EmerGent

EMERGENCY MANAGEMENT IN SOCIAL MEDIA GENERATION

Deliverable 7.3

Guidelines to increase the benefit of social media in emergencies

Final

Alexis Gizikis, Tony O'Brien & Iratxe Gomez Susaeta (EENA), Matthias Habdank & Annika Schubert (UPB), Christian Reuter & Marc-Andre Kaufman (USI), Joe Cullen (TIHR), Andrew Muddiman (OCC), Mattia Perruzza & Uberto Delprato (IES)

May 2017

Work Package 7

Project Coordinator

Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme

for Research and Technological Development

COOPERATION

SEC-2013.6.1-1: The impact of social media in emergencies

Distribution level	Public
Due date	31/05/2017 (M38)
Sent to coordinator	29/05/2017
No. of document	D7.3
Title	*Guidelines to increase the benefit of social media in emergencies*
Status & Version	*Final*
Work Package	*7: Guidelines, Dissemination, Exploitation and Ethics*
Related Deliverables	*D2.2, D2.3, D2.4, D2.6, D2.7, D3.1, D3.2, D3.3, D3.5, D3.6*
Leading Partner	*EENA*
Authors	*Alexis Gizikis, Tony O'Brien, Iratxe Gomez Susaeta, EENA* *Matthias Moi, Annika Schubert, UPB* *Christian Reuter and Marc-Andre Kaufman, USI* *Joe Cullen, TIHR* *Andrew Muddiman, OCC* *Mattia Perruzza, Uberto Delprato, IES*
Reviewers	*Dieter Nuessler, FEU*
Keywords	*Social media for emergency management, guidelines, social media strategy, policy, ICT Tool for social media analysis, VOST*

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608352.

Table of contents

List of Figures 4

List of Tables 5

List of Abbreviations 6

1 Introduction 8
1.1 Abstract 8
1.2 Purpose of the document 8
1.3 Target audience 8

2 Foreword 9
2.1 Purpose of the guidelines 9
2.2 Who the guidelines are for? 9
2.3 Structure of the guidelines 11
2.4 Methodology used to develop the guidelines 12

3 Preliminary considerations 13
3.1 Potentials and opportunities of using social media in emergencies 13
3.1.1 Potentials of using social media 13
3.1.2 Opportunities for using social media in emergency management 13
3.2 Risks associated with using social media in emergencies 15
3.3 Organisational and professional factors inhibiting the use of social media 15
3.4 Lessons learnt from organisations that experimented with social media 16

4 Guidelines for emergency services & public authorities 17
4.1 Prepare to start using social media 17
4.1.1 Consider the legal implications 17
4.1.2 Consider the needs in human and financial resources 18
4.1.3 Prepare a social media strategy 19
4.1.4 Clearly communicate the social media strategy and provide staff training 23
4.1.5 Use of ICT tools for social media monitoring and analysis 25
4.1.6 Use of smartphone apps for direct communication (A2C and C2A) 26
4.1.7 Plan the next steps to start using social media 29
4.2 Before an emergency 30
4.2.1 Provide information about your organisation, its operations and emergency prevention and preparation 31
4.2.2 Raise awareness on the use of social media 32
4.2.3 Use of ICT tools for social media monitoring and analysis 34
4.2.4 Team up with other groups and organisations 35
4.2.5 Publish alerts for the risk of an upcoming emergency 37
4.3 During an emergency 37
4.3.1 Understand how citizens use social media during emergencies 38
4.3.2 Establish communication with the public 41
4.3.3 Request information from the public 43
4.3.4 Use of ICT tools for social media monitoring and analysis 44
4.3.5 False information during emergencies 45
4.3.6 Collaborate with emergent group initiatives 49
4.4 After an emergency 50
4.4.1 Continue the communication with the citizens 50
4.4.2 Evaluate your social media use during the emergency 50

5 Guidelines for citizens 52
5.1 General Aspects while using social media 52
5.2 Before an emergency 52
5.3 During an emergency 52
5.4 After an emergency 53
6 Annex I: Methodology for the derivation of the following guidelines 54
6.1 Review of existing guidelines 55
7 Annex II: Data Protection and Privacy Guidelines for Processing Social Media Data 58
7.1 Overview 58
7.1.1 Target Audience 58
7.1.2 Document Organisation 58
7.1.3 Disclaimer 59
7.2 Responsibility 59
7.2.1 Project responsibility 59
7.2.2 Who do you answer to? 60
7.3 Is what you are proposing lawful? 61
7.3.1 Consent 61
7.3.2 Transparency 61
7.3.3 Special Categories of Personal Data 62
7.4 Data rights of the citizen 62
7.4.1 Subject Access Request 62
7.4.2 Right of Erasure 63
7.4.3 Data Portability 63
7.5 Project controls 63
7.5.1 Data protection officer 63
7.5.2 Privacy impact assessment 64
7.5.3 Continuous monitoring 64
7.6 Infrastructure controls 65
7.6.1 Privacy by design 65
7.6.2 Codes of Conduct 66
7.6.3 Breach handling 67
7.6.4 SAR handling 68
8 Annex III: Publication and dissemination of guidelines 70
8.1 How to publish guidelines 70
8.1.1 Full-text version of the guidelines (printed and digital) 70
8.1.2 Hand-outs (printed and digital) 71
8.1.3 Poster 74
8.1.4 “Interactive” internet pages 77
8.1.5 Creating videos 82
8.1.6 Including guidelines in existing “emergency apps” 84
8.1.7 Seminars, information events and workshops 84
8.1.8 Final view on the publication of guidelines 85
8.2 Where to publish guidelines 85
References 87

List of Figures

Figure 1: Overview of the guidelines structure and the topics presented within each main section. 11
Figure 2: Infographic “Social media & emergencies: the basics of how your smartphone can help you”, source: EENA [WWW42] 33
Figure 3: Examples from ES and public authorities using hashtags to report false information Left: Police in Germany, source: [WWW37] - Right: Police in Spain, source: [WWW38] 47
Figure 4: Tweet of the French Ministry of Interior during the Nice attack on 14 July 2017 responding to several tweets about an ongoing hostage situation, source: [WWW39] 47
Figure 5: Tweet of the French government during the Nice attack on 14 July 2017 suggesting to relay messages only from official accounts, source: [WWW40] 48
Figure 6: Underlying principles and objectives for the development of the EmerGent guidelines 54
Figure 7: Methodology for the development of the EmerGent guidelines 55
Figure 8: Risk Assessment for each identified hazard 64
Figure 9: Data breach management 68
Figure 10: Page 1 and 5 from [ARC10] as example for a handout 72
Figure 11: [BTHW11] as example for a handout 73
Figure 12: Example QR-Code [WWW04] 74
Figure 13: Poster “15 ‘Dos’ for Pinterest” [WWW02] 75
Figure 14: Poster “Before you post: THINK” [WWW03] 76
Figure 15: Motives of the posters for the campaign for alcohol prevention from the BZgA [BZgA16] 77
Figure 16: Overview COSMICs preparation of their guidelines for public authorities [COSM14a] 78
Figure 17: Detailed view on COSMICs preparation of their guidelines for public authorities [COSM14a] 79
Figure 18: Overview COSMICs preparation of their guidelines for citizens [COSM14b] 80
Figure 19: Detailed view on COSMICs preparation of their guidelines for citizens [COSM14b] 81
Figure 20: YouTube-Video “Mr. Bean goes online” by Tchibo [Tchi11] 82
Figure 21: YouTube-Video “Employee Social Media Guidelines” by Great-West Life [GWL15] 83
Figure 22: YouTube-Video “Social Media Guidelines at Linde” by Linde [Lind13] 83
Figure 23: Overview how to disseminate guidelines 86

List of Tables

Table 1: Possible uses of social media in different phases of the Emergency Management Cycle 14
Table 2: List of guidelines for the use of social media in general 55
Table 3: List of guidelines for the use of social media in crisis management 56
Table 4: Overview of Data Protection and Privacy Guidelines for Processing Social Media Data 59
Table 5: Possibilities how to release guidelines 70

List of Abbreviations

Abbreviation	Expression
A2C	Authorities to Citizens communication flow
BBK	Federal Office for Civil Protection and Disaster Assistance Germany (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe)
BZgA	Federal Centre for Health Education (Bundeszentrale für gesundheitliche Aufklärung)
C2A	Citizens to Authorities communication flow
COSMIC	Contribution of Social Media in Crisis management
DPO	Data Protection Officer
DPP	Data Protection and Privacy
GDPR	General Data Protection Regulation
EAB	End user Advisory Board
EAC	Ethics Advisory Committee
EENA	European Emergency Number Association
EMC	Emergency Management Cycle
EmerGent	Emergency Management in Social Media Generation
EPRR	EmerGent “Privacy Risk Register”
ES	Emergency Services
EU	European Union
FEMA	Federal Emergency Management Agency
ICO	Information Commissioners Office (UK)
NINA	Emergency Information and News App (Notfall-Informations- und Nachrichten-App)

PIA	Privacy Impact Assessment
SMEM	Social Media for Emergency Management
THW	Federal Agency for Technical Relief Germany (Technisches Hilfswerk)
VISOV	Volontaires Internationaux en Soutien Opérationnel Virtuel
VOSG	Virtual Operations Support Group
VOST	Virtual Operations Support Teams. In France, they are called VISOV (Volontaires Internationaux en Soutien Opérationnel Virtuel)

1 Introduction

1.1 Abstract

This deliverable summarises the findings and conclusions of EmerGent in the form of guidelines for end users for increasing the benefit of social media use during emergencies. It provides a list of recommendations for emergency services and citizens on how to make the most of social media use, explore and benefit from the opportunities offered and take the necessary steps to achieve a smooth and beneficial use of this medium.

The deliverable provides guidelines for emergency services and citizens structured in four main sections:

- Prepare to start using social media, describing all the steps that should be considered by an emergency service to develop a social media strategy and policy
- Recommendations and good practice for using social media before, during and after an emergency.

1.2 Purpose of the document

This deliverable directly contributes to the fourth objective of EmerGent, "O4: Provide officials and the public with guidelines for social media use in emergencies", by documenting the results identified, the knowledge gathered and the conclusion drawn during the research and empirical work in EmerGent. In more detail, the purpose of this deliverable is to communicate the results of EmerGent to its stakeholders in the end user community.

The purpose of the EmerGent guidelines is explained in detail in section 2.1.

1.3 Target audience

The target audiences of this deliverable are:

- Emergency Services (ES), their staff and authorities involved in the emergency management lifecycle
- Communication experts and advisers in using social media for emergency management
- Research teams and working groups in the field of social media for emergency management
- The EmerGent Consortium
- The European Commission

2 Foreword

2.1 Purpose of the guidelines

It is necessary to deal with and to specify the intended purpose of guideline documents before their derivation. The "United States Department of Veterans Affairs" gives the following definition concerning the word "guidelines":

> *"A guideline is a statement by which to determine a course of action. A guideline aims to streamline particular processes according to a set routine or sound practice. By definition, following a guideline is never mandatory. Guidelines are not binding and are not enforced." [USDV16]*

The following guidelines are not and should not be considered as rigid rules. They rather describe the recommendations of the EmerGent consortium on how to communicate in social media and help to decrease the uncertainty with this new, changing and maybe unfamiliar medium [WWW01].

Purpose of the Emergency Services Guidelines:

- provide a concise set of recommendations that will guide ES to develop their own strategy, plan and code of conduct for social media
- explain all the considerations to take into account before and while an ES uses social media and provide examples and good practice to extend and enrich current use
- act as template of the social media strategy under development or revision

Purpose of Citizen Guidelines:

Since citizens' guidelines should be accurately corresponding with the expected use of social media by citizens, as communicated by local or national ES, the EmerGent guidelines for citizens are provided to ES, as an example and template to derive and communicate their own guidelines for citizens.

2.2 Who the guidelines are for?

In our experience in EmerGent, use of social media during emergencies is a diverse topic that at the moment, it almost seems impossible to plan every detail of using social media. In most cases, ES have started experimenting with social media and then found their way through this channel, after the initial considerations and experimentation. In this respect, it is up to you to develop a new social media strategy, or extend your existing, to the fullest possible extent that can offer the most to your operations.

The EmerGent guidelines are provided for ES, their staff and authorities involved in the emergency management lifecycle. The guidelines are intended for all these organisations regardless of their level of experience in using social media. Organisations new in the use of

social media may use the guidelines as a starting point to formulate their own social media policy and dig deeper to customise the policy to their own operational structures and practices.

While developing the guidelines the following three levels of experience have been considered:

1. **Starter**
   ES that are **not** currently **using social media**, or the current use is based on providing general information and advice to citizens
2. **Intermediate**
   ES that currently **use social media to communicate with the public and have developed a draft social media strategy**, even if this is not thoroughly documented or communicated across the organisation
3. **Advanced**
   ES that currently **use social media to communicate with the public during all phases of an emergency and have developed a clear social media strategy**, even if this is not thoroughly documented or communicated across the organisation

Depending on the experience in current use of social media for an ES, readers with different experience will find different information useful. Examples are given below:

If you are a starter in using social media:

Section 4.1 “Prepare to start using social media” will provide a list of considerations that can help to devise your social media strategy. Sections 4.2 “Before an emergency”, 4.3 "During an emergency”, and 4.4 “After an emergency” will be helpful to plan for the future use and should be considered from the beginning to define the level of engagement you wish to achieve. Section 4.1.7 “Plan the next steps to start using social media” is a useful section that outlines a plan to gradually increase the engagement level as you become more experienced.

If you are an intermediate user:

You already have experience in using social media and you have developed your own strategy. You can look at sections 4.1 “Prepare to start using social media” and 4.2 “Before an emergency” to see if there is something that can extend or improve your social media strategy. Since you already communicate with the public in social media, you may consider sections 4.3 "During an emergency”, and 4.4 “After an emergency“ which can be helpful to make the most out of social media during an emergency and to establish a method for evaluating the social media use and make necessary improvements, if needed.

If you are an advanced user:

As an advanced user, you already use social media to actively engage with the public during all phases of an emergency. You have a social media strategy already in place and you most likely have all procedures to operate the strategy, monitor it and improve it. In this case, you may have already gone through mostly everything described in this document. However, since this document is currently up to date with the latest available information and recommendations, as well as it introduces good practice identified in the three-year research for EmerGent, we propose to browse the guidelines and the call out boxes at the end of each section to see if there is something for you. As we value your experience and knowledge gathered in this exercise, we welcome your feedback. Should you believe that these guidelines can be

improved with your experience, please let us know. We are looking forward to including all valuable feedback that can help less advanced users.

2.3 Structure of the guidelines

Two sets of guidelines are included in this document:

- Guidelines for **Emergency Services** (Section 4)
- Guidelines for **Citizens** (Section 5)

Both sets of guidelines are divided in four distinct sections:

- **Prepare** to start using social media
- Use of social media **before** an emergency
- Use of social media **during** an emergency
- Use of social media **after** an emergency

Figure 1 gives an overview of the guidelines structure and the topics presented within each main section.

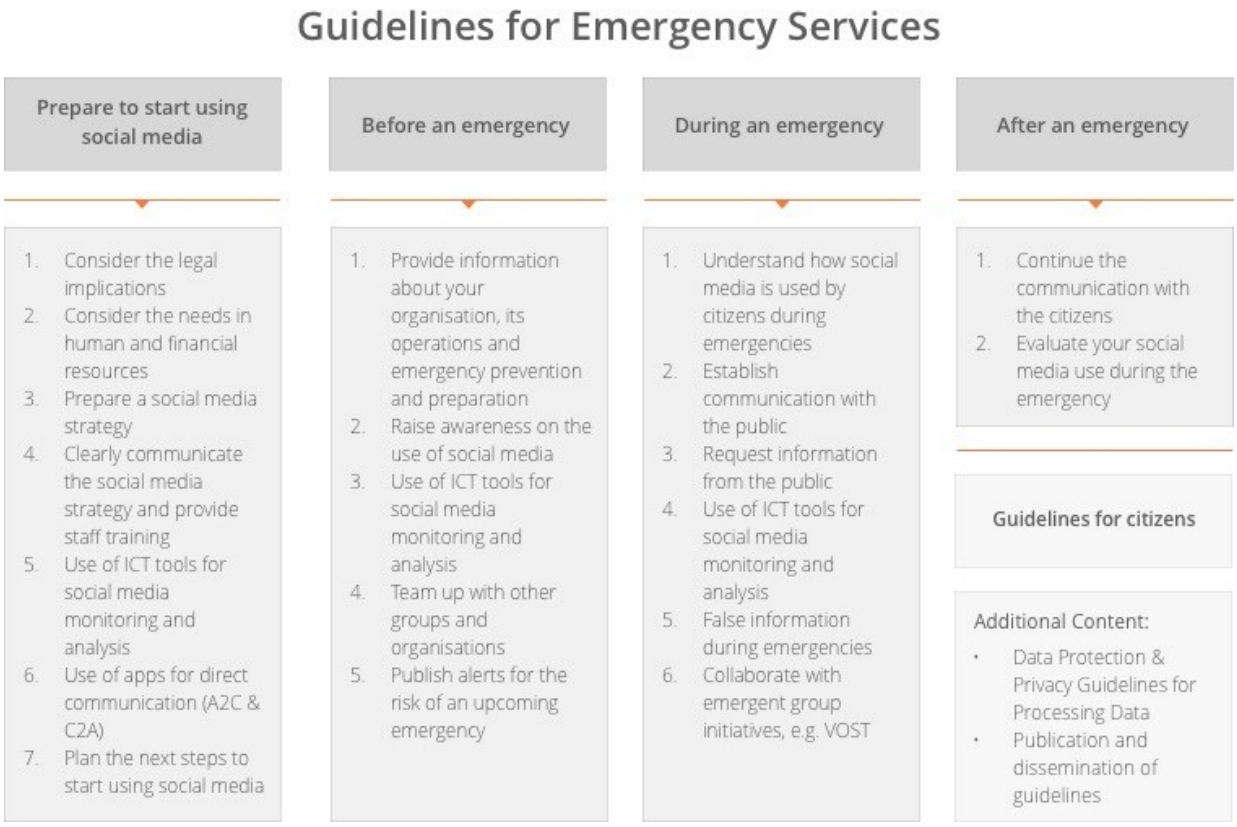


Figure 1: Overview of the guidelines structure and the topics presented within each main section.

Additionally, this deliverable provides:

- Data Protection and Privacy Guidelines for Processing Social Media Data (Section 8)
- An analysis of the method to publicise and disseminate the guidelines (Section 7)

Social media is a relatively new communication channel during crises, with rapidly changing characteristics following its increasing use and the many opportunities it offers for both ES and citizens. These opportunities raise the need for careful attention to ensure the smooth and beneficial operation of social media as a communication tool.

Since this document targets users of social media with all levels of experience, including those just starting to use this channel, we have aimed to explain all details and provide as much information as possible. Achieving this aim resulted in a long and rich document. To also cater for the readers who want a brief overview or the more advanced users, we try to summarise the content in the call out boxes at the end of each section, offering the take away points or some examples with shorter descriptions.

