 2, (4): 283-305.
- [94] Norris, Pippa, 2001, *Digital Divide. Civic engagement, information poverty, and the internet worldwide*. Cambridge University press.
- [95] Adams, A. S., Soumerai, S. B., Lomas, J., & Ross-Degnan, D. (1999). Evidence of self-report bias in assessing adherence to guidelines. International Journal for Quality in Health Care, 11(3), 187-192.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	129 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



- [96] Crow, G., Wiles, R., Heath, S., & Charles, V. (2006). *Research ethics and data quality: The implications of informed consent*. International Journal of Social Research Methodology, 9(2), 83-95.
- [97] Klauser, F. (2008). *Spatial articulations of surveillance at the FIFA World Cup 2006TM in Germany*. Technologies of insecurity, 61-80.
- [98] Finn, R. L., & Wright, D. (2012). *Unmanned aircraft systems: Surveillance, ethics and privacy in civil applications*. Computer Law & Security Review, 28(2), 184-194.
- [99] Rothbauer, Paulette (2008) "Triangulation." In Given, Lisa (Ed.), "The SAGE Encyclopedia of Qualitative Research Methods." Sage Publications. pp. 892-894.
- [100] MissionMode, 2012, 15 Disaster, Emergency and Crisis Management Apps for iPhone and iPad. Available at: <u>http://www.missionmode.com/15-disaster-and-crisis-apps-for-iphoneand-ipad/</u>
- [101] Anson, S., Said, M., Watson, H., & Wadhwa, K. (2016, October). Improving First Aid Skills: How Local Conceptions of Risk Influence User Engagement with the First Aid App in Israel and Malta. In International Conference on Information Systems for Crisis Response and Management in Mediterranean Countries (pp. 15-21). Springer International Publishing.
- [102] Levy, G., Blumberg, N., Kreiss, Y., Ash, N., & Merin, O. (2010). Application of information technology within a field hospital deployment following the January 2010 Haiti earthquake disaster. Journal of the American Medical Informatics Association, 17(6), 626-630.
- [103] Olavsrud, Thor, 2012, *How IT Leaders Can Best Plan for Disaster*. CIO. Available at: http://www.cio.com/article/2390572/disaster-recovery/how-it-leaders-can-best-plan-fordisaster.html
- [104] Dahl, J. Y., & Sætnan, A. R. (2009). "It all happened so slowly"–On controlling function creep in forensic DNA databases. International journal of law, crime and justice, 37(3), 83-103.
- [105] Dumais, S., Cutrell, E., Cadiz, J. J., Jancke, G., Sarin, R., & Robbins, D. C. (2016, January). Stuff I've seen: a system for personal information retrieval and re-use. In ACM SIGIR Forum (Vol. 49, No. 2, pp. 28-35). ACM.
- [106] Marshall, C. C., & Shipman, F. M. (2013, May). Experiences surveying the crowd: Reflections on methods, participation, and reliability. In Proceedings of the 5th Annual ACM Web Science Conference (pp. 234-243). ACM.
- [107] Auferbauer, D., Ganhör, R., & Tellioglu, H. (2015). Moving Towards Crowd Tasking for Disaster Mitigation. In Proceedings of the ISCRAM 2015 Conference (pp. 9-3).
- [108] Howell, A. (2015). Resilience as Enhancement: Governmentality and Political Economy beyond 'Responsibilisation'. Politics, 35(1), 67-71.
- [109] Mythen, G., & Walklate, S. (2006). Communicating the terrorist risk: Harnessing a culture of fear?. Crime, Media, Culture, 2(2), 123-142.
- [110] Headey, D. (2011). Was the global food crisis really a crisis? Simulations versus self-reporting. In International Conference on Applied Economics (ICOAE) (pp. 233-43).

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	130 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- [111] Havlik, D., Egly, M., Huber, H., Kutschera, P., Falgenhauer, M., & Cizek, M. (2013, October).
   Robust and trusted crowd-sourcing and crowd-tasking in the Future Internet. In International
   Symposium on Environmental Software Systems (pp. 164-176). Springer Berlin Heidelberg.
- [112] Lemish, D., & Cohen, A. A. (2005). On the gendered nature of mobile phone culture in Israel. Sex Roles, 52(7-8), 511-521.
- [113] Oh, O., Kwon, K. H., & Rao, H. R. (2010, August). An Exploration of Social Media in Extreme Events: Rumor Theory and Twitter during the Haiti Earthquake 2010. In ICIS (p. 231).
- [114] Brown, I., & Korff, D. (2009). Terrorism and the proportionality of internet surveillance. European Journal of Criminology, 6(2), 119-134.
- [115] Cavoukian, A. (2012). Privacy and drones: Unmanned aerial vehicles (pp. 1-30). Ontario, Canada: Information and Privacy Commissioner of Ontario, Canada.
- [116] Stewart, David W. and Ingrid M. Martin, "Intended and Unintended Consequences of Warning Messages: A Review and Synthesis of Empirical Research", *Journal of Public Policy & Marketing*, Vol. 13, No. 1 (Spring, 1994), 1-19
- [117] Sætre, Simen, -Hemmeligheter er en trussel mot demokratiet. Morgenbladet, no. 1/ 2.-8 January 2015.
- [118] Jenille Fairbanks, Kenneth D. Plowman and Brad L. Rawlins, "Transparency in government communication", Journal of Public Affairs, (February 2007) Volume 7, no. 1, 23–37
- [119] Beck, Ulrich, 1999, World Risk Society, (Cambridge, Polity Press, 1999) 4.
- [120] Castells, M. (2013). Communication power. OUP Oxford.
- [121] Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management, 15(1), 50-59.
- [122] Slovic, P. E. (2000). The perception of risk. Earthscan publications.
- [123] Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management, 15(1), 50-59.
- [124] Cutter, S. L., Burton, C. G., & Emrich, C. T. (2010). Disaster resilience indicators for benchmarking baseline conditions. Journal of Homeland Security and Emergency Management, 7(1).
- [125] Glickman, T. S., & White, S. C. (2006). Security, visibility and resilience: the keys to mitigating supply chain vulnerabilities. International Journal of Logistics Systems and Management, 2(2), 107-119.
- [126] Boin, A. (2005). The politics of crisis management: Public leadership under pressure. Cambridge University Press.
- [127] Coppola, D. P. (2006). Introduction to international disaster management. Butterworth-Heinemann.
- [128] Van Wassenhove, L. N. (2006). Humanitarian aid logistics: supply chain management in high gear<sup>+</sup>. Journal of the Operational research Society, 57(5), 475-489.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	131 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



- [129] Rutherford, W. H. (1990). The place of exercises in disaster management. Injury, 21(1), 58-60.
- [130] Kennedy, J., Ashmore, J., Babister, E., & Kelman, I. (2008). The meaning of 'build back better': evidence from post-tsunami Aceh and Sri Lanka. Journal of contingencies and crisis management, 16(1), 24-36.
- [131] Maizels, A., & Nissanke, M. K. (1984). Motivations for aid to developing countries. World Development, 12(9), 879-900.
- [132] Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2009). What-You-Look-For-Is-What-You-Find-The consequences of underlying accident models in eight accident investigation manuals. Safety Science, 47(10), 1297-1311.
- [133] Wang, X., & Wan Wart, M. (2007). When public participation in administration leads to trust: An empirical assessment of managers' perceptions. Public Administration Review, 67(2), 265-278.
- [134] Hart, P., & Saunders, C. (1997). Power and trust: Critical factors in the adoption and use of electronic data interchange. Organization science, 8(1), 23-42.
- [135] Black, D. (1948). On the rationale of group decision-making. The Journal of Political Economy, 23-34.
- [136] Abelson, J., & Gauvin, F. P. (2006). Assessing the impacts of public participation: Concepts, evidence and policy implications. Ottawa: Canadian Policy Research Networks.
- [137] Oberschall A. and Kim H. (1996). Identity and Action. Mobilization: An International Quarterly: March 1996, Vol. 1, No. 1, pp. 63-85.
- [138] Hall, Stuart (1990) 'Cultural identity and diaspora' in Jonathan Rutherford (ed.) Identity: community, culture, difference, London: Lawrence & Wishart.
- [139] NATIONAL RESEARCH COUNCIL (2013) Geotargeted alerts and warnings, the role of Geotargeted alerts and warnings in disaster response.
- [140] World Health Organisation (2016), Zika Strategic Response Framework & Joint Operations Plan. Available at: <u>http://www.who.int/emergencies/zika-virus/strategic-response-framework.pdf</u>.
- [141] International Federation of Red Cross and Red Crescent Societies (2010), A practical guide to Gender-sensitive Approaches for Disaster Management. Available at: <u>http://www.ifrc.org/PageFiles/96532/A%20Guide%20for%20Gender-sensitive%20approach%20to%20DM.pdf</u>.
- [142] Coombs W. T. (2007), Crisis Management and Communication. Available at: http://www.instituteforpr.org/crisis-management-and-communications/
- [143] CDC (2014), Crisis Emergency Risk Communication. Available at: https://emergency.cdc.gov/cerc/resources/pdf/cerc\_2014edition.pdf.

[144] Kotsiopoulos I., COSMIC project, Social Media in Crisis Management: Role, Potential and Risk, Available at: <u>http://www.cosmic-project.eu/sites/default/files/conferences/Social%20Media%20in%20Crisis%20Management.pdf</u>.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	132 of 159	
Reference:	D840.21	Dissemination:         PU         Version:         3.0						



[145] Vliegenthart R. (2012), Framing in Mass Communication Research – An Overview and Assessment, Sociology Compass 6/12: 937–948.

[146] Rijken M. (2016), MEDI@4SEC project. The lay of the land - rising to the challenges of social media. Available at: <u>http://media4sec.eu/layoftheland/</u>

[147] State-of-the-Art review (2016), MEDI@4SEC project (forthcoming)

[148] Ernston, H., (2014), Stop calling me RESILIENT. Comment on Tom Slater's blog post "The resilience of neoliberal urbanism", <u>http://www.rhizomia.net/2014/02/comment-on-tom-slaters-blog-post.html</u> retrieved November 20, 2015.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	133 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# Annex 1- Societal Impact Assessment Questionnaire

# **Societal Impact Assessment Questionnaire**

Introduction

Please fill out the following questionnaire per solution. Different solutions require different questionnaires. If you can, complete this questionnaire in a group. If you do, can you write down the number of people who worked on this questionnaire?

1. Which solution are you working with? *Please fill out:* 

\_\_\_\_\_

a) Are the assignment of functions and tasks to the tested solution correct? Do they need updating? If so, how? *Please cross off those functions that are according to your view relevant for your solution. If you need a definition for the functions, please consult the relevant pages in D840.21.* 

-----

b) How well does your solution comply with the key recommendations given?
 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did. Please only conduct the recommendation ranking for the functions relevant to your solution.

-----

2. What are the solution's functions? From function 1-16 below, please cross off the functions that are relevant to your solution and in a second step rate the recommendations given for the functions you have crossed off.

Function 1: Community Engagement: "Training Communities for Psychosocial Support" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well* 

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	134 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please use the [ ] field for your ranking. Please explain why you ranked your compliance with the recommendations as you did.

# Key Recommendation 1 [ ]

When engaging with communities as trainer you should ensure that all participants can speak or contribute in an equal way, promoting a climate of openness. Also think of power relations between members of the community which may not be visible and hinder certain members to speak freely. Also reflect about the power imbalance between trainer (CM professional) and trainee (lay public). Thus foresee both a joint oral and anonymous written feedback mechanism so that people are able to articulate their views.

**1-sentence Explanation of your ranking:** 

# Key Recommendation 2 [ ]

When designing a training curriculums and selecting participants ensure that socio-cultural diversity is taking into account in the curriculum and the profile of trainees is as inclusive as possible, especially since members of specific groups, such as migrant communities and social minorities, are often underrepresented within CM professionals and volunteers. Trainers should also be able to deliver training activities to various societal target groups and take into account different culturally bound coping mechanisms.