2.4 Methodology used to develop the guidelines

We consider that the methodology used to develop these guidelines should not interrupt the flow of this document for its main target audiences. The methodology is available in the section 6.

3 Preliminary considerations

This chapter deals with different preliminary considerations concerning the derivation of guidelines for the use of social media in emergencies and crisis situations. Based on the purpose of guidelines previously established, it is necessary to consider how social media can help coping with a crisis (section 3.1), the risks and dangers that accompany its use (section 3.2), and lastly, the lessons learnt from organisations that started to use social media (section 3.4).

The integration of social media into existing organisational structures can help to increase the efficiency of emergency management. Especially while digitisation is rising, social media can improve the communication between public authorities and the younger generation. The following sections describe why social media should be implemented and included in daily work and which potentials are arising from their use. Additionally, there are some incurred risks that should be considered before implementing social media. But these risks can be handled if they are known and considered beforehand.

3.1 Potentials and opportunities of using social media in emergencies

3.1.1 Potentials of using social media

- Social media can improve the acquisition and dissemination of information as an additional communication channel [BlKa11]
- Possibility to spread not just text messages but also pictures, video or audio files
- The spreading of information via social media is very fast [BlKa11], accessibility is good
- Alerting via push-messages possible
- Sometimes in a crisis there is a failure of telephone networks but the mobile internet connection is still working or the other way around [PYKI+13]. In this situation, public authorities should use as many channels as possible to stay in contact with citizens [PYKI+13].
- Social media provides the opportunity to receive more local information [BlKa11] e.g. from the local fire department or other affected citizen

Different opportunities to use social media during the phases of the emergency management cycle can be derived from these potentials.

3.1.2 Opportunities for using social media in emergency management

- **Dissemination of warnings:** Fast spreading of warnings among citizen [PYKI+13]
- **Dissemination of recommendations for actions:** Fast spreading of recommendations among the citizens [PYKI+13]
- **Raise the awareness of risks/promote prevention:** E.g. through spreading pictures about possible consequences to encourage preparation [PYKI+13]
- **Spread out status updates:** Fast spreading of information through social media can support provision of real-time updates
- **Request of affected for help/offer help:** Affected people can request help via social media, not affected people can offer help to affected citizens [BlKa11]

- **Evaluation of the situation through authorities (by using information from social media):** E.g. Photos or videos concerning possible needs in affected areas can be evaluated before authorities or help aid organisations are on site [BlKa11]
- **Enabling/engaging a dialog between public authorities and citizens**
- **Aftercare for victims and relatives:** Spreading information about possibilities to handle the event recovery
- **Search missing people:** Fast spreading and generally much sharing of search request for missing people [BlKa11]
- **Coordination of volunteers:** E.g. collaboration of public authorities and self-help communities or effective allocation of volunteers
- **Mobilisation of volunteers:** Mobilisation of volunteers at the scene or donations [BlKa11]
- **Search for witnesses:** In the case of man-made crisis public authorities can request hints from citizens to identify offenders or reconstruct courses
- **Building a relation and trust between authorities and general public**
- **Obtain and provide feedback:** Evaluation of crisis management and processes as well for public authorities as for citizen

Table 1 summarises these opportunities and shows them linked with the pertinent phases of the Emergency Management Cycle and information flows. Detailed information about the Emergency Management Cycle and the different information flows can be found in earlier EmerGent deliverables (e.g. see [CSJD+14] and [RLFM+14]).

Table 1: Possible uses of social media in different phases of the Emergency Management Cycle

	Prevention & preparedness phases			Response phase			Recovery phase		
	C2A	A2C	C2C	C2A	A2C	C2C	C2A	A2C	C2C
Dissemination of warnings		■			■				
Dissemination of recommendations for actions		■			■			■	
Raise awareness of risks/promote prevention	■	■	■				■	■	■
Spread out status updates				■	■	■			
Emergency calls (e.g. at overstrained telephone network)				■					
Request of affected for help/offer help				■	■	■	■	■	■
Evaluation of the situation through authorities (by using information from social media				■			■		
Enabling/engaging a dialog between public authorities and citizens	■	■		■	■		■	■	

	Prevention & preparedness phases			Response phase			Recovery phase		
	C2A	A2C	C2C	C2A	A2C	C2C	C2A	A2C	C2C
Aftercare for victims and relatives							■	■	■
Maintain contact with family/friends						■			■
Search missing people								■	■
Coordination of volunteers					■	■		■	■
Mobilisation of volunteers					■	■		■	■
Search for witnesses								■	
Building a relation and trust between authorities and the public		■						■	
Obtain and provide feedback							■	■	

3.2 Risks associated with using social media in emergencies

Furthermore, some risks should be considered before using social media in crisis management:

- Verification/quality evaluation of information [BlKa11]
- Difficult to correct false information/reports [BlKa11]
- Needs of human resources [BlKa11] and staff training, budget needs
- Maintaining social media accounts (especially during a crisis) needs time [BlKa11]
- Information overload especially during a crisis
- Suspicion of innocents [PYKI+13]
- Fast dissemination of confidential information e.g. police information [PYKI+13]
- Expectations of citizen/expecting quick answers [BlKa11]
- Emergency calls through social media [PYKI+13]
- Perceived coercion for “non social media user” to use it to stay up to date

3.3 Organisational and professional factors inhibiting the use of social media

In the case study analysis performed during EmerGent, we highlighted four key organisational and professional factors inhibiting the use of social media in emergencies [SJCD+16]:

- **Lack of organisational structures and procedures in place:** the structures and networks already developed in emergency services to support the use of social media are usually limited, including the technical infrastructure. In Wroclaw floods, for example, the website of the city of Wroclaw was down throughout most of the emergency, so there was no information available on help and support. Ironically, this created the opportunity for

"external" actors to rapidly develop and deploy social media-led responses to the emergency.

- **Lack of resources, staff and skills**: Emergency services reported that they had no personnel trained in using social media, and a similar lack of tools and expertise. In other cases, whilst use of social media was seen as an efficient way of spreading information, the unforeseen consequence of this was that the emergency services were found without the staff necessary to adequately handle the volume of replies and queries from citizens responding to such social media broadcasts. Other challenges highlighted included: knowing what hashtags to search for, how to limit key word searches so that geographically relevant information comes up; not being part (or perhaps knowing) of any local Facebook sites that may have been set up; and not knowing who the active social media users are in communities.
- **Information overload**: Most case studies illustrated the extent to which emergency services were often unprepared for the scale of data generated through the use of social media, resulting in an information overload.
- **Verification of information**: Related to the issue of information overload, the cases showed that organisational structures and processes were unable to adequately and efficiently validate the information generated through social media. In the Tbilisi floods in June 2015, the unique characteristics of the event, involving escaped wild animals, generated visual content that was amplified by citizens. This had a negative impact on the clarity, quality and quantity of information produced through social media, supporting the dissemination of inaccurate information. In other case studies in Germany and in Western Norway, issues around information verification were compounded by emergency services' anxieties about ensuring that information privacy and sensitivity needs were respected.

3.4 Lessons learnt from organisations that experimented with social media

Despite the numerous potentials, opportunities, and risks associated with social media that need exhaustive consideration, many emergency services have published their experience with social media. These case studies provide good guidance on the final outcome and findings of the experimentation with social media that can shift the focus from the thorough analysis that is needed and provide a bigger picture. In most cases, use of social media is a "learning by doing process". An example is the lessons learnt that are outlined in the case study of the Queensland Police Service, quoted below [QPS1.0]:

- *If you are not doing social media, do it now. If you wait until its needed, it will be too late*
- *Rethink clearance processes. Trust your staff to release information*
- *Add a social media expert to your team. While there should be shared responsibility for uploading information and moderating social media sites, expert technical advice and trouble-shooting will be necessary from someone with an IT background*
- *Do not treat social media as something special or separate from normal work processes. It should be integrated as standard practice*
- *Do not use social media solely to push out information. Use it to receive feedback and involve your online community*
- *Established social media sites are free and robust which can handle volumes of traffic much larger than agency websites*

4 Guidelines for emergency services & public authorities

The guidelines for ES are divided in four sections:

- Prepare to start using social media
- Before an emergency (prevention & preparedness phases)
- During an emergency (response phase)
- After an emergency (recovery)

4.1 Prepare to start using social media

4.1.1 Consider the legal implications

The empirical studies in the project indicate the need for a legal basis for what emergency services are allowed to and could do with data from social media, to prevent legal concerns and insecurities. Data protection concerns make a legal and organisational foundation on how to act and how to handle collected data. This would give the staff a foundation they can rely on.

Dealing with Social Media may lead to additional responsibility for emergency services. Question that always emerge when considering the use of social media, are:

- Does an emergency service need to react if someone writes that is in need of help?
- Are emergency services liable if a request for help on social media is missed?
- Are emergency services liable if some harm is unknowingly done, e.g. publishing the false message by mistake?

Although these are valid concerns, it is not possible to provide a recommendation on how they should be addressed. The national legislation and the operational policies must be considered. Expert advice with a good understanding of legal frameworks, emergency services and social media will help answering these questions.

These considerations should be covered in the social media policy of the institution and clearly communicated to citizens, so they are fully aware of what they should expect from emergency services in social media. In the experience of EmerGent, most emergency services are not ready or do not yet wish to receive requests for help or emergency calls from social media. This should be clearly stated and communicated to the public, but the social media policy should take into account that there have been past emergencies, like the attack at the Bataclan concert hall, in Paris in November 2015, that it was not possible to make an emergency call due to the nature of the emergency. People in need of help published their requests in social media instead.

Legal implications also extend to taking the appropriate measures to adhere to the legislation for Data Protection and Privacy. Section 7 provides concise guidelines centred around how a project that mines social media can meet the its obligations under the European Union's (EU) General Data Protection Regulation (GDPR) that was adopted in April 2016 and comes into force within the following twenty four months.

4.1.2 Consider the needs in human and financial resources

The use of social media entails operational costs and needs in human resources that should be considered beforehand.

During the EmerGent empirical studies, the following conclusions were drawn:

1. **Emergency Services need social media expert users**.
    - Expert users are the ones who control the social media dashboards and choose the search protocol for gathering and monitoring information from social media. They are also the users that provide crisis communication on social media, as there is a requirement to be very familiar with social media "language" to be able to communicate in the most appropriate way.
    - Basic users are, for example, PSAP operators who just have to get information from social media when it's relevant.
    - The use of social media should not interfere with the operation of emergency services staff and should not add additional work to them. In the context of EmerGent, the role of the social media manager was defined, as a user of social media accounts and ICT tools. This role is responsible for gathering, filtering and publishing information and collaborates with other staff to extract information for publication and also feed filtered and assessed information that will help recovery operations.
    - The Wellington Region Emergency Management Office [WREM14] suggests to "*move past the we don't have the resources frame of mind to a more adaptive approach where you can bring in expertise as necessary*". In the empirical studies of EmerGent, staff of emergency services who use social media responded that staff with skills to use social media were identified from within the organisation. Collaboration with volunteers and VOSTs can help reduce the needs in human resources. Supervision will be needed but it will be reduced over time. For more information about collaboration with VOSTs see sections 4.2.4 & 4.3.6.
2. **Emergency Services need the ICT tools to gather information from social media**, especially in times of increased communication during emergencies and **also need the skill to verify the collected information**. ICT should support them in these tasks.
    - Addressing this point helps to enable social media use in the future, not only for spreading information, but also for using information provided by citizens.
    - There is a need for ICT support tools to achieve this goal, as well as a need for staff training and these activities should be considered in the financing of the organisation to enable the effective use of social media. While this was not the case in all the observed empirical studies, some cases reported that use of social media was covered from budget categories not explicitly determined for that use.

EmerGent has not studied these financial needs in terms of estimated figures, but provides a list of cost categories that should be considered before starting to use social media. It is not mandatory to consider all the following costs in the budget estimation of an emergency service organisation, as there are different levels of using social media and organisations may work with staff that is already familiar with these technologies. In the EmerGent case studies,

we came across emergency services staff with the role of a Public Information Manager, a person who deals with all media communications including social media.

- Cost of ICT tools to gather and monitor information from social media[1]
- Cost for staff training
- Cost of staff using/monitoring social
- Cost of using the advertising platforms of social media channels to increase the reach and engagement in content

Although not possible to measure, the use of social media is sometimes considered to reduce overhead costs during an emergency, for example by reducing the number of incoming calls to emergency numbers that are only seeking information.

4.1.3 Prepare a social media strategy

A social media strategy should clearly describe the objectives of using social media, who, how and when to use social media during all emergency phases. Social media should be seen complementary and not as a substitute of the existing communication channels.

Social media guidelines should be derived from objectives and the social media strategy the organisation already has established or is in the process of establishing [BITK10]. The Guidelines should include the following aspects [BITK10]:

- which objectives the organisation pursues with the use of social media,
- which content should be published,
- which content is not permitted to publish,
- which social media channels should be used,
- who is the target group,
- who administers the different social media channels and
- who is the contact person if there are any questions concerning social media.

If you already have a communication strategy, the social media strategy is its extension and should not be strict but aim to achieve its organic evolvement. The following section outlines the subjects that the social media strategy can address.

4.1.3.1 Define the roles of staff and their responsibilities

You can adapt your existing communication strategies, by identifying clear ownership of responsibilities during the four emergency phases [HSGM+14], analysing information flows and adapting them to the use of social media [HSGM+14]. Clear answers to the following questions will help define responsibilities and roles:

- What social media platform(s) will be used and what accounts should be monitored?
- Who is responsible to monitor and manage them? Is there additional information to monitor, e.g. hashtags? Note that hashtags follow trends and they rapidly change.
- Do these responsibilities change if a major incident occurs? How?

[1] Cost of social media analysis tools can range between less than $2K to more $7K per year depending on functionality. See [Tril15, p.16] for more detailed analysis.

- What is the content approval process? Having a mandatory content approval policy may impose a barrier in achieving smooth communication via social media. Aim to distinguish content that needs and does not need approval and when the approval is not needed?
- Which users have access to post information and respond to incoming information requests?
- While defining roles and responsibilities, consider the shift changes and staff needs if you are going to use social media on a 24-hour basis. Information may need to be passed from one shift to the next.
- Think about securing social media accounts e.g. the password policy, where are passwords retained, who has access, how often do passwords change?

Examples:

- The UK West Midlands Police have produced a 'Social and Digital Media Policy' [WWW13] which sets out to all officers and staff the definitive Force corporate approach to the use of social media accounts i.e. Twitter, Facebook, YouTube and blogs etc. in line with their work. This sets out: the purposes of social media accounts; procedures for opening an account; procedures for monitoring and supervising the content of the account; management and updating of content; account security and training.
- See the "Social Media Policy and Guidance" of the Leeds Community Healthcare for an example of defining the roles and responsibilities [Neil15].

4.1.3.2 Define the content strategy

When to post?

Social media cannot be used only during emergencies. Continuous use is required before and after. Publish content and information updates regularly to keep your audience involved. A good starting point is to make a post daily. Before emergencies don't publish many posts during one day, to keep the interest of your readers and avoid overwhelming them. Social media networks suggest to experiment with different times to post content and observe the differences using the analytics tools. Experimenting with different frequencies and times to make a post, will help find a good measure of the frequency for sharing information [Unic12].

What to post?

Be active in social media, but not boring. Identify interesting content to post, but always be professional. You need to balance the different types of content, e.g. funny, interesting and serious, and try to keep it interesting enough for people to follow it. For example, in Antwerp the location of a speed limit enforcement unit is posted regularly to keep the interest of the followers. More detailed suggestions can be found in the following sections, divided in content useful before, during and after emergencies.

Remember to always use a spell checker before posting your content to prevent negative reactions for misspelling that can be easily avoided. During the preparation phase, you can

also create a set of responses to frequently asked questions during emergencies, to save time when an incident occurs [HSGM+14].

Social media content can include content already published, although original content achieves greater results:

- Follow official accounts of other emergency services and public authorities and repost their content for increased reach
- Refrain from following or publishing posts of commercial brands
- Consider having an approved list of other followed official accounts that you can share information from during an emergency
- Verify the information before you post something [HSGM+14]

Where to post?

Think about your target group, the aim of your social media presence and the channels already in use in your region [HSGM+14] to choose the right channels. Note the specific channel characteristics, e.g. use Twitter for short status updates or Facebook to discuss with people and build a community. You may also consider the appropriate social media platforms based on the audience you want to target and the hours of monitoring or social media presence. See the flow charts for Facebook and Twitter prepared by the Australian Capital Territory Government [ACTG12].

Depending on size of the organisation, use only one channel at the beginning and introduce more later. Use verified accounts when possible and promote your social media presence [HSGM+14] by including them on your website and other public material.

Writing for social media

The writing style and tone of content can achieve more greater audience reach and greater impact (enable the public to clearly understand and act on the content). Content should be [CDC12a, GIS11]

- **Credible**: content that is accurate, fair, thorough and transparent
- **Relevant**: content that is influential to the audience, based on time, geography, audience or interests
- **Useful**: content that helps the audience learn something they didn't know, or act upon a request
- **Interesting**: content that captures the attention of the audience

Use a friendly tone and plain language in your messages. Talk to readers as you would speak to people [WREM14, p. 8] in everyday life, always maintaining the level of professionalism expected from your organisation. The social media policy and the staff training should emphasise that official accounts should not spread personal opinions [ACTG12] and additionally, the responsibility of personal accounts when a connection to the organisation is visible. The writing style during a crisis will usually need to adopt a more serious tone. See the "Guide to Writing for Social Media" by the Center for Disease Control and Prevention [CDC12a] that explains the importance of plain language and gives good and weak examples on writing in plain language.

While writing content and using images, remember to:

- **Be aware of privacy**: Ensure that privacy and protections is respected in all communications [Daim12], e.g. do not publish information with faces of people, number plates of cars, phone numbers etc.
    - Respect confidential information or information that should not be made public, and do not talk about a third person without their approval [Daim12]
    - Privacy becomes more important with the capabilities offered by social networks to repost already existing information. Several users may post content without considering the privacy considerations. Ensure not to reuse this content without adhering to privacy regulations.
    - If you cannot ensure privacy of information when sharing content, you may consider adopting a policy that does not allow sharing content from unofficial or untrusted sources.
- **Respect intellectual property**: When publishing information to social media some content, e.g. photographs, may have intellectual property rights and its use could be allowed only in specific cases, e.g. for personal use only. Intellectual property rights may exist for text, photos, pictures, graphics, audio and video files [BFW12]
    - Before reusing existing content, always look for the content license. If the content is not in the public domain, give credit to the creator. See the Creative Commons licenses to understand how content can be used [WWW06] and the best practices for attribution to find good examples of giving credit [WWW07].
    - Add references when reusing existing content and specify the sources [Daim12]
    - Mark quotations [DCV11]

4.1.3.3 Handle negative or irrelevant feedback

Negative or irrelevant feedback requires monitoring your accounts to first identify the content and assess if a response should be provided. When negative feedback is received, the following reactions are possible:

- **Delete**: Depending on the functionality of the social media platform, deleting a comment or post may remove it from your account, but may remain visible to other users. Deleting a comment should usually be avoided [DRK11], but there are cases when deletion can be considered for non-constructive comments, e.g. comments that are offensive, violate the terms of use published on your social media account or are "spam" messages. See the "Social Media Public Comment Policy" of the Center for Disease Control and Prevention [WWW08]. Publishing terms of use on your social media accounts may help achieve responsible and effective use of social media. The terms of use can be used to justify the deletion of comments and to reduce non-transparency in the process. Other options to consider for offensive content, are to contact the commenter privately and explain the violation of the terms or report the post and the author to the social media platform.
- **Ignore**: Leave the comment on your account but don't respond to it. This is useful if your reply will not add any value to the discussion.
- **Respond**: If the comment received contains correct facts or is constructive you should never ignore it, even if it contributes to a negative impression on your organisation. Use the opportunity to engage the author in a discussion [DSTL12] and reply kindly as soon as possible. State any facts that are incorrectly reported, explain how you are going to address the criticism.