# 1-sentence Explanation of your ranking:

-----

# Key Recommendation 3 [ ]

As CM organisation providing PSS training, select PSS-Trainers carefully to guarantee that confrontation techniques and methods of self-awareness are applied rightly and trainers do not overestimate their skills. Think about regular external evaluation of your trainers. Having a qualified psychologist in the host organisation overseeing the development of PSS training programmes and monitoring their application can assure the proper application of the former points.

# 1-sentence Explanation of your ranking:

\_\_\_\_\_

# Key Recommendation 4 [ ]

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	135 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



Training curriculums should also pay special attention to how to establish a sphere of trust among trainers and trainees and include adequate evaluation and feedback mechanisms.

1-sentence Explanation of your ranking:

\_\_\_\_\_

# Function 2: "Community Engagement: Building and Measuring Community Resilience" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

# Key Recommendation 1 [ ]

Explain in easy terms what you are doing and how especially the expected added value for the participant.

**1-sentence Explanation of your ranking:** 

-----

# Key Recommendation 2 [ ]

Solution developers shall be careful with sharing a quantitative visualisation of the resilience assessment. Such graphical representations might be appropriate for decision makers to get a quick overview, making them available to the public might trigger stigmatisation, which is especially problematic, when the assessments rely on very small samples.

**1-sentence Explanation of your ranking:** 

# Function 3: "Community Engagement: Volunteer Management (Incl. Crowd Tasking" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	136 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# Key Recommendation 1 [ ]

In order to not create suspicion regarding the effort from the population or to misuse volunteers for other tasks than originally indented, a four-eye principle<sup>107</sup> should be put into place, ideally separating the level that a) requests b) alerts and deploys the volunteers and c) the level which gives clearance to the deployment.

# **1-sentence Explanation of your ranking:**

\_\_\_\_\_

# Key Recommendation 2 [ ]

Crisis Managers responsible for applying organisation and mobilisation concepts shall see the willingness to help as chance to foster social cohesion and shall provide the organisational (e.g. safe procedures) and legal framework (e.g. insurance coverage for time on mission) for individual spontaneous volunteers as well as for grassroots initiatives to assist.

# 1-sentence Explanation of your ranking

-----

# Key Recommendation 3 [ ]

When selecting the target group for the organisation and mobilisation concept, operators shall not only think in "hard" operational efficiency parameters easy to be benchmarked (e.g. time to shovel 100 sandbags) but also "soft" parameters such as interpersonal skills relevant for cultural mediation.

# 1-sentence Explanation of your ranking

\_\_\_\_\_

# Key Recommendation 4 [ ]

Even if the willingness to help is temporarily restricted to the aftermath of a disaster, where it is needed most, people who spontaneously volunteered once may be wanting to help again. Thus CM organisations can establish pools of "potential" spontaneous volunteers. This functions best when pre-registering and asking them what kind of contributions they could imagine to make. When establishing structures for managing spontaneous volunteers

<sup>&</sup>lt;sup>107</sup> This principle is described as following by United Nations Industrial Development Organization : « The four-eyes principle means that a certain activity, i.e. a decision, transaction, etc., must be approved by at least two people. This controlling mechanism is used to facilitate delegation of authority and increase transparency ». Available at: <a href="http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html">http://www.unido.org/en/overview/for-member-states/change/faq/what-is-the-four-eyes-principle.html</a>

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	137 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



don't mix up these activities with your recruitment activities for regular CM volunteers. Better see spontaneous volunteers as additional flexible "time donation". If you proactively try to persuade them to become regular volunteers this can lead to unease on side of the volunteers.

#### **1-sentence Explanation of your ranking**

\_\_\_\_\_

# Function 4: "Crisis Communication: From Crisis Managers to Citizens (public)" []

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

# Key Recommendation 1 [ ]

In cases, where openness of the communication process cannot be put into practice because, e.g., it affects other core values such as data protection, crisis communicators shall make sure to explain the need and benefit of such tools, helping the public to decide whether they want to use this tool.

# 1-sentence Explanation of your ranking:

\_\_\_\_\_

# Key Recommendation 2 [ ]

Technical solution providers for communication tools from CM to population, shall ensure that the amount of information that is shared is scalable but very clear and understandable so the population doesn't have the feeling lacking information about the "bigger picture" or some population groups are locked out of the communication process. Regarding information – the content – what to communicate is quite stable and there is a common understanding on preparedness measures, guidelines and tips. The means – the how to communicate differs and may be the key to a better-prepared community, which is to be evolved together between disaster management professionals and media experts.

#### 1-sentence Explanation of your ranking

Document	D840.21 – A gui	N840.21 – A guide assessing unintended societal impacts of different CM Page:					
name:	functions – Vers	Unctions – Version 1 Page:					
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# Key Recommendation 3 [ ]

Strive for the highest ethical standards when communicating with the public during or after a crisis. Any damage to the political reputation of the CM organization can be hard to restore.

\_\_\_\_\_

1-sentence Explanation of your ranking

\_\_\_\_\_

# Key Recommendation 4 [ ]

Ensure that the communication to the public takes account of cultural and gender differences, and that e.g. crucial messages are given in the most relevant languages. Take account of all societal groups when communicating.

1-sentence Explanation of your ranking

\_\_\_\_\_

# Function 5: "Crisis Communication: Media & Policy communication" (subcategory) [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

# Key Recommendation 1 [ ]

Joint trainings between responsible crisis communicators and media stakeholders contribute to the openness and transparency of the communication process and a better mutual understanding. Ensure that functioning cross-organizational and cross-border coordination mechanisms are in place in order to avoid non-harmonized or even conflicting messages through different channels or in different countries.