Consider creating a flow chart to direct decision making for when to react to negative feedback. See the following examples:

- Social Engagement handbook by the American Red Cross [ARC2.0]
- ACT Government Social Media Policy Guidelines [ACTG12]

4.1.3.4 React to a mistake

Accept that mistakes will happen, as they also happen with other media and communications. The aim is not to restrict your content policy to avoid mistakes but to correct them with honesty [Daim12]. The fast information flow in social media increases the risk to make mistakes. It shouldn't make the strategy too rigid and remember that social media communication demands rapid response. When you discover a mistake, don't stay quiet. Respond quickly, apologise for the mistake, explain why it happened if possible, provide the correct information and explain any measures taken to avoid it happening again. Responding to mistakes will show the human side of your organisation.

4.1.4 Clearly communicate the social media strategy and provide staff training

During the empirical studies of EmerGent, we came across the need of a clear social media policy that explains what is allowed and expected, and the need for staff training [RLKS16].

To ensure the adaption of social media in emergency services it is needed to prepare the staff for this new way of communication. Our studies showed that a main factor for enabling the use of social media in emergency services were the staffs' skills, interests and the organisational culture. Training the staff would increase their skills and would therefore be a major enabling factor by lowering the entry barrier. As the studies also showed, staff with more experience in using social media were more likely to expect an increased use of it. This could mean that they see the potential of its use, training other staff members could let them see its potential too and reduce negative attitude towards it.

Staff training can extend on the following subjects. The details depend on the social media policy of the organisation, but they should be clear to all staff. During the studies performed in EmerGent, we identified that the main skills needed are an understanding of social media, a feel of social media network characteristics, the behaviours of people, and a clear understanding of the organisation's social media policy and objectives.

- Present what is allowed and expected when using social media
- Cover the rights and duties of staff using the social media accounts of the organisation
- Train staff to deal with social media and to become familiar with it [WREM14]
- Describe the risks and danger that may arise while using social media (see section 3.2 Risks associated with using social media in emergencies)
- Explain the main principles of the communication strategy
    - Always aim for a polite and respectful interaction with others [BTHW11]
    - Be honest and credible [Daim12]
    - You alone are responsible for the writing, think about possible consequences before posting a statement [BTHW11]
    - Be aware that it's hard to delete content in social media [DRK11]
- Personal responsibility
    - Difference between social media use as an institution and for personal use

- Private statements in social media may influence the perception of the whole organisation [BFW12]
- Suggest using a disclaimer on private accounts stating that the views expressed on a personal account do not represent the views of an associated institution [DRK11]. Personal staff statements on social media may be noticed from the public as an official statement of the organisation [BITK10]. What colleagues may publish on social media and what they are not allowed to say concerning the organisation, may differ within each organisation [BITK10]. It becomes necessary to sensitise staff for the right use of social media. Internal social media guidelines can help to protect the reputation of an organisation and to initiate a successful communication [BITK10].
- Only authorized people may give official statements [DCV11]

- How to verify information
  - A challenging and very important topic while using social media, especially during crises. *The "European Journalism Centre" (EJC) has published the book "Verification Handbook: A definitive guide to verifying digital content for emergency coverage"* providing guidelines for journalists and aid responders, for verifying online content. The book provides valuable advice such as tracking original content, verifying its origin, doing reverse image search etc. and can be used by emergency communication specialists [WWW05].
- Respect intellectual property rights
  - Always respect the intellectual property rights, by checking content licenses and give credit or provide attribution to the owner according to the license. Credits and attribution should be given even if no content licence is available. See more information in section 4.1.3.2 Define the content strategy.

ES staff should be trained not only for social media itself, but also for the additional ICT tools to use for moderation and excessing its information. EmerGent's empirical studies focusing on volunteers and not on professional emergency services, recognized how time-consuming the process of moderation social media channels can be during a crisis. Even if ICT tools can reduce the overhead, the interviews indicated that there were problems adapting to new technology in emergency situations, so they have to be already comfortable using it.

Example:

In Rotterdam, in addition to running a public awareness-raising campaign, the Safety Authority has invested significant resources in promotion and awareness-raising to persuade emergency service staff of the value and credibility of information coming from the public. Part of this awareness-raising effort involved taking the data analysis platform into emergency control rooms, to demonstrate how it worked in practice. A formal social media training programme was also set up to ensure that there is a continuing supply of trained personnel capable of using social media effectively in emergencies. The programme uses a 'train the trainer' method, so that graduates from the programme can expand the skills base throughout the Rotterdam Safety Region through mentoring and 'buddying' (learning by doing).

4.1.5 Use of ICT tools for social media monitoring and analysis

A reliable internet infrastructure is mandatory to extend the use of social media in emergency services as well as appropriate software tools to support the staff with the use of multiple social networks and the amount of information that comes with them. If social media will be used by emergency services, it has to be available all time especially during a crisis, since this is the time emergency services are needed the most and have to expect the most engagement through social media. Most activity in social media is expected during emergencies, a time of increased communication in all communication channels and also a period of time that staff has the least amount of time to deal with it. Additionally, extracting data from social media during emergencies requires extra efforts to search and find helpful information. The use of ICT tools to support the ES staff becomes important and almost mandatory during this time intensive period.

There are different tools that can support emergency services. Some tools specialise in the emergency services domain, but other tools, intended for organisations and companies to monitor social media for their brands and products, also provide useful features and functionality to:

- Gather & filter information cross-media (e.g., Blogs, Facebook, Forums, News Pages, RSS, Twitter, YouTube etc.) with customizable search terms
    - Directly subscribe to arbitrary topics by search terms that are relevant for your organisation
- Detect anomalous events, topics and trends in social media
- Sentiment analysis to grasp the mood of the population
- Dashboard visualisation (e.g. charts and maps) and export (e.g., CSV or PDF) of results and reports
- Estimate the quality of information and providing an indicator of how much real it appears or how much it can be trusted
- Directly push/publish information to many social media platforms from one tool without the need to sign in to each of those platforms (one to many communications in terms of A2C)

The EmerGent deliverable D3.2 “Guidelines for Social Media integration into existing EMS systems” [RFMB+14] describes that currently, ES use a number of experimental tools for receiving and providing information via Social Media. Generally, they are stand-alone tools used by dedicated personnel of the EMS, who check Social Media trends for spotting critical situation, getting alerts and collecting direct information about on-going events. In parallel, they inform citizens with public warnings and messages. The situation is quickly changing and this rapid evolution does not allow providing an exhaustive list of possible solutions.

The selection of the most appropriate tool for your organisation depends on the intended use of social media, the functionality sought in the tool and the available financial resources. [Tril15] has published a report on the findings of a Comparative Review of social media analysis tools for preparedness, funded by the Global Disaster Preparedness Center/American Red Cross. This work was designed to support Red Cross Red Crescent actors and other humanitarian actors in their selection and use of social media analysis tools for disaster preparedness and disaster risk reduction. While going through the selection and evaluation process for an analysis tool, EmerGent’s deliverable D3.5 “User Requirements, Version 2”

[AFA16] provides the user requirements documented by EmerGent while designing the project's ICT tools.

Example:

Emergency services and other agencies responsible for crisis management tend to select 'generic' tools to monitor and analyse social media data. These tools are broad-brush tools with a wide range of applications, including supporting customer services management, publishing and assessing the impact of social media content and supporting 'reputation management', including analysis of competitors and markets. However, most emergency services who have started to use such tools do so because of their data research capabilities. This enables the capture, filtering and analysis of content from social networking sites, blogs, forums, (online and offline) news sites, radio and television. They usually provide Boolean search operators and cross-reference searching; filtering; geolocation analysis and data export. The Rotterdam Safety Authority uses such a tool for real-time situation analysis, its capacity to search, capture and analyse large amounts of current information. Similarly, Antwerp Fire Department use their tool in two main ways: for 'Big Data' analysis - to detect trends and to inform the big picture about an event, and for micro-information - to find individual bits of information, such as video, photos or descriptions that can aid the emergency response. More recently, similar tools have been developed specifically for agencies responsible for public safety.

4.1.6 Use of smartphone apps for direct communication (A2C and C2A)

When receiving an emergency call, any ES tries to obtain as much information as possible, so to understand what is needed to do and how to intervene. Actually, the European ES use phone calls to receive emergency alerts from citizens, which is the standard procedure according to national laws.

Nevertheless, in the recent years both the latest technological developments and the increase of the use of smartphones created an expectation for the citizens: they want to be able to contact emergency services with the technology they use every day. Such technology is well-represented by their smartphones [WWW34]. In the last years, many "SOS" and "help" Apps have been created, and some ES are experimenting the use of such 112 apps (e.g. *Emergency 100* and *Reporty* in Israel). A 112 app is a smartphone application that allows the citizens to contact the ES in case of emergency with a built-in emergency voice call functionality.

In 2014 EENA (European Emergency Number Association) released a document, "112 Smartphones Apps" [WWW34], about the potentialities of using a smartphone app for the emergency calls. This document states that other than the characteristics related to allowing a reliable emergency call (absence of voice delays, routing to the appropriate PSAP, plus the guarantee of a minimum set of data -MSD-, which is a requirement specific for applications and not for phone calls), a 112 app should include also other functionalities that enhance the efficiency and efficacy of ES operations. A 112 app should:

- ensure the availability of the Call-back to the citizen functionality

- be able to send and receive extra information (photo and video) from people in or witnessing an emergency
- be able to make optional additional data available in a format that can be shared with the emergency service
- be able to facilitate the communication from emergency services towards citizen
- be able to work with the more used operating systems.

Beside the 112 apps that provide emergency call functionality, some other apps, related to event alerting, have been developed without this functionality. These apps provide other functionalities that can support the ES operations and event management nonetheless.

As an example, the EmerGent project has developed the EmerGent app, which allows citizens to report any dangerous event near them. This kind of app can be useful for ES or local/regional authorities for receiving alerts about incidents or events in their territory. Moreover, such apps can support the communication activities of ES in two directions: from Citizens to Authority (C2A) and from Authority to Citizens (A2C).

4.1.6.1 C2A and A2C

In C2A, 112 apps allow people to call ES and report any emergency, like a normal phone call. These calls could be treated by the ES as normal phone calls, thus included in the call-taking system and managed as phone calls.

A 112 app can include also multi-media files such as videos and photos. This functionality is useful because it helps the ES in having a better situational awareness and deciding what actions are needed to be taken. The ES Control Room interface should be able to include in the incident management all the information that comes with the emergency call made with a 112 app (e.g. photos, user's location, video).

In A2C, a 112 app must ensure that the ES can call-back the citizen that is using the app [WWW34]. This is one of the mandatory requirements for a 112 app: a functionality that provides direct communication from the Authority to the Citizen. This communication can be only one-on-one (the ES operator and the citizen).

An ES should look for an app that allows the Authority not only to create a one-on-one conversation, but also to create an A2C channel that reaches more than a single person, thus alerting a selected group of people or areas about a dangerous event (see also next section, 4.1.6.2).

4.1.6.2 Support apps

As stated above, there are some apps that do not provide the emergency calling functionality, but are focussed to other functions related to dangerous events and emergencies instead.

EmerGent chose to focus on this support functionality based on the idea of making citizens part of the emergency management process, representing the main source of information about events but still maintaining a strict link to the Social Network realm. In fact, the EmerGent application can collect information from citizens' posts on Social Networks in an indirect C2A function. This capacity categorises the app as a *non*-112 app, since, according to the current national laws, a message posted on a Social Network cannot yet be assimilated to (the same level of) an emergency call. The main reasons refer to user's identification, user's

location and to the recipient of the message (appropriate PSAP). Therefore, the app developed by EmerGent can be classified as a support app for the ES.

With this app, the citizens can report any dangerous or relevant event that is happening around them to the competent authority. The report includes location, description, category and sub-category of the event and multi-media files. The information included in the reports ease the work of the Control Room operators: they will have a better situational awareness (even better in case of reports from several citizens about the same event), which will help them in better identifying the actions that need to be taken.

This support app has an A2C functionality that allows the ES to send alerts to people standing within a certain area or to a selected group of people. The ES can also send alerts to selected specific areas or users, so to limit the coverage of the warnings to the users that are actually affected to the event/incident. Furthermore, the ES may provide multiple information to the citizens, including multi-media files and instructions, which will help the population in taking the right actions, thus minimising the impact of the event.

In A2C, since no communication channel reaches 100% of the population, an app can improve the number of the citizens that may be alerted in case of emergency. The alert will arrive directly to their smartphone, which is actually one of the most used – if not the most used – device by the population: „*The use of smartphones is increasing in Europe. Nowadays in some countries, the number of smartphones is higher than the number of mobile phones*" [WWW34]; „*The most common mobile devices for internet connections were mobile or smart phones, laptops, notebooks, netbooks or tablet computers*" [WWW35]; „*in 2015 there were 1.8 billion smartphone users worldwide and 218 million users in Western Europe*" [WWW36]. Reaching the smartphones guarantees a solid coverage and a high probability that they will read the alert (also, a notification feature will increase this probability).

Also, the EmerGent app can put together C2A and A2C functionalities by creating a direct communication channel between one or more user and the ES. This channel can be regarded as a "chat", where the user and the ES can share information about user's location, psychophysical status, updates from the user or the ES and any other relevant information such as photos from the incident. As an example, this communication channel can be useful in case of a user trapped within a collapsed building.

This application can also provide other functionalities that help operators in their work: the quality control on the reliability of the alert, based on multiple factors (such as distance from the event, user's reputation, relevance of the photos) is a characteristic that allows the ES to identify better which alerts need a quick intervention and which ones do not. Also, the app needs every user to register her/himself providing personal data (e.g. name, surname, address), so to make people accountable for their reports thus lowering the number of fake calls and hoaxes, a significant problem for the ES Control Room operations.

4.1.6.3 Benefits of using 112/support apps

While the most used channel for getting emergency calls remains the normal phone call, the ES should look for providing to the citizens the possibility to contact them with a 112 app and/or a support app that provides other functionalities useful for situational awareness and management of events. These kinds of apps can enhance the efficiency of the ES operations in several ways:

- Both A2C and C2A functionalities
- Better situational awareness thanks to the presence of multi-media files and more information included in the alerts
- Event location thanks to GPS system
- Crowdsourcing from several citizens' alerts in case of large events
- Direct communication link with citizens, with both A2C and C2A functionalities
- Better selection of citizens and areas to be reached by the warning
- Quality control of the reliability of the alerts, lower number of fake/inappropriate calls
- Link with Social Networks and Social Network sharing (if allowed)

4.1.7 Plan the next steps to start using social media

The steps to start using social media vary across different organisations. Organisations will typically first go through a discussion and approval process before developing their social media policy. The introduction process can start from a passive non-engaging phase of only listening and gradually continue to more advanced uses that include publishing and monitoring information and responding to citizens' queries. Different groups outline several introduction steps.

The Scottish government [ScGo12] describes a five step social media engagement model which can be used by an organisation to start and increase its involvement in social media. The model consists of three phases:

1. The **passive phase** utilising only one-way communication to disseminate information and passively monitor information to:
    a. understand your audience
    b. identify key stakeholders
    c. become accustomed to monitoring specific events to increase situational awareness
    d. assess how your organisation is viewed by the public
2. The **active phase** utilising two-way communication to actively engage with the public and real time monitoring for operational use to gain awareness
3. The **proactive phase** utilising two-way communication to establish fully operational social media use model that can be used to receive validated information from trusted sources that can be linked into operational systems and provide an additional, or alternative to, emergency call systems.

As an organisation moves from the first to the third phase the benefits, costs and risks increase. Similarly, the Wellington Region Emergency Management Office [WREM14] describes the following levels of engagement:

- **Observer**
    - Monitor social media channels but do not publish content
    - Allows to monitor public opinion, and gather information on events, including during a response.
    - Relatively low resource needs, which will increase in an emergency.
- **Broadcaster/ Dabbler**
    - Use social media as a new communication channel, or use it during emergency events for publishing public information

  - As social media users may be unaware that you aren't engaging in conversation, they will be disappointed when you do not respond.
- **Fully immersed**
  - Use social media as an additional channel to engage with your community day-to-day and make it part of your operational practice for community engagement before and during an emergency response
  - Generate and publish content for discussion
  - Respond to questions, comments and engage in conversations
  - This level requires the highest level of resourcing and provides the greatest benefit

The empirical studies in EmerGent identified that the first step towards using social media should be the increased use of it in prevention, inform the people how to avoid accidents and how to behave when they occur. Most emergency service staff expected their organisations to increase their use of social media in the future. While the expectations increase as more experience in social media is gained, most staff agree that a good starting point for using social media is for prevention messages. This kind of use does not depend on the trustworthiness of citizen-generated content and is not critical in terms of data protection.

During the 2nd EAB workshop, three different types of C2A communication from the perspective of the authority were examined:

1. **Passive monitoring**: citizens communicate about an incident with or without the intention of alerting the authorities. The authorities have a passive monitoring (human or software) and try to capture this communication. The benefit is that this type of monitoring doesn't cost much effort. The downside is that there is no guarantee of capturing the C2A communication.
2. **Active monitoring with a VOST**: citizens communicate about and incident with or without the intention of alerting the authorities. The authorities have a dedicated VOST to monitor C2A communication and try to capture this communication. The benefit is that specialists are monitoring and that more information is captured. The downside is that there is funding and an effort needed to organize the team.
3. **Active monitoring on hashtags**: citizens communicate about and incident with the intention of alerting the authorities and use dedicated hashtags that are monitored by Authorities. The benefit is that in theory all C2A communication is captured (it is like calling 112). The downside is that information that is sent without this hashtag is not captured.

4.2 Before an emergency

Information posted before an emergency should be informative and interesting to the citizens. The information published should aim to help build and grow a community of followers, establish a good relationship with the public, and enable citizens to better understand the work of emergency services, the existing limitations, and how they can contribute and benefit.

4.2.1 Provide information about your organisation, its operations and emergency prevention and preparation

ES regularly give advice to the public on how to act in emergencies, especially in regions vulnerable to natural disasters. Traditionally these recommendations are distributed in printed form, for example through leaflets and although sometimes this information is also available online, it is difficult to find it or the public will not look for it. Social Media offer the possibility to directly present the recommendations to the citizens in the tools they use in everyday life. Additionally, more detail can be given and citizens can seek clarifications and receive answers to their questions [RFMB+14].