# **1-sentence Explanation of your ranking:**

# Key Recommendation 2 [ ]

Unless there are good reasons for it, withholding information in the media should be avoided – the best strategy for disaster managers is generally communicating and acting truthfully to avoid sending mixed messages. In a cross-sectoral or cross-border crisis, a coordinated media

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	139 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



communication strategy is important to avoid mixed messages, confusion and erosion of trust.

**1-sentence Explanation of your ranking** 

-----

# Key Recommendation 3 [ ]

Make sure that the messages that are being sent through the media or in policy related communication, take into account and respect the full diversity of the society, e.g. cultural groups and gender differences. Enable communicators to select media channels and frame messages considering socio-cultural factors such as language, language proficiency, gender, nationality, ethnicity, class, age and/or physical limitations.

1-sentence Explanation of your ranking

\_\_\_\_\_

# Key Recommendation 4 [ ]

Respect the sources of information during a crisis as these could be particularly vulnerable, and follow the relevant data protection legislation when it comes to collecting or sharing personal data. Always ensure conformity with European data protection legislation and rights.

1-sentence Explanation of your ranking

-----

# Function 6: "Crisis Communication: From the Citizens to Crisis Managers" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

# Key Recommendation 1 [ ]

Limit the amount of data that is being collected. Apply the principle of data- minimization to collect only necessary and suitable information- of a proportional size.

# 1-sentence Explanation of your ranking:

Document	D840.21 – A gui	de assessing uninter	140 of 159				
name:	functions – Vers	sion 1					
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



# Key Recommendation 2 [ ]

When collecting personal data from the public, it is very important that the privacy of the individuals from whom the data is collected is being respected. And that safeguards (some sort of censorship or screening) are taken to prevent pictures being posted which are violating in one way or the other.

1-sentence Explanation of your ranking

\_\_\_\_\_

\_\_\_\_\_

# Key Recommendation 3 [ ]

Encourage different societal groups to make use of the communication tool, or consider alternative measures to ensure diverse input from the public.

1-sentence Explanation of your ranking

\_\_\_\_\_

# Key Recommendation 4 [ ]

Be careful not to base the deployment of resources entirely on self-reported information from the field, but rather use it as a supplement to more traditional crisis management information channels such as information form first responders or volunteers.

# 1-sentence Explanation of your ranking

\_\_\_\_\_

Function 7: "Identification & Awareness: Gap Analysis for Community Resilience" [ ]

These are the key recommendations for this particular function. *Please rate how well your* solution complies with them: 1 (not at all) to 10 (maximum attention paid). *Please explain* why you ranked your compliance with the recommendations as you did.

# Key Recommendation 1 [ ]

From the various gaps you will reveal, identify and rank the *key gaps* to be covered in order to avoid over-engineering CM and creating unease. For any key gap, provide for a strategy to

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	141 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



close such gaps with a clear assignment of responsibilities, as well as definitions and delimitations of related tasks. If you share knowledge about gaps publicly ensure that for any gap a related strategy to close this gap is communicated in a transparent manner.

1-sentence Explanation of your ranking:

#### -----

# Key Recommendation 2 [ ]

Design gap analysis methodologies that rely on comprehensible and transparent parameters to ensure that they are reproducible. When putting gap analysis methodologies to use, ensure to have mechanisms in place that identify potentially hidden political or commercial agendas. For example, define a set of indicators that determine political and commercial influence on gap analysis to ensure protection against the misuse of gap analysis methods or a focus on irrelevant gaps. When conducting the analysis, use a broad variety of data sources to avoid producing skewed results. Ensure to repeat gap analyses regularly in order to take account of changes and assist in creating sustainable solutions. Include mechanisms to challenge each step in the gap analysis to check whether it speaks to the overall goal.

1-sentence Explanation of your ranking

# Key Recommendation 3 [ ]

Conduct gap analyses only at cross-border level if goals, instruments and methodologies have been synchronized before and both parties agree to the analysis. If international cooperation for gap analysis is needed due to specific cross-border scenarios, ensure to coordinate with the relevant partners beforehand, potentially during exercises. Create common standards, variables and methodologies for gap analyses.

1-sentence Explanation of your ranking

-----

# Key Recommendation 4 [ ]

Make sure the team defining parameters for gap identification is diverse. This does not only refer to the inclusion of analysts with a cultural and gender-sensitive perspective, but also relates to any kind of professional diversity needed for a thorough gap analysis. Time permitting, run a pre-analysis identifying those players and representatives who know best about gaps in a specific area. Include them into the identification of gaps. Define the

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	142 of 159
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0					



parameters of gaps under the participation of those groups for which the analysis' theme will be most relevant.

# 1-sentence Explanation of your ranking

------

# Function 8: "Identification & Awareness: Situational Analysis & Impact Assessment" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

#### Key Recommendation 1 [ ]

Make sure to clearly define the scope of the data that is supposed to be collected via airborne sensors, social media or apps. Clearly mark these methods and tools as something that belongs to the crisis management context, for example by marking UAVs with the logo of the organization that uses them. If possible, always contextualize the use of airborne sensors through brochures and information campaigns before usage. Organize information campaigns in advance about the why and how of data collection (e.g. how it will be used) and collect informed consent of populations wherever possible.

#### 1-sentence Explanation of your ranking

-----

# Key Recommendation 2 [ ]

Clarify the kind of data to be collected for situational analysis long before related tools are being put to use. Describe the limits of the data that you collect. Devise a clear code of conduct for how this data is being used and protected from misuse. Dedicate resources to the identification of deceptive information. Share the code of conduct and all protective measures with the people whose data you are likely to collect. If you collect data for situational analysis via apps and mobile phones, devise a clear and easy-to-understand consent form that people will read before they provide data. Avoid implementing such consent forms directly on the phone because people give easily consent on the phone without reading the terms of conditions. If you do implement consent forms to be signed directly on the phone, provide for a step-by-step consent form rather than a very condensed text. Communicate the added value of crowd-tasking and clarify where the responsibilities to collect information lie.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	143 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



1-sentence Explanation of your ranking

# Key Recommendation 3 [ ]

If you foresee the usage of social media and apps for reporting, avoid asking for information that may lead to the identification of the sharing person. Protect the networks and platforms that collect and aggregate information for situational analysis according to highest standards. Devise clear guidelines for sharing information about bottlenecks and vulnerabilities, and limit the amount of people who have access to aggregated information and results to those parties which are strictly necessary.

# 1-sentence Explanation of your ranking

\_\_\_\_\_

# Key Recommendation 4 [ ]

When developing a crowd-tasking mechanism, include not only an informed consent form, but in the best case scenario also a code of conduct. This should outline the ethical principles relevant, when sharing information about situations and fellow citizens, in order to inspire a culture of care and solidarity and avoid negative effects on social cohesion.

# 1-sentence Explanation of your ranking

-----

# Function 9: "Identification & Awareness: Early Warning, Risk Analysis, Forecasting" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

# Key Recommendation 1 [ ]

Only send warnings when clear indicators for an imminent crisis exist. Even if the threshold for these indicators is low - to be on the safe side – ensure that the affected populations and recipients of the warning understand these indicators and take them seriously. Once you issue a warning, send as much context information as possible so that receivers of such

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	144 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final


warnings know how to react and take the warning seriously. Give concrete advice on how to react. Through that you ensure the sustainability of such systems.

#### 1-sentence Explanation of your ranking

-----

#### Key Recommendation 2 [ ]

Clarify the responsibilities and accountabilities concerning both the risk assessment procedure, the issuing of warnings and the actual response strategies before making any related public announcement. Identify who is responsible for which part of the process. Clarify lines of communication. If you work with collective models of responsibility, ensure that they can be implemented fairly.

#### **1-sentence Explanation of your ranking**

#### \_\_\_\_\_

#### Key Recommendation 3 [ ]

Communication strategies on risks and early warnings should be honest and transparent. They should include the most feasible extent of information about what is known and what is not known about the future. Risk analyses should furthermore include explanatory information about the solutions: why are specific solutions best suited to address a specific risk? Methodologies for conducting risk analysis and related communication standards need to be developed in a transparent manner, identifying the context information that is necessary for a recipient to know in order to react.

#### 1-sentence Explanation of your ranking

\_\_\_\_\_

#### Key Recommendation 4 [ ]

If possible, make a thorough screening of all societal groups to ensure that risk assessment solutions take account of diverse risk perceptions and needs across society. Plan risk communication and early warnings while taking all potential audiences, their risk perceptions and the specific risks they face into consideration. Organize communication and media strategies that allow for specific risk communication and early warnings for different groups.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	145 of 159	
Reference:	D840.21	D840.21 Dissemination: PU Version: 3.0						



Reflect whether the formulation of the alert can have any negative impact on a particular group, area or activity.

#### **1-sentence Explanation of your ranking**

-----

#### Function 10: "Identification & Awareness: Identification of critical infrastructure" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

#### Key Recommendation 1 [ ]

Choose resilience indicators and measures for contingency plans that strengthen resilience without causing too many follow-up measures. Reflect on the influence that commercial or political actors may have on the selection of resilience indicators.

1-sentence Explanation of your ranking

-----

#### Key Recommendation 2 [ ]

Make a screening of all relevant actors to CM. Ensure that the partners that are responsible for core infrastructures in the city are part of the process of identifying resilience indicators. Carrying this out as a democratic and inclusive process will create an ownership that can be beneficial also in the long run.

1-sentence Explanation of your ranking

-----

#### Key Recommendation 3 [ ]

Reflect upon and steer the influence of political agendas on contingency planning, keeping in mind the basic needs and principles that exist in society (almost) regardless of political or commercial influence. The selection of resilience indicators should reflect whether they are prone to political or commercial misuse.

#### **1-sentence Explanation of your ranking**

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	146 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



#### Key Recommendation 4 [ ]

Information about the vulnerability and resilience of logistical domains and infrastructure can be confidential. Those who assess key functions, vulnerabilities and indicators need to ensure that they do not infringe upon legality and only obtain information about (potentially private) infrastructures and processes with consent. Keep a clear overview of the relevant approvals and requirements to ensure compliance with relevant data protection regulations, in order to protect privacy in case there is personal data involved. For secret of confidential data, particular rules may apply, and the local Data Protection Authority should be consulted.

**1-sentence Explanation of your ranking** 

-----

\_\_\_\_\_

#### Function 11: "CM Coordination, Command & Control: Tasking and resource management" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

#### Key Recommendation 1 [ ]

Make sure that the distribution of human and financial costs and resources are fairly distributed, especially when planning or developing solutions for resource management or contingency efforts with low-income countries. If the distribution of resources and/or preparation of contingency plans involve (personal) data collection, these data have to be protected according to relevant national legislation. Inform the public accordingly when contingency plans or similar are tested through CM exercises, and disseminate the achievements and lessons learnt from them.

#### **1-sentence Explanation of your ranking**

\_\_\_\_\_

#### Key Recommendation 2 [ ]

Avoid complete dependency on a certain technological solution, e.g. for coordinating the distribution of resources during a crisis. Make sure that the contingency plan takes account

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	147 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



for the fact that certain technologies can fall out, and that there are alternative ways of e.g. informing both the population and the crisis managers in case of such an occurrence.

1-sentence Explanation of your ranking

#### -----

#### Key Recommendation 3 [ ]

Tools and measures to improve the distribution of resources and to manage the supply chain (whether human, material or financial) need to adhere to both national and international legislations, (for the UAV e.g. in terms of data protection). Pay attention to grey areas and legal vacuums, particularly when developing and deploying new solutions or tools to be used across borders. When organizing international solutions, seek to create positive spill over effects on international relations by harmonizing regulation.

#### 1-sentence Explanation of your ranking

\_\_\_\_\_

#### Key Recommendation 4 [ ]

Ensure that the resources and content of the supply chain respects the diversity of the target population by taking gender, religious and/or cultural needs and rights into consideration. This could e.g. mean to include hygiene articles suitable for females, and include food that is suitable for all relevant religions. Ensure that the distribution of resources does not discriminate against any social groups in a way that can be seen as denying the dignity of people.