According to the experience gathered in EmerGent the following are acknowledged as helpful: information, tips and advice about prevention of accidents and reduction accident effects, e.g. emergency plans, protective actions, recommendations and reminders to avoid incidents, training resources etc. Active education of the public can help avoid some mistakes in the future. For example, posting after a house fire with the question “why did the fire break out”, followed by an answer, or posting useful information “how to prevent a fire, how to prevent a burglary during your vacation, why to install a smoke detector, how to perform CPR, etc.” can have impact to the citizens. These types of posts can provoke C2A and C2C communication, and can have outstanding results by asking citizens to start thinking or even acting differently in particular scenarios [RPSD14].

ES and other organisations regularly publish the latest data, which indicate possible threats, such as water levels, weather data, or information on big events, to keep people informed. Social Media could be used to establish information streams operated by ES to gather and publish this kind of information. Interested people could subscribe to such a service to stay informed automatically without spending efforts in searching for it [RFMB+14].

Other information that can be published to help prevent and prepare for emergencies or helps the operation of ES:

- Explain when to contact emergency services and the information that is needed when an emergency call is placed
- Encourage the public to call 112 to request help, remind people that 112 is the emergency number in all EU member states, useful to remember while travelling
- Remind people how they can alert emergency services or communication channels for people with disabilities
- Explain the obstacles that affect the work of emergency services or information that will help the operation of emergency services, e.g. false calls and how they can be avoided
- If your ES offers an app for communication with the citizens, promote the download and use of the app

To keep the audience interested, prevention tips should be mixed with other lighter or interesting content. Using funny and entertaining content but related to the operations of the authority raises the interest of citizens. Use of humorous content not related to the operation of your ES should be assessed before published.

4.2.2 Raise awareness on the use of social media

EmerGent's empirical studies identified that the use of social media by ES should be promoted, so that more citizens are aware of it, in case of a crisis [ReSp16]. Additionally, there is generally low awareness among citizens of existing social media safety services provided on Twitter and Facebook – thus, only 6% of citizens said they were "very aware" of Twitter Alerts, while only 3% were very aware of Facebook Safety Checks.

Building a large community in social media cannot happen in short time. Time is needed to gradually build it and increase the reach of your communication. It is essential to develop your followers list early and before an emergency, so the community is established and confidence has been established.

- Tell people you are available to respond to their questions and explain what to expect from you [ScGo12]
- When you will be available and how your availability changes during times of crisis?
- Encourage citizens to support emergency operations by using social media and provide them with information on how they should do it [HSGM+14]. Give examples how social media could be used [HSGM+14]
- Publish guidelines for citizens and describe the correct use of social media in emergency management [HSGM+14]
- Continue to emphasise that social media does not replace emergency calls [HSGM+14]
- Use traditional media equally [HSGM+14]
- Promote use of hash tags to make information easily identifiable. Developing your own hash tags helps people identify content.

Every year Europe celebrates the European 112 Day on 11 February. The day is dedicated to raise awareness of the European emergency number 112. Countries in Europe organise campaigns and other events to promote the European emergency number 112 and help spread the message. Each year, the European Emergency Number Association (EENA) proposes a theme to be highlighted in European countries. The theme proposed for 112 Day 2017 was "Emergencies & social media: how to react" [WWW41] and EENA created an infographic on this topic [WWW42]. Such graphic material (Figure 2) can be used to reach citizens and raise awareness on the use of social media.

Figure 2: Infographic "Social media & emergencies: the basics of how your smartphone can help you", source: EENA [WWW42]

Example:

The Rotterdam-Rijnmond Safety Authority have developed a dedicated on-line platform for co-ordinating social media information in the region, including raising awareness of how the Authority works. The platform - rijnmondveilig.nl –combines Twitter, Facebook, email and SMS to inform the media and the public and to alert them to disasters and incidents on a 24-hour basis. To publicise the platform, the Safety Authority invested significant resources in a public awareness-raising campaign. This had a broader objective - to support transparency and openness by government agencies. The rationale is that, if the Authority establishes its reputation as an open government agency, then it will build up trust and credibility over time with citizens; they will then be more motivated to provide social media information that is accurate, and will be more willing to collaborate with the Authority to counter misinformation and rumour.

4.2.3 Use of ICT tools for social media monitoring and analysis

In EmerGent, we conducted a study with 761 emergency service staff regarding their attitude towards and use of social media [RLKS16]. The study highlights the current and expected increase of future use of social media in their own organisation to:

1. Share information with the public about how to avoid accidents or emergencies
2. Share information with the public during emergencies about how to behave
3. Two-way communication with the public
4. Receive messages from the public
5. Search social media sites to gain situational awareness

If your organisation established multiple social media channels and you want to **share information** about how to avoid accidents or behave during an emergency, you might want to use an ICT tool that allows to publish content cross-media, e.g. regular and scheduled messages. Easy cross-media publication potentially saves effort and resources, and allows to prepare relevant information for predicted emergencies (e.g. in terms of upcoming blizzards or rising flood levels). ICT tools can furthermore provide combined streams of all received messages in your social media channels. This helps maintaining an overview of social media activity to **monitor** the mood of the citizens, to detect trends, topics and, finally, anomalous events like emergencies. It also may be the foundation to establish two-way communication with the public before and during an emergency.

Although the monitoring of own social media channels may be the first step to gain a basic **situational awareness**, ICT tools can further contribute by providing sophisticated **search and filter** mechanisms to gather specific social media data. Your organisation could monitor social media channels of other emergency services, specific communities and users, or pre-emptively search for specific terms or hashtags (e.g. blizzard or #floods) to establish data streams of common or predicted emergencies. In any case, ICT tools with customisable and rich **dashboard visualisations** (e.g. charts) can help to keep control over your social media presence in idle times and before emergencies.

Example:

In the 2010 Wroclaw flood in Poland, information was largely provided by bloggers who collected and shared updates, photos and videos. These media commonly featured flooded bridges, fallen trees, broken roofs and collapsed walls. In later floods such as the Elbe, Google maps were used to show threatened areas and sandbag depots. Google documents and live blogs were also used to openly collect information that could be used by other citizens. In the Elbe and Wiltshire floods, social media was also used to share data on water levels, with monitoring equipment tweeting regional water levels as well as webcams set up in at risk areas. Additionally, custom web tools were developed in order to structure the process of capturing and matching help requests and offers. In the area around Dresden, tweets were automatically generated by the account @FluDDHilfe whenever a user had created a help request or offer on the fluddhilfe.de website.

4.2.4 Team up with other groups and organisations

The social media world with its crowd sourcing approach has options to offer for Social Media for Emergency Management (SMEM), such as the so called digital volunteers [WWW15], i.e. "Virtual Operations Support Teams (VOST)". VOSTs are teams of trusted experts who provide support via the internet and social media technologies to those who may struggle to handle the traffic and data volume during a disaster, but also in day to day activities. VOSTs emerged out of the enthusiasm and passion of their volunteers in using social media and ICT tools for the benefit of recovery operations, and from the clear need to establish a group that would navigate through the vast amount of crisis information, prioritise it and send it to those on the front lines [WWW16].

4.2.4.1 VOSTs in Europe

VOSTs are formed by experts in public safety, communications and IT. Some of their members have previous experience as volunteers and others have professional experience. They are supported by an expanding network of VOST influencers and are backed by international network in Europe, the Americas and Oceania. VOSTs currently exist in Europe and worldwide, with different models of operation.

An example is the collaboration agreement between the Department of Security of the Basque Country in Spain and VOST Euskadi that adds them to the Civil Protection Volunteer Organisation registry and considers them in several regional emergency plans [WWW17]. A term of the agreement is the possibility of VOST taking over the official ES social media accounts in specific situations. France established a similar collaboration with Volontaires Internationaux en Soutien Opérationnel Virtuel (VISOV, French VOST) formally collaborating with several regional emergency response organisations [WWW18]. Similarly in Belgium, the Team D5 is promoted by Public Authorities and officially sanctioned for region and city support [WWW19].

Other organisations include Red Cross and their DiGIDOCs (i.e. "*Observatorio digital en el Centro de Operaciones de Cruz Roja Española*") and DigHums in general (DHN, SBTF, Humanity Road…).

The appearance of VOSTs is based on geographic regions and usually each team is directly related to a geographic region. For example, Spain currently has 13 operational teams[2] and other teams are currently being set up. Additionally, Spain has VOST Spain, the association of all regional VOSTs [WWW20] and is acting as a Virtual Operations Support Group (VOSG). VOST Europe [WWW21] is also being set up by VOST Spain and VISOV and aims to have other countries joining soon. On an international level, there is the global VOST Leadership Coalition uniting all groups in the world [WWW22], and other regional coalitions like VOST Americas (lead by VOST Panamá and VOSG [WWW30]) and VOST Oceania (lead by VOST Australia and NZ VOST [WWW31]) are also being created.

[2] As of December 2016

4.2.4.2 How do VOSTs operate?

The aim of VOSTs is to create the basis for effective collaboration between emergency personnel and those affected by an emergency [WWW16].

They operate under an agreement with the ES or other public authorities and two modes of operation are possible. A VOST can operate "in the shadow" and provide information to the ES, detect hoaxes etc. without this being directly observed by the public. The second model of operation is based on an open collaboration link between the two parties and in case of a crisis a VOST may take over the account of ES. Formal agreements are signed between the team and the authority that accurately describe roles and responsibilities and in what ways will the VOST help. For example, in Spain the agreement recognises the VOST as part of civil protection and they receive training and access to services that civil servants or other ES staff have. In France, VISOV is relaying information to ES via a "workbook" which is a Google spreadsheet and they serve only the filtered info to the ES. Using this online tool, the VOST can share with the authorities the most relevant information and all content that needs their action. A VOST can be self-activated or activated upon demand by an ES or a local authority and can operate on-line or sometimes on-site under the responsibility of local authorities in charge of the emergency.

Overview:

Engage with volunteer groups if available to develop close collaboration links that can be utilised during an emergency. Digital Volunteers such as VOST teams operate in close agreement with ES and different models of operation can be explored. See examples of how VOSTs can support ES during an emergency in section 4.3.6.

Examples:

The website of VOST Spain provides a map with ongoing incidents, updates and information about each incident and a list of detected rumours. The collaboration agreement between the Department of Security of the Basque Country in Spain and VOST Euskadi adds them to the Civil Protection Volunteer Organisation registry and considers them in emergency plans. A term of the agreement is the possibility of the VOST taking over the official ES social media accounts in specific situations.

The Rotterdam-Rijnmond Safety Authority's approach has been to develop a multi-stakeholder collaborative structure, involving 16 municipalities in the Rijnmond area; emergency services; other public agencies (Regional public broadcasting: – RTV Rijnmond, Public Transport – RET, Ministry of Defence, Water Boards, Royal Dutch Rescue Service, Health Services) and commercial organisations, including energy companies and 60 companies in the harbour and industrial areas in cooperation with the municipality of Rotterdam. This organizational structure has supported ownership and buy-in of social media at a high level. The partnership also makes a significant contribution to the efficiency and effectiveness of the social media capture, validation and analysis process. Stakeholders in the partnership play a leading role as co-producers of information as well as in cross-checking its validity.

4.2.5 Publish alerts for the risk of an upcoming emergency

ES seek ways to inform the public about emerging threats in the quickest possible way and try to reach as much of the population as possible. Social Media cover a large part of the population but also offer functionalities to share information that can amplify a message and make it reach more people. While social media should not be the only channel to disseminate early warnings, it is great for publishing warnings, directly exchanging information with the public, and giving advice on how to act in certain situations [RFMB+14].

When disseminating an early warning, the following considerations should be considered:

- Publish existing risks in social media as you would do in other communication channels [HSGM+14]
- Social media can't replace other traditional ways of alerting citizens and should not be the only available channel [HSGM+14]
- Give prevention tips and instructions for staying safe together with the warning
- Remember not to cause panic
- Note that this may not always be the duty of an ES, but public warning may be the role of a public authority or another agency – make sure this is clear in the social media strategy
- Visually distinguish warning from other content you regularly publish and mark that you are posting important information [SSG14]

Example:

The Rotterdam-Rijnmond Safety Authority uses its dedicated on-line platform - rijnmondveilig.nl - to inform citizens and other stakeholders about crisis situations and how they are developing, using some social media channels, including a live blog. For example, a recent major fire in the port led to a major alert being issued to advise people to close their windows and stay indoors. This alert was re-tweeted by citizens with high levels of followers and was also sent to collaborating journalists who passed on the alert via their traditional media channels. During 2015, the platform delivered 208 live blogs and 1,365 tweets, with 3,524 retweets or replies, which were seen 31,068,714 times. It posted 196 messages on Facebook, with 2851 comments or shares and published 100 "Risk Tips".

4.3 During an emergency

Social media provides a communication channel that operates bi-directionally for both A2C and C2A communication flows. During an emergency, increased feedback and information requests should be expected, while keeping on top of all the information and requests during a major crisis will be challenging. During this period, engaging with citizens on social media can be effective due to the speed, reach and direct link of this type of communication. Use your established social media accounts [HSGM+14] and use traditional media and other communication channels equally.

4.3.1 Understand how citizens use social media during emergencies

The latest research has focussed on understanding how citizens use social media during emergencies. Understanding how social media is used can help filter and interpret the information gathered and align the social media strategy during an emergency. This section outlines the findings of EmerGent regarding the social media roles taken up by citizens and a 6 phases theory of the cycle of reactions of citizens on Twitter during an emergency.

Overview of the use of social media by citizens during crises:

Case studies of flooding incidents show that citizens take up different roles in social media during emergencies, and they also use different technologies. Furthermore, there are country and demographic differences in scale and intensity of social media use. Younger people are more likely to use social media during an emergency. A key variable determining the use of social media in emergencies is already using it in normal daily life.

During emergencies, citizens are most likely to use social media for **information seeking** purposes, to search for information provided both by emergency services and other citizens. Some users also take up an **informant role**, alerting citizens or emergency services to specific events or conditions relating to the emergency. Citizens frequently use social media during the EMC to organise or volunteer for help. This is currently often ad hoc, responding to sometimes localised needs. **Amplifiers and citizen journalists** retweet or post messages from emergency services and fellow citizens, hence increasing the reach of social media messages. **Digital helpers** plug information gaps emergency services cannot provide (e.g. in Wiltshire setting up a webcam and broadcasting images of water levels), organizing relief efforts [Elbe, Tbilisi], or raising funds [Tbilisi].

A recent study [WWW14] on how people react in crises using Twitter, analyses recent crises in Europe and concludes to the following 6 stages of reaction: the **information phase**; the **phase of emotion**; the **transition phase**; the **organisational phase**; the **phase of interest**; and the **disorganisation phase**.

4.3.1.1 Roles of citizens using social media

Across the three rounds of case studies conducted as part of WP2 “Impact of Social Media in Emergencies”, we have identified the different roles taken up by citizens on social media [SJCD+16]:

- The **information consumer** role involved citizens using social media (Facebook, Twitter and occasionally a blog) to obtain information on the emergency as close to real time as possible, either from fellow citizens or from emergency services. This helped them navigate the emergency, especially where this information was highly localized.
- **Amplifiers** retweet or post messages from emergency services and fellow citizens, hence increasing the reach of social media messages.
- Digital **helpers** play a role in providing this information, motivated by using their social media skills to plug information gaps emergency services could not provide (e.g. in

Wiltshire flood in UK 2013/2014 setting up a webcam and broadcasting images of water levels at high intervals), organizing relief efforts, or raising funds.

- This role overlaps to an extent with the **citizen journalist** role which was present in several of our cases and involves posting images or text of the state of the emergency in their locality, re-posting messages from emergency services or even countering rumours.
- Whilst citizen journalists reported, **informants** intervened with fellow citizens or emergency services to provide information about local conditions. One of our case studies offered some examples where this information was incorporated into the tactical response effort. In another such information was provided via phone calls.

The case studies also shed some light on the role of **non-users** of social media during flooding emergencies. Reasons for citizens' non-use included: lack of need (no need to know about local road conditions for non-commuters or locations in difficulty being more immediately obvious in smaller locations), alternative means of staying informed or helping others working better (face to face in small localities or email), age divisions (younger people in villages being on social media but older people not), the type of flooding and the immediacy of the emergency (someone in the process of defending their home from flood may not have time to check or post on social media).

4.3.1.2 Patterns of social media use

Through the analysis of the case studies on flooding emergencies we found that the "purpose" for use was the most influential factor in shaping patterns of social media use and that patterns of use can be analysed by four types of "purposes" for citizens and emergency services during emergencies. Ordered from most to least common these purposes are: information seeking; mobilizing; broadcasting; and responding to queries:

Information seeking: The most common behaviour for citizens during the selected case studies was to use social media platforms to find out information about the flood. Information seeking was particularly common amongst those affected by the floods, or who were at risk of being affected. Other citizens sought information out of curiosity or even for fun. These users would monitor and share their information on a wide range of topics such as:

- Checking districts that were unsafe;
- Reporting the current status of recovery;
- Finding out about road conditions;
- Checking that friends were safe;
- Re-posting information from official announcements;
- Accessing videos and photos of places that were flooded or left unaffected;
- Reading security alerts to avoid specific areas due to expected worsening of weather conditions;
- Gathering information to understand the overall situation.

Mobilisation: The second most common purpose for social media use during the floods was the mobilisation of citizens. This took several forms, but mostly concerned citizens self-organizing on social media to help their local area recover from the flood damage. The main social media mobilisation activities included informing local citizens on:

- The needs for medicines, first aid items, food, clothing, baby diapers, household items and other essentials;
- Where volunteer work was needed to assist recovery operations of the flood;
- How to make donations;
- Calls to disseminate information about volunteer and support actions.

Broadcasting: By definition, the users who broadcast messages were usually official voices such as emergency services. Broadcasting was invariably used to give up to date information to citizens on the progress of the flood and clean-up efforts. The local media also shared this broadcasting role with emergency services in several cases.

The types of information broadcast were wide ranging in some areas and included:

- Sharing current news, warnings and field reports;
- Declaring areas safe;
- Providing information on where to get help, including sandbags;
- Disseminating government press releases, and information from other emergency services;
- Producing lists of Frequently Asked Questions (FAQs).

Responding to queries: For emergency services, responding to citizen enquiries through social media was less common than 'broadcasting'. In every case, queries were taken by phone which often led to a backlog of calls. The types of enquires received were varied and included:

- Questions about transportation and traffic issues in affected areas;
- Information on where volunteers were needed;
- Information about particular issues or topics.

You can find more detailed analysis on the roles and "purposes" of using social media in the EmerGent Deliverable 2.3 "Impact of social media on Emergency Services and Citizens" [SJCD+16].

4.3.1.3 Reactions of citizens on social media during an emergency

Recent research has outlined a 6 stages theory of the cycle of reactions from citizens during an emergency on Twitter. The background rationale of the theory is based on the observation that although the crisis lifecycle has been studied by many researchers, there is no theory on the lifecycle of people's reactions to a crisis.

Considering the growing involvement of citizens in Twitter during crisis situations, this work focussed on observations and analysis of the last 6 crises in France and Belgium with heavy human losses. It identified a "reactions' lifecycle on Twitter" and proposed a 6 stages theory describing the use of Twitter by citizens during a crisis:

1. **The information stage**: People's reactions are neutral and focus on seeking information about the event. Hashtags emerge related to the place/city of the event, a generic name related to the type of the attack e.g. Shooting, or bomb, the name of the business involved e.g. Germanwings, Boeing, a number distinguishing the event such as flight number or train line number.
2. **The emotional stage**: People start expressing emotions such as denial, shock, sadness or anger. No new hashtags appear during this stage, while the use of previous

hashtags continues. The theory describes that this phase includes information useful to the authorities to define and carry out the communication strategy.

3. **The transition stage**: While the previous two stages are ongoing, people follow them at different times and some people who recently found out directly enter the transition phase following up the content of the previous two stages. Hashtag changes to combinations of the place/city and the type of the event, e.g. #ParisAttack.
4. **The organisational stage**: Information is now widespread and people will form new hashtags to communicate, e.g. Jesuischarlie, PrayforParis, etc. During this stage, communication extends to different entities offering support and providing help to those affected, e.g. offer free meals, transportation or internet connection.
5. **The phase of interest**: New information appears that is helpful to explain the event or provide evidence useful to the authorities, e.g. videos, witness reports, etc. Commercial brands will start to get involved in the conversations in social media.
6. **The disorganisation stage**: Communities and use of hashtags starts becoming distributed while some people break away from previous communications to express their dissatisfaction, e.g. #IAmNotCharlie, "#PrayForParis is too religious". The organisation observed in the previous stages starts to disappear.

For more details, see [WWW09], available only in French, and its translation in English [WWW14].

4.3.2 Establish communication with the public

The aim for establishing communication with the public is to leverage the previously established community and engage in information exchange with the public. Following the previously described roles of citizens, the public will be eager to receive and send information, and will also try to request information from emergency services and the authorities. Taking advantage of this motivation and making the most out of it could support the recovery operations.

During EmerGent empirical studies, we identified that:

1. **Social media communications need a proper tone of voice to gain acceptance.**
    - Together with photos, the style of the messages is fundamental for the acceptance.
    - "In addition, the style of message writing was also seen as an aspect of quality, insofar as it influenced acceptance among of the various citizens and volunteers. For instance, emotionally supportive photos in conjunction with messages written in an appropriate style seem important to promote a positive climate among participants." [KaRe2016]
2. **Emergency Services have to be the source for reliable information during a crisis, especially on social media, since there is also a lot of false or incomplete information.**
    - The "confidence in the quality and data security of information shared on social media" is not that high, Emergency Services as recognised institutions can provide a sense of trust and therefore help spreading important information.
3. **Emergency Services need to monitor their social media sites and quickly respond to help-requests and questions.**

- The majority (69%) of citizens in a survey of citizens' attitudes towards social media agreed that emergency services should regularly monitor their social media sites, and 41% expected a response within an hour.

4. **Social media communication is a collaborative effort and is shared amongst all involved parties.**
    - It is necessary to keep close contact amongst all emergency services and authorities involved in the response to the emergency to establish a unified approach on the communication and directions to the public. All involved entities should give the same information via social and no two entities should be publishing different or conflict information to maintain the trust of citizens. In previous cases studies, authorities decided to give all info on one account or website. To maximise reach of citizens, it is also possible to have one authority publishing information online and other authorities reposting this information.

Communication with the public can start by informing or confirming that you are aware and responding to an incident. You may link to existing online resources previously prepared. It is preferred to publish regular updates, even if the situation has not significantly changed, to keep your followers informed. People following the incident will continuously seek new information. Information requests from the public will increase significantly and you may receive repeating requests. Remember that some of your readers may have not seen all previous updates. Sometimes posts in social media appear on people's timeline when a user connects to the platform and this may be a lot later. To overcome this, some emergency services include the date and time of the publication in the content. Using the pinned post functionality of social media platforms helps give a first overview to newcomers. Responding to all comments and information requests may not be possible at this time due to the high volume and you may need to prioritise your responses. Explain this to your audience. During a crisis, your pre-planned posting strategy should stop and focus should be shifted to the real incident:

- Communicate regularly, react quickly to information requests, be open and honest. Even during a crisis engage in a dialogue as far as possible and react to citizens' requests [HSGM+14]
- Publish updates and direct citizens to online sources that can answer their questions, e.g. identify what is of most interest to citizens or what information they are mostly seeking and provide a FAQ web page, or a web site that they can report incidents or provide information to the emergency services. Some of these resources can be prepared before the emergency response operation or even while preparing the social media strategy. This may help reduce number of emergency calls that only intend to ask for information updates.
- If possible, photos should be used in social media communication. Photos of helpers, volunteers and affected people can create identification and emotional involvement. This results in emotional comments full of "solidarity, sympathy and identification with the helpers, showing the potential of social media to influence a community's resilience in a positive way.
- Make information easily understandable by using clear and simple language.
- Make information actionable, when something is expected from the recipients of the information.

- Use hashtags or keywords - remember that during crises new hashtags develop naturally and rapidly.
- Republish information that originates from trusted sources or information that you have validated. Sharing valid messages from trusted social accounts will amplify the reach.
- Ask people to share received information with their contacts [HSGM+14]
- Provide instructions to citizens what to do if the emergency starts to directly affect them, e.g. in case of a forest fire.
- Ask the public to respect victims and ensure privacy for emergency operations, e.g. for Police operations.
- Mobilise volunteers and ask people to help each other and show possibilities to help [HSGM+14].
- Consider using programmes such as Twitter's "Ads for Good" that is also available for crisis and emergency response and provide an opportunity to use Twitter's advertising platform to amplify your messages. See [WWW10].

Example:

At the end of 2013, the heaviest rainfall the UK had seen since 1876 caused widespread flooding, power cuts and major disruptions to transport in several regions, including Wiltshire. During the flood, the civic authority (Council) used a combination of Twitter, Facebook and a blog to alert citizens to road closures, water levels and other key events. The live blog was accessible via a link from the Council's website and when clicked on would provide information on school closures, road closures etc. The blog was updated whenever new information about an event came in. In the Wroclaw flood, the blog Wroclaw by Choice received 300,000 visits with contributions by around 300 citizen journalists. This case appears to show that, even without an official broadcaster, an online voice with reliable information is strongly desired by citizens who will fill this gap themselves using familiar technologies if emergency services do not provide broadcasting.

4.3.3 Request information from the public

Social media can be used to request specific information from the public to assess the current situation, help gain better situational awareness or improve the operations in other ways [HSGM+14]. Emergency Services should communicate what kind of information they need, what would be helpful and in which form it should be presented. In the survey of citizens' attitudes towards social media, citizens expressed they wanted a clearer purpose of the information to share and they also expressed the need of "guidelines and encouragement from authorities" on how to best share information.

When requesting information from citizens, always report back on the same topic, for example:

- An example post you could make is "We have received information about x,y,z, can anyone confirm this? For example, ask people to report on the smoke level, if they are

in a specific location, by sending a reply, picture, video and their exact position [HSGM+14].
- Validate collected information, for example by sending professionals to measure smoke levels, or validating the photographic evidence received.
- Provide replies, e.g. we see and confirm smoke, but it is ok.
- Provide acknowledgements of good information

Crowdsourcing information can help you achieve a better understanding of what's happening. Instead of posting a question publicly, you may consider asking trusted members of your online community or ask people in a specific area.

Example:

In the 2010 Wroclaw flood in Poland, information was largely provided by bloggers who collected and shared updates, photos and videos. These media commonly featured flooded bridges, fallen trees, broken roofs and collapsed walls. In later floods such as the Elbe, Google maps were used to show threatened areas and sandbag depots. Google documents and live blogs were also used to openly collect information that could be used by other citizens. In the Elbe and Wiltshire floods, social media was also used to share data on water levels, with monitoring equipment tweeting regional water levels as well as webcams set up in at risk areas. Facebook groups and Facebook pages were both used to create communities of interested parties during floods. In other areas such as the Elbe, existing pages such as Mum's Help were used to mobilise people and coordinate activities. In Tbilisi, the crowd-funding site, Indiegogo, was used for donations.

4.3.4 Use of ICT tools for social media monitoring and analysis

In terms of **communication**, a recent study revealed that citizens expect emergency services to monitor their social media accounts and to respond to postings within an hour [ReSP16]. Furthermore, it is important to publish regular status updates and information about how to behave correctly during an emergency. Some ICT tools allow to publish content cross-media; however, the **specifics of social media** must be considered during an emergency. For instance, Twitter allows to publish public status updates, but the messages are limited to 140 characters, and Facebook allows longer messages with more detailed information, but the reach is restricted to certain communities, groups or pages.

ICT tools can furthermore provide combined streams of all received messages from all your social media channels. This helps maintaining an overview and **situational awareness** in terms of social media activity, to monitor the mood of the citizens and to handle increased (two-way) communication load. Because the latter issue may imply the need to raise personnel for social media monitoring, ICT tools can support with **collaborative** functions like shared inboxes or task management. Besides monitoring own social media channels, specific communities and users, ICT tools may allow continuously **search and filter** specific terms or hashtags (e.g. blizzard or #floods) to gather emergency-relevant information. On the one hand, broad search terms might result in information overload but, on the other hand, restrictive and specific search terms in information shortage. Having the right combination of

search terms (hash-tags) in time available is a difficult task that improves over time and with experience in using ICT tools. Since most ICT tools gather data based on a Boolean combination of search terms, it becomes important to consider the language that citizens use in comparison to the internal terminology in the organisation. Using the right search terms becomes important to collect the right data, as for example the public will not say "domestic fire", but "house fire".

To overcome information overload, the EmerGent platform, for instance, provides algorithms and visualisations to transform the high volume of noisy data into a low volume of rich content that is useful to emergency personnel. Here, it is important to visualise **geolocations** and potentially relevant **media files**. A study with 761 emergency service staff revealed that photos and videos are important types of information during emergencies, but also information about the **public mood** [RLKS16]. The latter might be supported by ICT tools that provide sentiment analysis and visualisation. Especially during emergencies, **the quality of information** is important to support ES. When it becomes time critical or stressful, ES need to take decisions very fast. Criteria like the relevance for the ES, timeliness or completeness could help ES to estimate the overall quality or trustworthiness of information. This could help for example to get correct and current information, and to prevent the spread of rumours.

Example:

Antwerp Fire Service uses a social media monitoring and analysis system to access, manage and analyse social media information. For example, there was a fire in the port on 1st September 2016. Within minutes, a video of the incident, posted on Twitter, was identified by the system. This provided useful information about the type of fire, the smoke direction and the smoke level above ground. Using the information accessed and analysed by the system, the Fire Service was able to share it with citizens – including a link to the service website for more details. The video was also relayed to operational staff on the way to the incident.

4.3.5 False information during emergencies

Case studies on the use of social media during emergencies suggests that issues of information quality arise, both intentionally (false rumours, etc.) and unintentionally (misinformation or misleading information) [SJCD+16]. An occurring emergency increases the risk for spreading misinformation and it becomes important for emergency services to provide information and quickly react to misinformation.

False information may involve posts and photographic material. For example, during the floods in Tbilisi, Georgia in June 2015, the Tbilisi zoo was flooded to the extent that is was almost totally destroyed. Some animals escaped from the zoo and were captured later. Rumours were particularly frequent in content about the search for zoo animals. People constantly posted pictures of wild animals, claiming that they were seen on the streets near them. In some cases, official news agencies also published this information. Many of these stories were not true and included photos that were not from the event or were altered (“photo-shopped”). Many users re-posted such content and made it gain a lot of attention. The popularity of this kind of content resulted in other people believing the inaccurate

information. Citizens and officials tried as fast as they could to establish the real facts, but rumours caused even greater panic and fear in society, making the situation tenser.

Social media also functioned as a corrective mechanism for such false rumours. Thus, the reaction to incorrect information in social media was high, with people on Twitter and Facebook pages correcting information all the time and warning their friends and followers that this information was misleading. After reaching a high volume of comments claiming the posts were inaccurate, misleading articles were identified and their spread was rapidly reduced. This example shows that the interactivity and open space for comments that is provided on social media networks in many cases can help correct misinformation quickly. For more details on how false information affects the quality of information, see [SJCD+16].

Promptly providing information by ES through multiple communication channels, including Social Media, website may help reduce the effects of false information. But it is also necessary to monitor social media for false information and provide corrective actions as soon as possible.

4.3.5.1 How does false information spread?

A rumour starts with someone posting false information and consequently this information is re-posted by several other people. The information gains a lot of attention and may become a trending topic on social media due to its large number of shares. As soon as people start to realise that it contains false or inaccurate information and post about it, the rumour starts to diminish until it is confirmed as false information. A recent study explains how a rumour develops in more detail by studying tweets during three recent attacks of 2015 and 2016 [Vand16]:

1. A real event occurs and is posted on social media
2. The rumour is propagated by people not on site:
    a. People asking what's happening
    b. "Twitter-journalists" or people not on site transmitting hearsay
    c. People sending prevention messages
3. The rumour is slightly altered, e.g. gunfire becomes an explosion
4. Witnesses on site falsely confirm the rumour by providing argumentation based an external element, e.g. I hear sirens
5. First counter-arguments appear that the rumour is not valid
6. First off-the-record statement of an official stating it is false information
7. An official statement confirms the false information

The same study also identified that rumours are spread by actors that are not on site.

4.3.5.2 How to correct false information?

False information should be reported as false or inaccurate as soon as possible. Give accurate information and ask the public to help you set it right, by sharing or retweeting your posts. If possible, find the authors of the false information and ask them to correct or remove the information from their profiles. The Queensland Police Service in Australia use the hashtag #mythbuster to make information correction messages more prominent and combat rumours and inaccurate information [QPS1.0]. See [WWW11] for examples of how the #mythbuster hashtag has been used since early 2011. Similarly, the Federal Emergency Management

Agency (FEMA) uses a rumour control section on their website under each reported emergency to correct misinformation, sometimes using the title “Know the facts and ignore the rumours”. This practice has continued over the years and more recently similar approaches have been used by other ES and public authorities. Police in Germany has use the hashtag #FALSCHMELDUNG (Figure 3 left), meaning false report, while the Police in Spain has used the hashtag #STOPBulos (Figure 3 right), a hashtag also used by VOST Spain.

Figure 3: Examples from ES and public authorities using hashtags to report false information Left: Police in Germany, source: [WWW37] - Right: Police in Spain, source: [WWW38]

Similarly, on 14 July 2017, the French Ministry of Interior tweeted that no hostages have been taken to respond to several tweets suggesting a hostage situation during the Nice attack (Figure 4).

Figure 4: Tweet of the French Ministry of Interior during the Nice attack on 14 July 2017 responding to several tweets about an ongoing hostage situation, source: [WWW39]

Another way of countering these rumours is to encourage citizens to look for “trusted accounts” providing official and verified information and repost only this information to avoid the spread of rumours. During the Nice attack, the French government tweeted about relaying messages only from official accounts (Figure 5). In the Elbe floods, citizens were deployed as ‘moderators’ using Facebook and internet blogs to provide updates and coordinate recovery efforts of citizens and to ensure that misinformation was not published or spread.

Figure 5: Tweet of the French government during the Nice attack on 14 July 2017 suggesting to relay messages only from official accounts, source: [WWW40]

Example:

In an example from Rotterdam, a rumour spread of a gunman approaching a shopping mall in Zuidplein. The rumour spread quickly, generating half a million messages on Twitter, Facebook and Whatsapp within an hour. One of these tweets showed a photograph of the gunman being trailed by police cars. This caused alarm throughout the city, with shoppers running in panic from the mall to escape the gunman. In the Rotterdam-Rinjmond Safety Authority information validation is done through triangulation. Social media information gathered through the on-line platform is cross-checked with the 112 information room emergency desk, with emergency service staff on the ground, with journalists and through feedback from citizens. In the case of the gunman reported in a shopping mall, the Safety Authority started the process of information validation. They contacted sources in the police, who stated that the alleged gunman (a well-known criminal who had been named in the tweet) was many miles away from the scene. The Safety Authority established that the tweet showing the photograph was a malicious piece of misinformation, generated by someone editing a photograph taken two weeks previously of police outside the mall monitoring a strike action. They then fed the real story through to journalists, who used their own social media networks to dispel the rumour. This was backed up by messages issued by the Safety Authority through the rijnmondveilig.nl platform.

VOSTs can support ES in correcting misinformation. For example, ES and VOST teams in Spain use the hashtag #StopBulos, which literally means #StopHoaxes, to identify misinformation and correct it. Several examples are available on the website of VOST Spain [WWW32], while ES also use the hashtag to indicate misinformation, e.g. the Twitter account of Police with more than 2.5M followers [WWW33].

4.3.6 Collaborate with emergent group initiatives

During emergencies and disasters, the challenge is to cope with either the lack of information or an information overload. Digital volunteers and the crowd sourcing approach of social media offers options to overcome this issue. VOSTs can provide support in hoax and abusive behaviour detection, in monitoring multiple channels, in amplification of information, and can sometimes even take over SM accounts in crisis situations. Building on the relationship and the agreements established with VOSTs before the emergency can be utilised during a crisis.

Overview:

Building on the relationship built and the agreements established with digital volunteers such as VOSTs before the emergency can be utilised during a crisis. They can help ES in the following ways:

- Collect online information, filter, evaluate it and forward it to ES
- Sharing useful information with citizens & amplify dissemination
- Provide useful advice to both citizens and crisis managers
- Helping ES, if necessary, by taking over the communication of ES with the public during emergencies
- Support in information verification, rumour detection & correcting misinformation

Example:

After the Brussels bombings in 2016, the Belgian Crisis Center communications team, supported by Team D5 and also from French authorities, among others, lead the communication to the public after the bombings. A complication was added to the already critical situation after the bombings; telephone communications were heavily disrupted, so people turned to social media for information and for letting others know how they were.

A team was in charge of monitoring and analysing information available online and also in the traditional media (TV, radio, print). The information analysis task was performed in the shadows with 45 volunteers active and communicating via a WhatsApp chat room dedicated to the situation. Tasks were split, so all channels (Twitter, Facebook, YouTube, Instagram, Periscope, etc.) could be covered. The team used Trello, an online collaboration tool, to classify and analyse relevant information collected according to 3 categories: information, behaviour and sense making. Once the information was processed, it was transmitted to the spokespersons and communicators to define the communication strategy and the appropriate actions.

A dedicated team helped in the implementation of the communication strategy, while access to the Twitter and Facebook accounts of the Crisis Centre were given to members of the "Team D5" who came to support. Having a good online reputation, and an active presence in Social Media, the Crisis Center provided fast and accurate

4.4 After an emergency

Social media use after an emergency can concentrate on continuing the communication with the public and evaluating the use during the emergency, aiming to extract the lessons learnt and improve the social media strategy.

4.4.1 Continue the communication with the citizens

Social media presence can continue to support the recovery operations [HSGM+14].