1-sentence Explanation of your ranking

\_\_\_\_\_

#### Function 12: "Information Management: Collection & Storage of Data" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well* 

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	148 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.

#### Key Recommendation 1 [ ]

The collection, storage and processing of data and information facilitated by the DRIVER solutions needs to uphold the data protection regulations to protect the privacy of those whose data may be collected. Data collection in a so-called open society adheres to the principles of privacy, data protection and integrity. It follows a process that is suitable to the cause and proportional to the task. This means that solution developers need to ask if the data collection is really necessary, and if those data are best suited to fulfil the given function. Are there alternatives to collecting personal data (in particular *sensitive* data), or can it be encrypted or anonymized? Seize opportunities to demonstrate best practice in terms of data protection, for example by consulting the local Data Protection Authority. To minimize potential infringements and to increase the social acceptability of the CM solution, consider embedding privacy friendly design choices and privacy friendly defaults in the data collecting tools, as part of a "Privacy-by–Design"- approach.

#### 1-sentence Explanation of your ranking

\_\_\_\_\_

#### Key Recommendation 2 [ ]

The risk for misuse of collected data needs to be actively counteracted in all phases of the CM solution's development and deployment. To minimize the risk of misuse, make sure to only collect the data you need for the predefined purpose and adhere to central data protection principles such as not reusing collected data uncritically. Have mechanisms for secured storage of the collected data in place. This can include locks and other physical security measures, but also password protection or encryption of data. Do not store data for longer than necessary. Regarding the application of new technology and unexplored legal fields (creating new vulnerabilities) for data collection, local Data Protection Authorities should be consulted when necessary.

#### 1-sentence Explanation of your ranking

#### Key Recommendation 3 [ ]

Data collection and storage must happen in a way that does not infringe upon the social cohesion of the population. Avoiding the collection of data that can create suspicion (e.g. if it

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	149 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



is seen as unjust or as fostering inequalities by focusing in particular on a certain ethic group without a clear reason), can happen by e.g. ensuring proportionality in the data collection, and by communicating this in an open and transparent manner to the individuals from whom the data is collected. The argumentation for the choices made should be as transparent as possible, and the data collected should be proportional to the case, e.g. not include more sensitive data than necessary. When relying on data collecting mechanism that require certain equipment (such as a cell phone or a computer), compensate for the fact that not all members of society have access to such equipment (for example due to low/ high age, loss of income, homelessness, etc.). Marginal groups should be equally included in the CM activity that includes the data collection as other groups.

#### 1-sentence Explanation of your ranking

# Key Recommendation 4 [ ]

When planning the CM activity, make sure that those subjects you collect data from are diverse, and selected on an equal and fair basis. Accounting for diversity concretely means including variables such as language, ethnicity, gender, culture and religion in the selection of participants or volunteers for the CM activity. This will ensure a more broad and accurate feedback, in addition to fostering opportunities for enforcing solidarity and diversity.

1-sentence Explanation of your ranking

\_\_\_\_\_

#### Function 13: "Information Management: Facilitating Data Processing " [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

#### Key Recommendation 1 [ ]

When planning CM measures, consider if there is a real need for facilitating the processing of data in the planned scale, and reflect upon whether the action is leaving you more vulnerable by creating more technology dependency. If this is hard to avoid, have backup solutions available, e.g. alternative ways of ensuring that the collected data is being protected according to relevant regulations. The general principle is to minimize data processing wherever possible, and to only collect the data that is needed for the activity.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	150 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



When designing the measures that lead to the processing of data, and to ensure the efficiency of the procedure, Consider if a risk- or Privacy Impact Assessment (PIA) could be useful to tailor the solution (e.g. by minimizing the amount of personal data that is collected for processing). Minimize secondary insecurities and challenges like function creep, misuse and the creation of new vulnerabilities by making the limitation of data processing a (built-in) feature of the solution, for example through making a PIA mandatory. Working with regional and international organizations to create platforms for facilitating the exchange of information (or other means of data processing) can be important to strengthen resilience<sup>108</sup> [50] and also push progress on the CM area.

#### 1-sentence Explanation of your ranking

#### Key Recommendation 2 [ ]

The facilitation of data processing largely falls under the general rules for data protection, and should adhere to the basic principle of legality. This includes acknowledging that although the data collection may be legal, the processing may not be- and vice versa. Especially if the processed data are sensitive data, particular measures and requirements may apply (depending on national regulation). To avoid lowering trust between partners facilitating data exchange or other forms of data processing, ensure that the process is transparent, open, and adhering to all relevant legal data protection frameworks. Be clear and transparent when communicating with the individuals from whom the data is collected about the processing of data, stating why it is necessary, and why it is suitable for pursuing the given objective. When facilitating data processing, in terms of sharing data between two or more partners (or the public), ensure that involved actors have the opportunity to voice their questions and concerns. This can enforce trustful relationships both in the short and in the long term, and may even have positive spill-over effects onto other domains of the cooperation. Consider also if the data processing tools are disproportionate in relation to the interests affected. The facilitation should include possibilities for encryption or anonymization of personal data whenever possible, even if this means that the possibility of the individual to withdraw (their data) from the activity or to access their data, disappears.

#### 1-sentence Explanation of your ranking

http://ec.europa.eu/echo/files/policies/prevention\_preparedness/DRR\_thematic\_policy\_doc.pdf. Retrieved 12 November 2015.

Document	D840.21 – A gui	de assessing uninter	e assessing unintended societal impacts of different CM Page					
name:	functions – Vers	sion 1						
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final	

<sup>&</sup>lt;sup>108</sup> As described e.g. in European Commission (2013): Disaster Risk Reduction. Increasing Resilience by Reducing Disaster Risk in Humanitarian Action.