Overview:

Information disseminated to the public after an emergency can include:

- Recovery information and follow-up guidance
  - Updates on completed recovery operations, i.e. infrastructure damage that has been recovered, e.g. opening of previously closed roads
  - Request information about locations where help for recovery is still needed
- Support citizens in the processing of events [HSGM+14, p. 16]
  - Use a positive tone in messages about the efforts of the public, e.g. publish thanks and appreciation messages [HSGM+14, p. 18], solidarity notes, happy ending stories
- After a crisis, some citizens will want to help
  - Elicit volunteering resources for the recovery
  - Encourage to help each other [HSGM+14, p. 16]
  - Show possibilities for the processing of the event e.g. self-help communities or psychologists [HSGM+14, p. 16f.]
- Report how the emergency was handled – this helps citizens appreciate the efforts of emergency services and can lead to receiving feedback for evaluation (see next section)
  - Share the workload of the response phase, prepare information with numbers that help understand the emergency encountered and how it was handled
  - Report on waiting times
  - Request feedback from those who communicated with ES during the emergency [HSGM+14, p. 17]

4.4.2 Evaluate your social media use during the emergency

After the emergency or soon after recovery operations are completed you can consider the evaluation of the previous use of social media, examining its strengths and weaknesses, and how it can improve, with the intention to identify the lessons learnt and revise your social

media strategy. Developing an evaluation procedure will help achieve these goals and it should include feedback from involved staff members, the broader group of services and authorities handling the emergency, and citizens.

As with most evaluation procedures, you should look at what has worked, what didn't work, the difficulties experienced, barriers to explore further opportunities, how the procedure and the collaboration of involved people can be improved, and if all stakeholders were able to receive and send the information needed. The evaluation should look at both quantitative and qualitative aspects. A perfect source of quantitative information is to use the internal analytics tools of the social media channels you use, or use external analysis tools to collect and assess several metrics and indicators, such as:

- Number of fans, visits, likes or posts for Facebook [FHH12]
- Number of followers or retweets [CDC11b]
- Assess the change of followers before and after the event and the reach of the public
- Which social media channels performed better? Which social media channels helped reach most audience? Are there correlations between citizens' demographics and social media channels?
- Positive and negative feedback received
- Response times to messages

Identifying metrics that did not perform well can help set the objectives of what changes are need to perform better. However, evaluation should not concentrate only on the numbers, but also look at the citizens' feedback. Inviting their feedback can be done publicly or to selected people and you can suggest a set of questions to evaluate the ES presence in social media during the emergency [HSGM+14]. Ask for their feedback and respond to their replies, even if they are not positive. The results of the evaluation and the lessons learnt should be widely communicated to all staff involved and taken into account to revise the social media strategy and achieve improved use the next time a similar incident occurs.

Overview:

- Develop an evaluation procedure
- Involve all stakeholders in the evaluation, including staff and citizens
- Look at quantitative and qualitative metrics and using social media analytics tools
- Invite citizen feedback via a questionnaire
- Learn from the evaluation and share its results with all involved parties

Example:

ES are now beginning to recognize that "first generation" social media – like Twitter and Facebook – though providing valuable information – have certain limitations and are beginning to be replaced by more recent social media. For example, evaluation of social media use by Antwerp Fire Department and Rotterdam Safety Authority showed that Twitter has a narrow user demographic, and younger people are much more likely to use WhatsApp, Instagram and Snapchat. Emergency services are therefore beginning to experiment with using these newer social media technologies.

5 Guidelines for citizens

Objective: to be concise and easy to remember

5.1 General Aspects while using social media

- Interact with respect and courtesy [BTHW11]
- You are responsible for your writing, think of possible consequences [BTHW11]
- Protect your privacy and check the privacy settings [DRK11]
- Respect intellectual property rights, including pictures, graphics, audio and video files [BFW12]
    - Add references [Daim12]
    - Make quotations marked [DCV11]
    - Specify sources [Daim12]
    - Without approval do not talk about a third person [Daim12]
- Verify your information before posting [HSGM+14]
- Correct a mistake if you made one [Daim12]

5.2 Before an emergency

Be prepared:

- Know the social media accounts of your local and national ES and follow them [HVGS+14]. This will help find real-time information during an emergency.
- Read what to expect from ES in social media. Are they always online? Do they reply to posts in social media?
- Look for apps that ES provide and download them to stay informed during an emergency
- Follow the information from ES on how to prevent and stay safe during emergencies [HVGS+14]

5.3 During an emergency

Stay up-to-date

- Follow official accounts and local organisations to get information updates [HVGS+14].

Social media does not replace 112

- Remember you can use social media for information updates, but it does not replace emergency calls [HVGS+14]. If in danger, always call 112 first.

Be responsible and avoid spreading rumours!

When you post information about an emergency in social media:

- Always mention the ES account or include any already used hashtags. When possible report a location and use photos [HVGS+14]
- Tell only facts and don’t send information you are not certain about [HVGS+14]

- Share only official and reliable information and avoid spreading rumours! The spreading of false information can threaten the smooth deployment of rescue teams and put you and your relatives at additional risk.
- If you spot or shared false information, please correct it [HVGS+14]
- Forward received official messages to your contacts or share them [HVGS+14]

Volunteering intiatives

- Look for emergent volunteer initiatives in Facebook groups, Google crisis maps or trusted users in Twitter; they may help to increase the impact of your activities!
- If you intend to initiate your emergent volunteer initiative, please check for existing initiatives first and carefully chose the scope of your possible contribution.

5.4 After an emergency

- Follow official accounts and local organisations to get information updates [HVGS+14]. Communicate even after a crisis and use social media for the processing of the event
- Give feedback to the authorities
- Restore missing contact and ask for welfare of family and friends
- Help others reconstructing/handling the event

6 Annex I: Methodology for the derivation of the following guidelines

The methodology to derive the EmerGent guidelines was based on three underlying principles and objectives:

1. All conclusions and result of the work in EmerGent should be documented in the guidelines
2. End users should be involved in the methodology to develop the guidelines
3. As many other guidelines and guidance documents already exist, the Emergent guidelines should acknowledge and reference previous work on this topic.

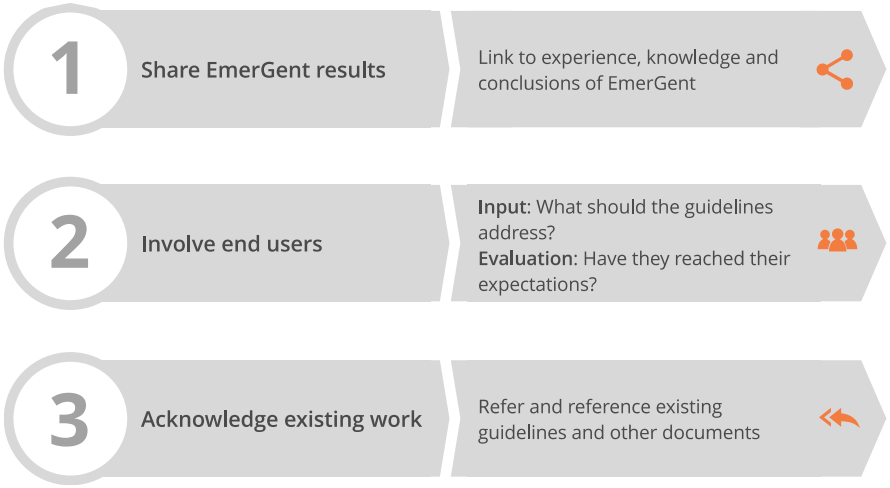


Figure 6: Underlying principles and objectives for the development of the EmerGent guidelines

Based on the above criteria a three-stage methodology was designed to develop the guidelines:

- **Stage 1** included a review of existing guidelines, identification of topics from the research in EmerGent and input from end users to define the outline of the guidelines.

- **Stage 2** included the evaluation of outline with end users to refine and produce the final outline and start the preparation of the content and produce its first full draft.

- **Stage 3** included the evaluation of the content with end users, address the received feedback and produce the final document in its full format and other shorter versions.

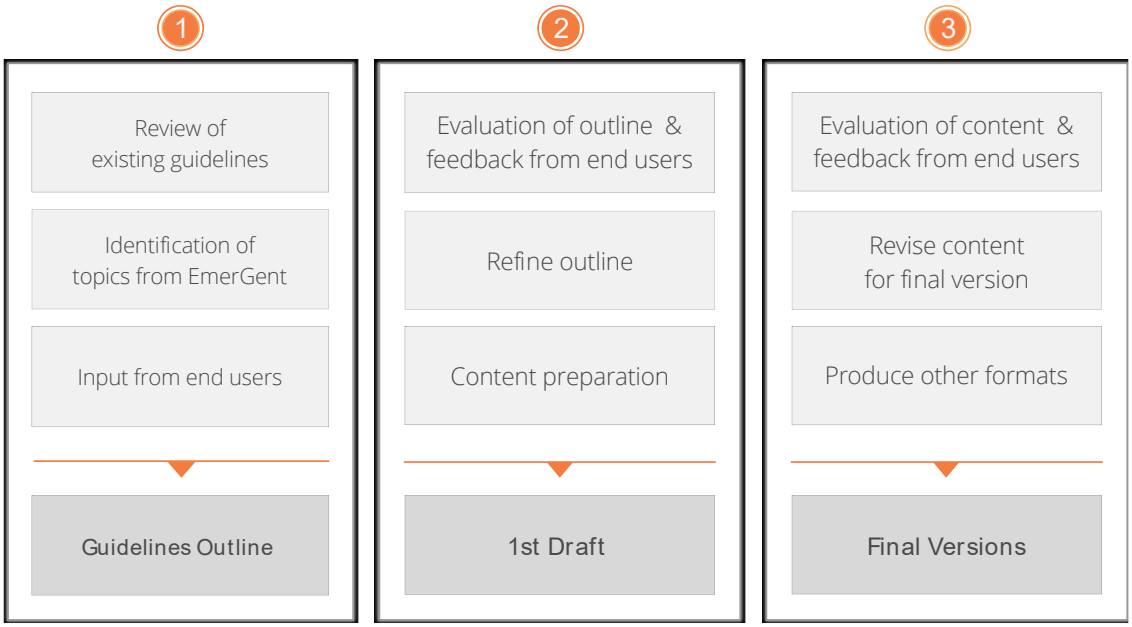


Figure 7: Methodology for the development of the EmerGent guidelines

In this three-stage procedure EmerGent's End user Advisory Board (EAB) and end users from consortium partners and their networks were involved in the tasks of each stage, where end users are indicated.

6.1 Review of existing guidelines

There are many existing guidelines concerning the use of social media in general as well as for use in crisis situations. For the derivation of guidelines, it is necessary to analyse existing documents and to formulate traits that must be followed by the final EmerGent guidelines. Table 2 and Table 3 give an overview of the analysed guidelines. There were two types of guidelines considered. Table 2 shows guidelines for a use of social media in general and Table 3 shows guidelines for a use of social media in crisis management. Guidelines for the use of social media in general were also considered because an appropriate crisis communication with social media is impossible without basic rules for acting in social media.

Table 2: List of guidelines for the use of social media in general

No.	Title	Publisher	Year	Country / Region
1.01	The health communicator's social media toolkit [CDC11b]	Centers for disease control and prevention	2014	USA
1.02	Verification Handbook - An ultimate guideline on digital age sourcing for emergency coverage [WWW05]	European Journalism Centre (multiple authors)	2014	EU
1.03	Social engagement handbook 2.0	American Red Cross	2012	USA
1.04	Social media handbook	United States Army	2014	USA
1.05	Ein Leitfaden zum Umgang mit Social	Deutsches Rotes Kreuz (DRK)	2012	Germany

No.	Title	Publisher	Year	Country / Region
	Media im DRK [DRK11]			
1.06	Social-Media-Guideline - Empfehlungen für einen sicheren Umgang mit sozialen Medien [BFW12]	Berliner Feuerwehr	2012	Germany
1.07	Verhalten in sozialen Netzwerken [BTHW11]	Bundesanstalt Technisches Hilfswerk	2011	Germany
1.08	Das soziale ins Netz bringen – die Caritas und soziale Medien [DCV11]	Deutscher Caritasverband	2014	Germany
1.09	Social media guidelines for IFRC staff [IFRC09]	International Federation of Red Cross and Red Crescent Societies (IFRC)	2009	International
1.10	Social Media - Guidelines for Canadian Red Cross Staff and Volunteers [CRC13]	Canadian Red Cross	2013	Canada
1.11	Rotkreuz-Social-Media-Policy [ARK10]	Österreichisches Rotes Kreuz	2010	Austria
1.12	ACT Government Social Media Policy Guidelines [ACTG12]	ACT Government	2012	Australia
1.13	Social Media in der Hamburgischen Verwaltung - Hinweise, Rahmenbedingungen und Beispiele [FHH12]	Freie Hansestadt Hamburg	2012	Germany
1.14	Social Media Guidelines and Best Practices - Facebook [CDC12b]	Centers for Disease Control and Prevention (CDC)	2012	USA
1.15	Social Media Guidelines and Best Practices - CDC Twitter Profiles [CDC11a]	Centers for Disease Control and Prevention (CDC)	2011	USA
1.16	CDC's Guide to Writing for Social Media [CDC12a]	Centers for Disease Control and Prevention (CDC)	2012	USA

Table 3: List of guidelines for the use of social media in crisis management

No.	Title	Publisher	Year	Country / Region
2.01	Guidelines for the use of new media in crisis situations [HVGS+15]	COSMIC project	2014	EU
2.02	Warning and informing Scotland using social media in emergencies [ScGo12]	Scottish Government	2012	Scotland

No.	Title	Publisher	Year	Country / Region
2.03	Social media for emergency management - a good practice guide [WREM14]	Wellington region emergency management office (New Zealand)	2014	New Zealand
2.04	Emergency 2.0 Wiki [WWW29]	Emergency 2.0 Wiki		International
2.05	Social Media in an emergency: Developing a Best Practice Guide Literature Review	Opus International Consultants Limited (New Zealand)	2012	New Zealand
2.06	Using social media for emergency notifications - 7 questions for emergency managers to consider	Twenty First Century Communications, Inc., technology company in Ohio, USA		USA
2.07	Social Media in Emergencies - UNICEF Guidelines for Communication and Public Advocacy [Unic12]	Twenty First Century Communications, Inc., technology company in Ohio, USA	2012	USA
2.08	Smart tips for category 1 responders using social media in emergency management [DSTL12]	Defense Science and Technology Laboratory	2012	UK
2.09	Crisis communications and social media- A best practice guide to communicating an emergency	IATA	2014	International
2.10	Next Steps: Social Media for Emergency Response	Homeland Security	2012	USA
2.11	Using Web 2.0 applications and Semantic Technologies to strengthen public resilience to disasters	Disaster 2.0	2013	EU
2.12	Bevölkerungsschutz: Social Media	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	2014	Germany
2.13	The Use of Social Media in Risk and Crisis Communication	OECD	2014	International
2.14	Leitfaden Krisenkommunikation [BMI14]	Bundesministerium des Innern (BMI)	2014	Germany

7 Annex II: Data Protection and Privacy Guidelines for Processing Social Media Data

7.1 Overview

This document has been written to provide concise guidelines centred around how a project that mines social media can meet the its obligations under the European Union's (EU) General Data Protection Regulation (GDPR) that was adopted in April 2016 and comes into force within the following twenty four months.

The text of the GDPR can be found at the following website:

http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

These guidelines have been developed as a direct result of creating documentation and project controls designed to handle the specifc requirements of the Data Privacy and Protection obligations for the EmerGent project.

7.1.1 Target Audience

We expect that this document will be applicable for any project (or organisation) that is undertaking large scale gathering and mining of online social media with the express objective of aiding emergency services and public bodies to plan for and respond to an incident. The term "project" in this Annex refers to any project, other activity, or organisation including ES, public authorities or government agencies gathering and mining data from social media for use in emergency management. Whilst not having the objective of being openly generic, other organisations that gather and mine social media for more commercial purposes may find the guidelines useful as a reference.

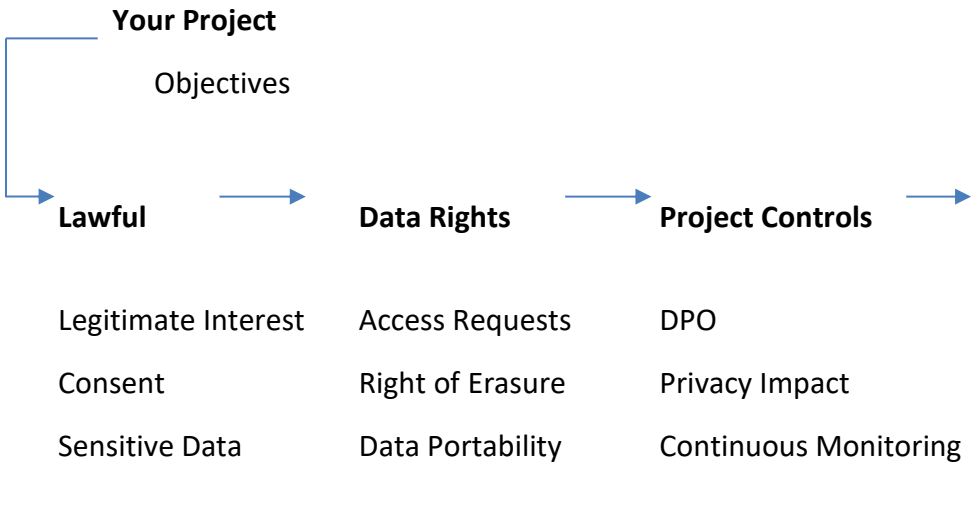
7.1.2 Document Organisation

This document is divided into sections that represent the path through which we recommend you take in designing and implementing your own approach to Data Protection and Privacy (DPP).

We start with a chapter on who are the main actors of GDPR and their scope of responsibility.

This is followed by four sections outlining common topics that contribute to complying with the GDPR. These can be taken in order, from the preparation of your project's initiation, understanding your legal obligations and the citizen's rights, through the project controls that will be used during continuous monitoring of the system and finally the infrastructure controls that underpin your technical implementation.

Table 4: Overview of Data Protection and Privacy Guidelines for Processing Social Media Data



7.1.3 Disclaimer

This set of guidelines is not exhaustive and should be read in conjunction the publicly advice provided by your national data protection regulator. When in doubt seek legal advice at the various stages of the project initiation as well as during the Business as Usual operation cycles.

7.2 Responsibility

In this chapter, we list out the some of the jargon and terminology that comes with Data Privacy and Protection (DPP) and the legislation from the General Data Protection Regulations (GDPR).

7.2.1 Project responsibility

We start by asking, is the project processing data that should be considered as subject to the GDPR and who should be considered responsible for DPP in the project.

Processing does not just refer to electronic records but any operations performed in an automated (or semi-automated way) on personal data in a variety of ways and uses. As you are reading this guideline then you are collecting and mining data and so you are processing data as it is definitely included in these categories (collecting, recording, structuring, storing, alignment or combination, etc.).

The follow up question is "Are you processing *Personal Data*?". Again, as you are collecting social media then the answer is undoubtedly "*Yes*" as that data will in a large proportion of the cases contain information that can relate to a natural person (or "*Data Subject*" as they are termed in the GDPR) who can be identified directly or indirectly through several factors (an id, name, location, online id, genetic, cultural, etc.). This broader concept reflects the realities of data aggregation and the ability to draw together many data points, such as those provided by social media, to produce information that could potentially reveal a natural person's identity.

In the case of the EmerGent project and its use of social media, this wider definition, alongside the approach to pseudoanonymity (the ability to identify a data subject with reference to other data sets), leads to an increased potential for social media posts to be categorised as personal data.

The GDPR makes provision for two types of processing actors; the data controller and the data processor.

7.2.1.1 Data Controller

This is considered as one or more people or entities that will decide how and why the personal data will be used and processed. According to the GPDR's new provision on accountability, the controller is responsible for upholding the principles relating to personal data and demonstrating that this is achieved. The data controller is responsible for showing that, where required, a data subject has consented to the processing of personal data. It is a role upon which the responsibility lies to uphold the rights of data subjects such as the rights of access, rectification and erasure.

7.2.1.2 Data Processor

This is the body (or person, public authority, agency, etc.) that will undertake the processing of the data on behalf of the data controller. So, while the controller makes the decisions relating to the processing it is the processors themselves who carry out the relevant tasks on the controller's behalf. The definition covers service providers; such as cloud computing providers who act under the direction of data controllers. The GDPR has extended the liability regime and places direct obligations on data processors. They, for example, need to maintain a record of all categories of processing activities carried out on behalf of a controller, notify controllers of any data breach without undue delay and, where required, implement security measures such as encryption and pseudonymisation.

7.2.2 Who do you answer to?

7.2.2.1 Supervisory Authority

Each Data Controller and Data Processor will answer to the national data protection regulator in which they are located. These bodies are called 'Supervisory Authority' and there can be more than one existing in a member state. It is their role to protect the rights of the Data Subject and protect the free flow of personal data within the Union.

This body will have the power to enforce the legislation and issues fines.

For example, in the UK, the supervisory authority is called the Information Commissioners Office (ICO). Please refer to their website for more information:

http://ico.org.uk

7.2.2.2 European Data Protection Board (EDPB)

The EDPB is a European structure ensures that the GDPR is applied consistently throughout the EU by member states and their relevant Supervisory Authority. It will also issue guidelines, provide opinions on codes of conduct and undertake dispute resolution between supervisory authorities.

7.3 Is what you are proposing lawful?

Before we start to look into how your project will process the data, you will need to consider if the collection and use of the data is lawful as well as fair and transparent.

The project needs to ensure that it can demonstrate that it has a legitimate reason to process personal data.

7.3.1 Consent

The project should obtain the consent of the data subjects prior to gathering any data. The GDPR states that this must be "freely given, specific, informed and unambiguous".

Given that your project will access data in an automated manner by accessing the interface to each online social media to request information, then you will be relying on the agreement that has been undertaken between the data subject and the social media organisation.

There is not one standard interface and so each social media organisation will require you to register for access to their individual data feed. During the registration process you will need to accept that organisations terms and conditions of use which may (and does) change from time to time.

It is necessary for you to read the terms to this interface to understand what data you are allowed to keep and display. We also advise that you read the terms that the data subject will sign up to when they create their personal account.

This is an important part of adopting a "Privacy by Design" approach to your processing architecture in order to make it flexible and responsive changes in the privacy requirements of the online social network.

If the project scrapes data from websites, then you must ensure the provenance of the data and ensure that you comply with the terms and conditions of that site.

7.3.2 Transparency

Your data processing should be seen as fair and transparent. Here the onus will be on you to explain by providing "*information notices*" (e.g., on the project website, literature, publicity) describing the fundamentals of how you collect data, handle data, retain and disseminate that data.

Clearly state:

- the contact detail of the data controller and where appropriate their data protection officer (DPO)
- the purpose of collection and processing data
- how the processing will respect the principle of data minimisation
- how long data will be retained
- if you intend to transfer data outside of the internally
- the rights of the individual under GDPR
- the source of the data where possible
- the citizens' data access rights (see section 7.5)

7.3.3 Special Categories of Personal Data

The GDPR expanded the definition of sensitive data ("*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership*") to include "*the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*". This type of processing is prohibited unless:

- the data subject has given explicit consent
- processing relates to personal data which are manifestly made public by the data subject
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

From the point of view of the EmerGent project, these exceptions are important. A full list of exceptions can be found in GDPR Article 9.

Note: Each member state may add further conditions and limitation with regard the processing of genetic data, biometric data or data concerning health in relation to sensitive data.

7.4 Data rights of the citizen

The GDPR makes explicit the rights of the citizen over the processing and storage of their personal data which has implications in data is stored and accessed in response.

7.4.1 Subject Access Request

The *right of access by the data subject* to the data held on them and information related to it is enshrined in Article 15 and allows for confirmation by the project whether it is processing the subject's personal data, in which case the project shall also be required to provide access to the data as well as providing:

- *the purposes of and legal basis for the processing;*
- *the categories of personal data concerned;*
- *the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;*
- *where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
- *the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;*
- *the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;*
- *communication of the personal data undergoing processing and of any available information as to their origin*

Note: It is a requirement that this information is communicated within *one month* of the request and in cases where there are any issues of complexity or a high number of requests then it can be extended by a further two months.

7.4.2 Right of Erasure

Under the *right of erasure*, data subjects have a right to ask the data controller to erase their data if they withdraw their consent or if the data is no longer necessary for the project's stated purpose.

The project board could potentially argue that the data is of public interest although the project board may consider any potential publicity counterproductive.

7.4.3 Data Portability

Data portability is a right that the data subject has allowing them to request a copy of their personal data in a "structured, commonly used and machine-readable format". So in addition to deleting any data under the right to erasure, the project will need to define methods by which data can be exported an acceptable format. The data subject will have the option of asking the project to transmit the data to another data controller (if feasible).

7.5 Project controls

In this chapter, we introduce the controls that we have implemented to manage the requirements of the GDPR.

7.5.1 Data protection officer

A data protection officer (DPO) is required to be appointed if, for example, the processing requires "*regular and systematic monitoring of data subjects on a large scale*" which describes the nature of projects collecting and mining data from a number of social media networks.

The ICO guidance on appointing a DPO states "The important thing is to make sure that someone in your organisation, or an external data protection advisor, takes proper responsibility for your data protection compliance and has the knowledge, support and authority to do so effectively. Therefore, you should consider now whether you will be required to designate a DPO and, if so, to assess whether your current approach to data protection compliance will meet the GDPR's requirements."

If your project has a number of partners then, the DPO should report directly to the Project Board. Measures must be put into place to allow each partner to access the DPO and his or her services on an equal basis. This article also states that the DPO shall be chosen on the "basis of professional qualities" and in particular "expert knowledge of data protection law".

The project should ensure that data subjects may contact the DPO about processing of their data, such as right of access, right of erasure and subject access requests.

DPO shall have at least the following tasks:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations
- to monitor compliance with the GDPR, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;

- to cooperate and act as the point of contact with the supervisory authority;
- The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

The DPO must be provided with all required resources to complete these tasks and must not be directly given instructions by data controllers and processors; the independence of the data protection officer is crucial.

Currently all these functions (with the exception of cooperation with the *supervisory authority* are undertaken by the internal Ethics Advisory Committee (EAC).

7.5.2 Privacy impact assessment

A new element of the GDPR is a requirement for data controllers and data processors to conduct a Privacy Impact Assessment (PIA) with the aim of ensuring that potential issues with respect to DPP are assessed and managed appropriately.

On the EmerGent project we incorporated a project-wide PIA from inception that allowed us to adopt a 'Privacy by Design' approach. The PIA is used as a control for the EmerGent project and implemented through a structure on the Emergent SharePoint document management system called the EmerGent "Privacy Risk Register" (EPRR). As part of the management of potential issues we incorporated a review of risks in every meeting agenda, as part of deliverables creation process as well as having a work stream dedicated to privacy.

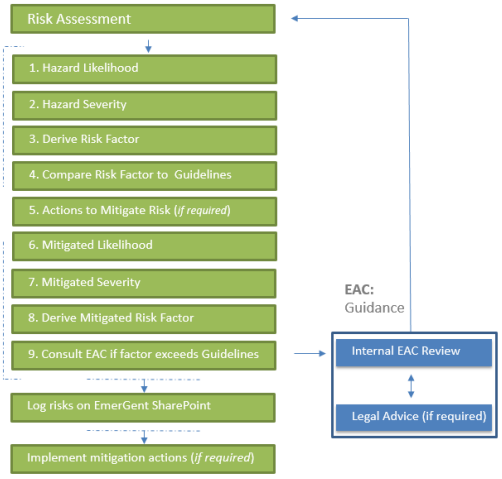


Figure 8: Risk Assessment for each identified hazard

The SWIFT based risk management technique was key to the assessment of risk to allow mitigated high risk items to be raised to the projects EAC as well as the project board. Figure 8 describes the EmerGent project's implementation risk management as part of the PIA.

7.5.3 Continuous monitoring

Due to the evolving nature of the internet, new online social networks will arise, DPP legislation will change with the full adoption of GDPR and guidelines will be issued on how to how to interpret the legislation and terms of use will be change for existing networks.

This presents a management challenge to ensure that your project's DPP controls keep pace with the changes and it has a mechanism to review and adapt to their effects.

7.5.3.1 Legislation and guidelines

The project should schedule tasks and allocate resource to monitor the development of legislation in member states and guides issued by the relevant supervisory authority on how to approach DPP. For example, the GDPR has made provision for the supervisory authority to develop a code of conduct with related certification which should be implemented by the project when available. For further details on codes of conduct please refer to section 7.6.2.

7.5.3.2 Social network terms of use

The project will rely heavily on the terms and conditions of each online social network from which you collect data. It is imperative that when you respond to changes in terms in a manner and timescale that ensures that the project complies not just with the terms but also how they impact on the GDPR.

We would suggest that a project control is created that record the online social network, the project's registration details, a copy of the terms, project compliance with the terms. This should be reviewed annually in case the project's implementation has changed or when the terms are updated.

Responding to changes in terms can be onerous and time-consuming, especially as some social networks issue new terms of use on a short basis – we have seen less than a week in some cases. This may be compounded if a member state issues legislation that has a knock on effect to one or more social networks. It is therefore important that the project builds in technical capability by adopting the "Privacy by Design" approach to respond to these changes to minimise the operational impact.

7.6 Infrastructure controls

7.6.1 Privacy by design

7.6.1.1 Technical and Administrative Security

Data protection needs proper technical and administrative measures corresponding with the risk to the security and misuse of personal data. Some prospective measures are:

- data access control (authentication and authorisation);
- system controls (ensuring that the application and web servers and software are maintained and regularly patched);
- secure data transmission (ensuring that data is encrypted in transit);
- data entry control (keeping track of who does what);
- contractual control (logical or physical separation of data from different customers);
- availability controls (protecting against unauthorised destruction or loss)

7.6.1.2 Pseudoanonymisation

Alongside encryption, pseudoanonymisation is an appropriate measure by which to uphold security of processing under Article 32. Pseudoanonymisation is the technique where a

specific attribute of a data record is transformed such that the data subject cannot be directly identified, without the use of additional information that is not contained in the record.

It is important to consider how to implement pseudoanonymisation on such variable data as social media posts. The scope of the technique should really form a cornerstone of your Privacy by Design rather than an afterthought. Although it should be noted that it is not a panacea for all your responsibilities to the GDPR. In particular, it is important to note the pseudoanonymised data is still considered to be personal data, and therefore subject to be treated as such, if it can be linked to a data subject (GDPR Recital 26): "*Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*".

7.6.1.3 Scope creep

As discussed earlier, the GDPR requires that your project undertakes processing in a transparent manner which is clearly described in official notifications. This will detail the scope and boundaries of the processing and use together with the length of time.

It is important that the design ensures that the scope of the processing does not exceed the project's stated boundaries. So if the stated aim of the project is to aggregate data to disseminate to emergency services aiding them in handling an incident then the project should ensure that users are not able to use the system for any other purpose.

7.6.1.4 Secure systems and transmission

Follow best practice when handling, storing and transmitting data, as well as providing external access to it. For instance:

- Internal systems should not be exposed to the internet except through designated firewall protected gateways
- All data is securely transmitted.
- Access control levels are created to ensure that personnel are able to view or modify information that for which they have been approved.

Where possible, ensure that all systems in the project's architecture include forensic ready evidence storage to aid the investigation into the reasons and extent of any breaches.

7.6.2 Codes of Conduct

The introduction of the GDPR brings with it the potential for an increased workload by supervisory authorities (potentially lower tolerance for breach notifications, increased subject access requests due to wider privacy expectations, the legal interaction resulting from fine increases). Compliance could be demonstrated if the project can show an adherence to an approved code of conduct or an approved certification mechanism.

Articles 40 and 42 allow Member states and supervisory authorities (such as the ICO in the UK, European Data Protection Board, etc.) to work with market bodies or interest associations (representing categories of controllers and processors) to produce a certification structure that will support code of conduct. Under Article 40 these codes of conduct should include:

- fair and transparent processing
- the legitimate interests pursued by controllers in specific contexts
- the collection of personal data
- the pseudonymisation of personal data
- the information provided to the public and to data subjects
- the exercise of the rights of data subjects
- the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained
- the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32
- the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects
- the transfer of personal data to third countries or international organisations
- out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects

In the UK, the ICO has been working on a privacy seal to be launched in 2016. This kitemark would be "awarded to organisations that demonstrate that they are not only meeting, but also surpassing, the requirements of the Data Protection Act when it comes to looking after people's information" [WWW12]. ICO expects three main benefits from this scheme:

- The awarding of a seal will help to promote organisations that are going above and beyond the call of duty when it comes to looking after people's information, giving them an opportunity to gain an advantage over their competitors.
- The seal will help to build consumer trust and choice, as it will demonstrate that an organisation is looking after their information to a notably high standard.
- More widely, the seal will raise the bar for privacy standards across the UK by incentivising good practice.

As the structures supporting codes of conduct and certificates (such as the ICO privacy seals) solidify over the next two years across Europe, any system like EmerGent that collects personal data will be expected to seek out an appropriate code of conduct to comply with the respective requirements and undergo audits by accredited organisations.

7.6.3 Breach handling

Under Article 34, data controllers must communicate a breach of personal data to Supervisory Authority. Also, the data subject should be informed if the breach results in a high risk to the data subject's rights and freedoms. This may not be required if, for example, the data has been properly encrypted or if the communication would involve disproportionate effort.

The project should design a process that will be enacted if it discovers or is notified of a data breach. In order to ensure familiarity, this should be based upon your project's other controls, consisting of a risk register and allowing for both mitigation and communication plans. An outline breach management workflow is described in Figure 9.

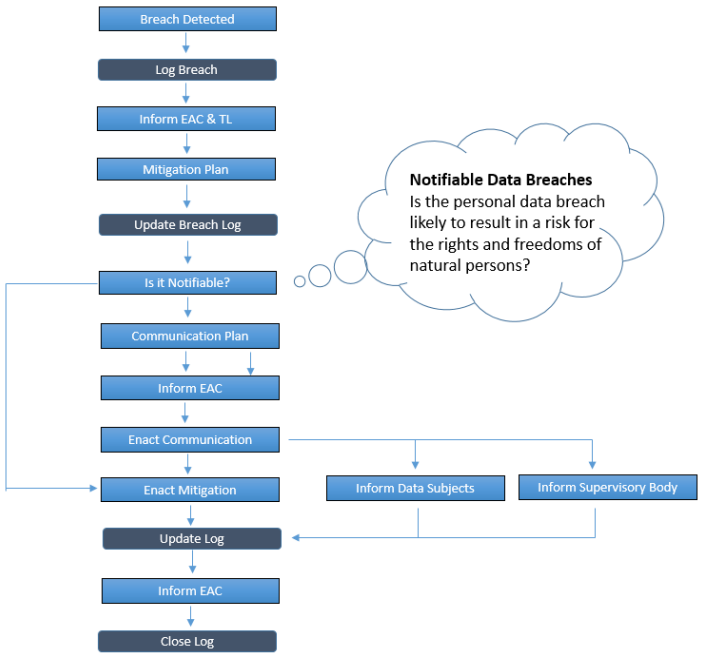


Figure 9: Data breach management

Note: On the EmerGent project the Ethics Advisory Committee (EAC) focuses on oversight of the projects data privacy & ethics approach, procedures and tools. It would work closely with the relevant Task Leader (TL) in order to shape the response to a breach. The EAC also contains an external DPP legal expert that it can call upon to verify the response, if necessary.

In practice, a breach will be notified to the project coordinator and when appointed, the project DPO. They immediately log the breach on the project control and then inform the internal EAC and relevant Team Leader. The risks should be assessed and a mitigation plan should be designed and the log updated accordingly.

Depending upon the breach, the team develop a communication plan so that the project can inform the relevant Supervising Authority of the breach and any affected data subjects how they have been affected as well as the plan that the project will undertake to mitigate the effects of the breach.

The nature of the personal data breach in relation to the risks to the "rights and freedoms of natural persons" directs the decision as to whether a communication plan is required. In practice, it is advisable to role play a number of potential scenarios so that the impact on the project can be gauged and formal responses (including communication plans) can be prepared.

7.6.4 SAR handling

Considering the breadth of social media and the number of people posting messages, there is the potential for SAR handling to overwhelm a purely manual process.

For EmerGent, we use a project control to record and support the administration of the process for any SAR received

In practice, the request will be received by the project coordinator or the DPO who would then log the details on the project control and delegate responsibility to the appropriate team

leader(s) to undertake the request. Due to the short turnaround time that is required by the legislation (refer to section 7.4.1), both the EAC and work package leaders should be informed of the nature of the SAR. The EAC will advise the work package leader if it needs to be escalated to the Project Board.

It is an important to include in the task a process to ensure that the SAR originates from a data subject whose identity can be verified.

The nature of the SAR will dictate the work that will need to be completed. This can be a matter of:

- running a number of reports and sending them to the citizen
- to preparing data for export
- deleting a personal information in transaction and archive data stores
- correcting any information that is incorrect

These technical tasks can be quite involved and so it is important that the handling of the request is included in the overall processing architecture at design time using the *Privacy by Design* approach.

8 Annex III: Publication and dissemination of guidelines

The developed guidelines need to be published and disseminated so that many organisations and citizens can use them. This chapter deals with this question. In the course of this, it has to be differentiated between how to publish and where to publish the guidelines. Section 8.1 deals with possibilities how guidelines could be prepared for the dissemination whereas section 8.2 gives suggestions where the different formats can be advertised.