#### Key Recommendation 3 [ ]

Make sure that the data processing solution does not facilitate data processing that favours one social group over another, unless there is a good cause for it (such as adjusting for lowincome countries). Such reasons should be communicated in a clear and transparent manner (cf. *transparency*). Ensure also that the data processing tools adhere to data protection legislation, and that they facilitate making claims of privacy such as exercising the data access right, which is a measure intended e.g. to create transparency in the data processing, and make it easier for the individual to know how their data is being processed. Developing and streamlining this practice can, especially in the long run, help fostering solidarity as it is an action that produces good standards in society.

#### 1-sentence Explanation of your ranking

## Key Recommendation 4 [ ]

Make sure that the data processing is based on ethically acceptable methods, e.g. data protection regulations, in order to enforce the accountability of the data processor(s) by valuing core principles for good governance. The method or tool for facilitating data processing (such as data exchange), should include a mechanism for informing the individuals from whom the data is collected about how her personal data is taken care of in the process. To avoid negative standardization of data processing routines, planning- and impact assessments can verify whether the process. Following particularly good routines or mechanisms for ensuring legal compliance (and taking better care of individual privacy) contributes to a (positive) standardization or a normalization of best practice.

#### 1-sentence Explanation of your ranking

#### Function 14: "Information Management: Analysis & Evaluation" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

#### Key Recommendation 1 [ ]

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	152 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



Make sure that data analysis happens with a clear and predefined purpose, meaning that the use of it is controlled and specialized to the aim. Make sure that the data is only put to use for the purpose it was collected for, to uphold or strengthen the integrity and political reputation of the data controller, and to minimize the risk of function creep. To enforce trust, set rules that limit the role of the data controller or the legally responsible actor, e.g. to ensure that the data is secure with regards to confidentiality, integrity and accessibility.

#### 1-sentence Explanation of your ranking

#### Key Recommendation 2 [ ]

The purpose for data analysis or evaluation must be clearly communicated. When analysing personal data, the individuals from whom that data was collected must be made aware of the full use of the data, and their claims and comments should not be re-interpreted in a different context later. For example, when collecting data for one purpose, e.g. gather information about the movement patters of residents in a certain area for CM logistics purposes, this data cannot be reused in order to analyse their health status. To enforce trust, and to minimize the potential for misuse and suspicion, rules should be set to limit the role of the data controller or the legally responsible actor. Consider setting goals like the authentication of system users, the use of encryption and decryption, deletion of data in case of system failure (especially for sensitive data), and other goals to ensure trustable and secure data processing. Such measures can foster trust in the more general sense, both from the user's perspective and from the perspective of the individuals from whom the data is collected.

#### 1-sentence Explanation of your ranking

#### Key Recommendation 3 [ ]

In addition to not collecting and analysing more data than you need for the particular purpose (and to not reuse this data uncritically), the process of doing data analysis and evaluation needs to be transparent and as open as possible in order for the involved actors to experience that their data is being processed in a rightful manner, and to ensure that the accountability of the data processor is maintained. When relevant, ensure that the analysed

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	153 of 159		
Reference:	D840.21	Dissemination:	V840.21 Dissemination: PU Version: 3.0						



data is made up of contributions from a wide range of diverse societal groups, as equality and freedom of thought are examples of traits of an open society<sup>109</sup>.

#### 1-sentence Explanation of your ranking

\_\_\_\_\_

#### Key Recommendation 4 [ ]

Plan the analysis and evaluation process adhering to high ethical and societal principles (such as privacy) in data analysis to enforce the accountability and integrity of the actor(s). Aim for best practice in the data analysis, including the encryption of data when possible, and by only collecting or drawing out the data you need for doing the particular analysis.

1-sentence Explanation of your ranking

\_\_\_\_\_

#### Function 15: "Information Management: Communication between first responders" [ ]

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

#### Key Recommendation 1 [ ]

Minimizing the amount of data that is being exchanged will automatically minimize the risk of misuse of the data. Unnecessary data exchange should be avoided, and the risks and threats should be evaluated, to minimize the risk of function creep. The rules for data protection need to be carefully upheld in order to limit or prevent potential misuse of the information. Ensure that the receiving partner has a satisfactory level of protection for the exchanged data, and if in doubt, aim for complying with the legislation or regulation with the highest requirements.

#### 1-sentence Explanation of your ranking

<sup>109</sup> The concept of the open society was originally brought forth by Henri Bergson. See for example Henri Bergson, Les Deux Sources de la morale et de la religion, Félix Alcan, 1937 [1932], pp. 287–343. Available at :

https://fr.wikisource.org/wiki/Les\_Deux\_Sources\_de\_la\_morale\_et\_de\_la\_religion/Chapitre\_IV. It is commonly discussed in various academic disciplines, such as criminology and political science.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	154 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



#### Key Recommendation 2 [ ]

Ensure conformity with European data protection regulations when implementing communication tools for communication between crisis managers (both ICT – and nonelectronic based) and relevant national regulations. As policy maker you shall clearly set out safeguards to protect personal data, such as setting limits for what the communication technology will be used for, to minimize the risk of misuse. Access to databases must be limited both practically and legally. Solutions for encryption should be considered. This means that the very process and principle of exchanging information and data needs to be deemed the best solution for the issues at stake, a reflection which would include evaluating the applicability of the data exchange. For sustainable data sharing, especially on the European level, creating a constructive culture of data sharing can include, for example, developing financial and legal frameworks by working together with relevant partners and organizations. In addition to that, developing sustainable funding solutions for such initiatives is crucial<sup>110</sup> [53]. Ensure that the data exchange process is open and transparent (as far as it is possible and reasonable), i.e. let the individuals from whom the data is collected know in advance to what extent their data will be exchanged and shared.

#### 1-sentence Explanation of your ranking

\_\_\_\_\_

## Key Recommendation 3 [ ]

Data exchange should happen only after a critical evaluation of the integrity of the receiver and after ensuring that the receiver upholds standard routines and regulations for processing the exchanged data. Be aware of this risk when exchanging data with third countries outside the Schengen- or EEA area. For CM professionals, avoid exchanging data with partners that fundamentally conflict with society's common principles, interests, objectives or standards. Ensure that the process happen in a transparent manner, in order to better overlook that the interests of the different partners are accounted for. Make sure the data being exchanged are representative of the cause, i.e. that it takes, for example, diversity, cultural and gender differences into account.

#### 1-sentence Explanation of your ranking

 <sup>&</sup>lt;sup>110</sup> As explained e.g. by The Alfred Wegener Institute for Polar and Marine Research (ed.): Ten Tales of Drivers & Barriers in Data Sharing. *Setting Course for a Data Sharing Culture*. Brochure of the ODE project (Opportunities for Data Exchange), 2011. <u>http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2011/10/7782\_ODE\_Brochure\_v5.pdf</u>.
Retrieved 11 November 2015.

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	155 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



#### Key Recommendation 4 [ ]

Make sure that the data exchanging process happens according to relevant legal frames. Ensure that the data exchange is proportional to the case at stake, that it is suitable to solve the issue, and that it is necessary. The latter is important because the exchange can increase the risk of misuse or function creep. Make sure that the exchange happens in a transparent manner. This includes making sure that all relevant data protection regulations and laws are being followed. Especially when exchanging personal data with other actors, clearly state the limitations of the data processing already before the data collection phase in order to limit the feeling that the individuals from whom that data was collected are subject to unjust control. If possible, seize opportunities to establish best-practice rules for data exchange in your company or organization, and investigate how your local Data Protection Authority can be of assistance in such a process. Consider building on networks that might emerge from the data exchange process. These can be beneficial in other areas of the crisis management operation as well.

#### 1-sentence Explanation of your ranking

\_\_\_\_\_

#### Function 16: "Competence- Building for Decision- Makers and Organizations" []

If you have crossed off this function as relevant to your solution, please continue reading here. Below are the key recommendations for this particular function. *Please rate how well your solution complies with them: 1 (not at all) to 10 (maximum attention paid). Please explain why you ranked your compliance with the recommendations as you did.* 

#### Key Recommendation 1 [ ]

When putting a competence-development framework to use, ensure to identify all relevant stakeholders first. Reflect on their respective positions and stakes and ensure that everyone's position is taken account of when identifying and discussing competences, gaps in competences and new ways of building competences to foster a culture of trust.

#### **1-sentence Explanation of your ranking**

#### Key Recommendation 2 [ ]

When designing quantitative decision-making models, evaluate carefully which decisionmaking parameters can be translated into numeric values and how. Design decision-making

Document name:	D840.21 – A gui functions – Vers	de assessing uninter sion 1	nded societ	al impacts o	of different CM	Page:	156 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



models in which each parameter is clearly defined and its users will have a clear understanding of the results presented to them. Through that, you can control the misuse of decision-making methodologies for unintended political or institutional agenda-setting.

1-sentence Explanation of your ranking

-----

#### Key Recommendation 3 [ ]

Clarify where and how a decision-making methodology provides for rationales to take specific decisions. Make these rationales explicit and allow the decision-maker to reflect about the effect that these decision-rationales have on their own accountability when taking such decisions.

1-sentence Explanation of your ranking

-----

#### Key Recommendation 4 [ ]

Devise frameworks as transparent as possible so that they are actionable. Identify the concrete problems to be solved or gaps to be closed and reflect about the different context-factors that influence the respective decision-makers position. At best, decision-making frameworks document and make comprehensible any step of decision-making in order to make decision-making as transparent as possible. Make sure that political agenda-setting is not covertly integrated into decision-making processes by including methodologies that overtly address political agenda setting and priorities.

1-sentence Explanation of your ranking

\_\_\_\_\_

### Feedback & evaluation

To be filled out by everyone.

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					Page:	157 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



3. Do the functions need more updating? *Please describe which additional function/s your solution would cover and why. Keep in mind that a new function would need to be relevant to several solutions:* 

4.	Dic	you read the full assessment per function in D840.21? Yes [ ] No [ ]				
	a)	a) If yes, what was the most helpful part of the assessment?				
		Did you make use of the assessment? Yes [ ] No [ ]				
	b)	If no, why did you not consult the full assessment?				
	[]	I couldn't find it				
	[]	I had no time				
	[ ] The content was too complicated					
	[ ] The language was too complicated					
	[ ] The assessments turned out to be irrelevant, so I stopped reading them					
	[]	Other:				
	De	pending on your choice above, what measures do you suggest for a revision?				

\_\_\_\_\_

5. In the process of working with your solution, which ones were the most relevant criteria for your work? *Please choose five criteria, and rank from 1-5 (1 is least relevant and 5 is most relevant)* 

Document name:	D840.21 – A guide assessing unintended societal impacts of different CM functions – Version 1					Page:	158 of 159
Reference:	D840.21	Dissemination:	PU	Version:	3.0	Status:	Final



CRITERIA	YOUR RANKING (1-5)
Unease - Calmness	
Suspicion - Trust	
Misuse - Protection	
New Vulnerabilities - Progress	
Technology Dependency - Flexible Solutions	
Function Creep - Specialized and Controlled Use	
Sustainability	
Accountability	
Transparency	
Integrity	
Negative – Positive Standardization	
International Relations	
State-Citizen-Relationship	
Political Reputation	
Social Cohesion & Solidarity	
Participation	
Diversity	
Open - Control Society	
Cultural & Gender Sensitivity	
Suitability, Necessity & Proportionality	
In/justice & In/equality	
Dignity /Autonomy	
Non-Discrimination	
Privacy & Data Protection	
Freedoms & Protest	

Figure 3: SIA Criteria

6. In the process of working with your solution, did you identify new criteria, negative impacts or opportunities that were not yet part of the given assessments? *This feedback is very valuable for the revision of the SIA framework, please indicate below.* 

Document<br/>name:D840.21 - A guide assessing unintended societal impacts of different CMPage:159 of 159Reference:D840.21Dissemination:PUVersion:3.0Status:Final

\_\_\_\_\_