8.1 How to publish guidelines

There are many possibilities to publish guidelines for the use of social media in emergency situations to different target groups, in which every organisation needs to decide the right way depending on their operation area. EmerGent establishes a set of guidelines for public authorities and citizens. These guidelines can be the base for other organisations to develop their guidelines adapted to their work and target group. The following possibilities to release guidelines are suggestions but need to be tailored to the target group and basic conditions. In general, the guidelines for citizens should be short, straightforward and easy to remember, whereas the guidelines for public authorities should be detailed and include all necessary information to handle social media. **Table 5** shows some suggestions how such guidelines could be published in which guidelines for public authorities and guidelines for citizens will be distinguished. These suggestions will be specified in the following sections.

Table 5: Possibilities how to release guidelines

How guidelines could be published		Guidelines for emergency services & public authorities	Guidelines for citizens
Printed	Full text document	✔	
	Handout	✔	
	Poster		✔
Digital	Full text document	✔	(✔)
	Handout	✔	✔
	"Interactive" internet pages		✔
	Video	(✔)	✔
	Including into existing "emergency apps"		✔
Seminars, information events, workshops		✔	

✔: suitable; (✔): limited suitable

8.1.1 Full-text version of the guidelines (printed and digital)

Description: Full-text version means a detailed listing of all guidelines as it is given with the guidelines in chapter 4 and 5. These documents could be published as book, as a PDF-Document or as flowing text on the internet.

Examples: Next to EmerGent's guidelines see COSMIC's guidelines [WWW23] for the use of new media by public and private organisations [HSGM+14] as well as by the public [HVGS+14].

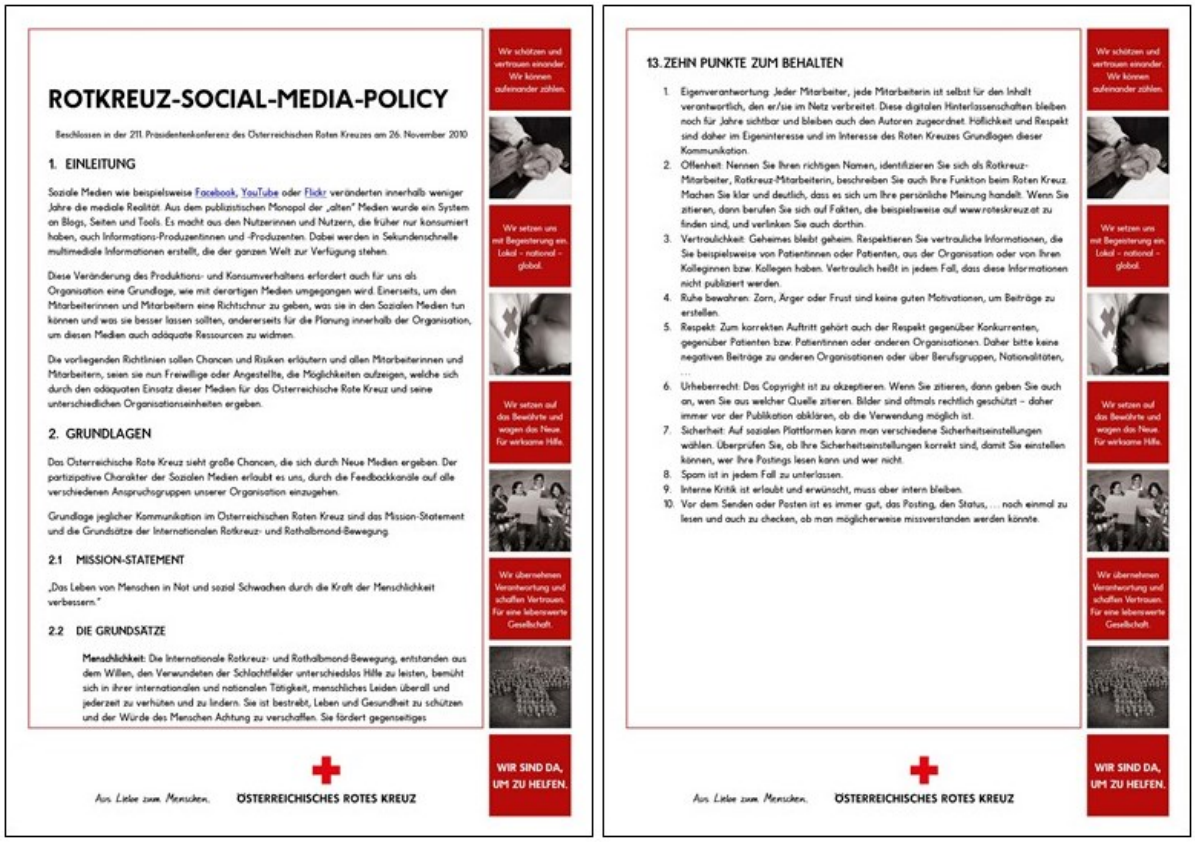
Guidelines for emergency services and public authorities: Emergency services and public authorities should have access to a detailed version of the guidelines. They are the operating actors in social media and responsible for a successful support of the emergency management through social media. The guidelines in printed form could be handed over with the contract of employment or similar to ensure every employee knows them. Additional the guidelines could be published in digital form on the intranet so that everyone has access to them anytime.

Guidelines for citizens: For the release of guidelines for citizens, full text documents are only conditionally suitable. Guidelines for citizens should be short and simple so that citizen can easy remember the content. So it is more expedient to use hand-outs for spreading them. Additional the spreading of printed documents is difficult to cope in most instances. Maybe a digital full text document with detailed information for interested people may be published on the website but this should happen only additionally to other ways of publishing the guidelines for citizens. Independently to the publishing of a full text version it should exist because public authorities should also know the content of guidelines for citizens to incorporate it into their work with social media.

8.1.2 Hand-outs (printed and digital)

Description: Hand-outs should contain a short and easy to remember version of the corresponding guidelines so that they serve as a reference book. Short handouts may help remember the guidelines while working with social media.

Examples: Concerning the layout see the social media Policy of the Austrian Red Cross (especially the last page on the right in Figure 10) [ARC10] as well as the guidelines from the "Federal Agency for Technical Relief" (THW) from Germany (see Figure 11) [BTHW11].



ROTKREUZ-SOCIAL-MEDIA-POLICY

Beschlossen in der 211. Präsidentenkonferenz des Österreichischen Roten Kreuzes am 26. November 2010

1. EINLEITUNG

Soziale Medien wie beispielsweise Facebook, YouTube oder Flickr veränderten innerhalb weniger Jahre die mediale Realität. Aus dem publizistischen Monopol der „alten" Medien wurde ein System an Blogs, Seiten und Tools. Es macht aus den Nutzerinnen und Nutzern, die früher nur konsumiert haben, auch Informations-Produzentinnen und -Produzenten. Dabei werden in Sekundenschnelle multimediale Informationen erstellt, die der ganzen Welt zur Verfügung stehen.

Diese Veränderung des Produktions- und Konsumverhaltens erfordert auch für uns als Organisation eine Grundlage, wie mit derartigen Medien umgegangen wird. Einerseits, um den Mitarbeiterinnen und Mitarbeitern eine Richtschnur zu geben, was sie in den Sozialen Medien tun können und was sie besser lassen sollten, andererseits für die Planung innerhalb der Organisation, um diesen Medien auch adäquate Ressourcen zu widmen.

Die vorliegenden Richtlinien sollen Chancen und Risiken erläutern und allen Mitarbeiterinnen und Mitarbeitern, seien sie nun Freiwillige oder Angestellte, die Möglichkeiten aufzeigen, welche sich durch den adäquaten Einsatz dieser Medien für das Österreichische Rote Kreuz und seine unterschiedlichen Organisationseinheiten ergeben.

2. GRUNDLAGEN

Das Österreichische Rote Kreuz sieht große Chancen, die sich durch Neue Medien ergeben. Der partizipative Charakter der Sozialen Medien erlaubt es uns, durch die Feedbackkanäle auf alle verschiedenen Anspruchsgruppen unserer Organisation einzugehen.

Grundlage jeglicher Kommunikation im Österreichischen Roten Kreuz sind das Mission-Statement und die Grundsätze der Internationalen Rotkreuz- und Rothalbmond-Bewegung.

2.1 MISSION-STATEMENT

„Das Leben von Menschen in Not und sozial Schwachen durch die Kraft der Menschlichkeit verbessern."

2.2 DIE GRUNDSÄTZE

Menschlichkeit: Die Internationale Rotkreuz- und Rothalbmond-Bewegung, entstanden aus dem Willen, den Verwundeten der Schlachtfelder unterschiedslos Hilfe zu leisten, bemüht sich in ihrer internationalen und nationalen Tätigkeit, menschliches Leiden überall und jederzeit zu verhüten und zu lindern. Sie ist bestrebt, Leben und Gesundheit zu schützen und der Würde des Menschen Achtung zu verschaffen. Sie fördert gegenseitiges

Aus Liebe zum Menschen. ÖSTERREICHISCHES ROTES KREUZ

Wir schätzen und vertrauen einander. Wir können aufeinander zählen.

Wir setzen uns mit Begeisterung ein. Lokal – national – global.

Wir setzen auf das Bewährte und wagen das Neue. Für wirksame Hilfe.

Wir übernehmen Verantwortung und schaffen Vertrauen. Für eine lebenswerte Gesellschaft.

WIR SIND DA, UM ZU HELFEN.

13. ZEHN PUNKTE ZUM BEHALTEN

1. Eigenverantwortung: Jeder Mitarbeiter, jede Mitarbeiterin ist selbst für den Inhalt verantwortlich, den er/sie im Netz verbreitet. Diese digitalen Hinterlassenschaften bleiben noch für Jahre sichtbar und bleiben auch den Autoren zugeordnet. Höflichkeit und Respekt sind daher im Eigeninteresse und im Interesse des Roten Kreuzes Grundlagen dieser Kommunikation.
2. Offenheit: Nennen Sie Ihren richtigen Namen, identifizieren Sie sich als Rotkreuz-Mitarbeiter, Rotkreuz-Mitarbeiterin, beschreiben Sie auch Ihre Funktion beim Roten Kreuz. Machen Sie klar und deutlich, dass es sich um Ihre persönliche Meinung handelt. Wenn Sie zitieren, dann berufen Sie sich auf Fakten, die beispielsweise auf www.roteskreuz.at zu finden sind, und verlinken Sie auch dorthin.
3. Vertraulichkeit: Geheimes bleibt geheim. Respektieren Sie vertrauliche Informationen, die Sie beispielsweise von Patientinnen oder Patienten, aus der Organisation oder von Ihren Kolleginnen bzw. Kollegen haben. Vertraulich heißt in jedem Fall, dass diese Informationen nicht publiziert werden.
4. Ruhe bewahren: Zorn, Ärger oder Frust sind keine guten Motivationen, um Beiträge zu erstellen.
5. Respekt: Zum korrekten Auftritt gehört auch der Respekt gegenüber Konkurrenten, gegenüber Patienten bzw. Patientinnen oder anderen Organisationen. Daher bitte keine negativen Beiträge zu anderen Organisationen oder über Berufsgruppen, Nationalitäten, ...
6. Urheberrecht: Das Copyright ist zu akzeptieren. Wenn Sie zitieren, dann geben Sie auch an, wen Sie aus welcher Quelle zitieren. Bilder sind oftmals rechtlich geschützt – daher immer vor der Publikation abklären, ob die Verwendung möglich ist.
7. Sicherheit: Auf sozialen Plattformen kann man verschiedene Sicherheitseinstellungen wählen. Überprüfen Sie, ob Ihre Sicherheitseinstellungen korrekt sind, damit Sie einstellen können, wer Ihre Postings lesen kann und wer nicht.
8. Spam ist in jedem Fall zu unterlassen.
9. Interne Kritik ist erlaubt und erwünscht, muss aber intern bleiben.
10. Vor dem Senden oder Posten ist es immer gut, das Posting, den Status, ... noch einmal zu lesen und auch zu checken, ob man möglicherweise missverstanden werden könnte.

Aus Liebe zum Menschen. ÖSTERREICHISCHES ROTES KREUZ

Wir schätzen und vertrauen einander. Wir können aufeinander zählen.

Wir setzen uns mit Begeisterung ein. Lokal – national – global.

Wir setzen auf das Bewährte und wagen das Neue. Für wirksame Hilfe.

Wir übernehmen Verantwortung und schaffen Vertrauen. Für eine lebenswerte Gesellschaft.

WIR SIND DA, UM ZU HELFEN.

Figure 10: Page 1 and 5 from [ARC10] as example for a handout

Technisches Hilfswerk

Bundesanstalt Technisches Hilfswerk
Verhalten in sozialen Netzwerken

Öffentliche Wahrnehmung
Soziale Netzwerke wie Facebook, Google+, Twitter, Youtube und andere mehr bieten neue Möglichkeiten, im Internet Meinungen, Erfahrungen und Gedanken auszutauschen.

Täglich wird über das THW im Internet berichtet und diskutiert. Da jeder THW-Angehörige durch seine Äußerungen in sozialen Netzwerken die öffentliche Wahrnehmung des THW beeinflussen kann, sind folgenden Punkte zu beachten:

Für sich selbst sprechen
Offizielle Stellungnahmen, Mitteilungen und Berichte werden in sozialen Netzwerken ausschließlich von den dafür befugten Personen (siehe Geschäftsordnung) getätigt. Sprechen Sie nur für sich selbst und benutzen Sie „ich" statt „wir", um Ihre persönliche Meinung von offiziellen Aussagen abzugrenzen.

Sie sind selbst verantwortlich
Bedenken Sie vor Veröffentlichung mögliche Folgen Ihres Handelns. Sie selbst sind dafür verantwortlich und beeinflussen durch Ihre Aussagen möglicherweise die öffentliche Wahrnehmung des THW.

Beachten Sie unsere Werte
Das THW begegnet allen Menschen offen und vorurteilsfrei und fördert eine tolerante und weltoffene Haltung, heißt es im siebten Leitsatz des THW. Diese Werte gelten selbstverständlich ebenso im Internet und in sozialen Netzwerken.

Respekt gilt auch im Netz
Ein höfliches Miteinander und ein respektvoller Umgang wird auch im Internet erwartet. Bedenken Sie Ihre Aussagen vor der Veröffentlichung und beachten Sie, dass Ironie und Sarkasmus ohne Mimik und Gestik im Internet oft nicht richtig verstanden werden.

Transparenz zeigen
Machen Sie sich, wenn Sie sich zu THW-Themen äußern, als THW-Mitglied erkennbar. Bewahren Sie Ihre Objektivität und bleiben Sie sachlich.

Privatsphäre schützen
Veröffentlichungen im Internet sind häufig für alle einsehbar und können selten wieder gelöscht werden. Schützen und wahren Sie Ihre eigene Privatsphäre sowie die anderer Personen.

Interne Informationen
Geben Sie keine Informationen weiter, die nicht für die Öffentlichkeit bestimmt sind. Dies gilt besonders, wenn diese durch das Kürzel „VS-NfD" (Verschlusssache — Nur für den Dienstgebrauch) gekennzeichnet sind. (siehe Geschäftsordnung)

Einheitliche Argumentation
Schwierige Themen erfordern eine einheitliche Kommunikation, um ein stringentes Bild in der Öffentlichkeit zu erzeugen. Beachten Sie deshalb die Argumentationshilfen der THW-Leitung, die diese zu bestimmten Themen wie zum Beispiel der Aussetzung der Wehrpflicht herausgibt.

Das Internet ist „live"
Zentraler Bestandteil des Internets und sozialer Netzwerke ist deren Schnelllebigkeit. Moderne Handys ermöglichen es, in wenigen Sekunden Bilder und Texte über Twitter und Facebook zu veröffentlichen. **Beachten Sie, dass die Nutzung solcher Möglichkeiten während eines Einsatzes nicht gestattet ist.** Ausnahmen können Auslandseinsätze sein. Dies muss jedoch durch die THW-Leitung genehmigt werden.

Gesetze gelten auch im Netz
Die Gesetze der Bundesrepublik gelten auch im Internet. Verletzungen des Urheberrechts werden zum Teil streng geahndet. Veröffentlichen Sie deshalb nur Bilder, Texte und Videos, die sie selbst produziert haben. Achten Sie bei der Veröffentlichung von Fotos vor allem auf das „Recht am eigenen Bild".

Nutzen Sie das Extranet
Nutzen Sie die Möglichkeiten des Extranets. Interne Fachgespräche und konstruktive Kritik sind im THW herzlich willkommen, haben in sozialen Netzwerken jedoch nichts zu suchen. Sie können dem öffentlichen Bild des THW schaden. Tragen Sie daher Konflikte, die das THW und handelnde Personen betreffen, nicht in sozialen Netzwerken aus.

Unterstützen Sie uns
Facebook und Twitter bieten eine unüberschaubare Menge an Informationen. Stoßen Sie auf Lob, Kritik oder für das THW interessante Themen, leiten Sie diese an Ihren Beauftragten für Öffentlichkeitsarbeit, Ihren Landesverband oder die THW-Leitung weiter.

Besuchen Sie unsere offiziellen Seiten unter:

www.facebook.com/thw
www.facebook.com/reininsthw
www.gplus.to/thw
www.youtube.com/thwleitung
www.twitter.com/thwleitung
www.twitter.com/thwpresse

Stand: Dezember 2011

Kontakt und Informationen:
Bundesanstalt Technisches Hilfswerk
Provinzialstraße 93
53127 Bonn
E-Mail: oeffentlichkeitsarbeit@thw.de
www.thw.de

www.thw.de

Figure 11: [BTHW11] as example for a handout

Guidelines for emergency services and public authorities: Hand-outs can be published both printed and digital. Printed copies could be handed over with the contract of employment too, as part of seminars or similar. Additionally, the hand-outs could be hung at the bulletin board, maybe with a reference to the full text document (e. g. as QR-Code, see Figure 12). Digital versions should be accessible for example on the intranet or spread out with a newsletter to draw attention on the new guidelines for handling social media.

Figure 12: Example QR-Code [WWW04]

Guidelines for citizens: Handouts with guidelines for citizens should be accessible in a digital version to transfer basic information about using social media in emergency situations in a short and easy to remember way. Printed versions are, similar to the full text documents, not suitable for presenting citizen guidelines. But maybe as part of local information events printed handouts could be distributed.

8.1.3 Poster

Description: Poster means a useful preparation of basic information in a simple and visual appealing way. Posters should be used as an assistance to recall already known information and to promote new content.

Examples: See Figure 13 and **Figure 14** for simple and rememberable posters.

Figure 13: Poster "15 'Dos' for Pinterest" [WWW02]

Figure 14: Poster "Before you post: THINK" [WWW03]

Guidelines for emergency services and public authorities: Posters are not suitable for presenting guidelines to emergency services because the content on posters should be very short. But emergency services and public authorities need to have detailed information to enable an appropriate dialogue.

Guidelines for citizens: Posters can mediate content in a memorable and simple way. With an appealing design it is possible to raise the awareness of citizen of the guidelines and promote the content. Maybe it could be developed a set of posters in which every poster visualises another rule. As example see **Figure 15**. It shows a set of six posters for a campaign for alcoholic prevention. Maybe the guidelines could be visualised similar to this campaign. For each rule a poster could be designed for the dissemination and promotion of the guidelines. Additional posters should include a reference (maybe in form of a QR-Code because to scan this code is easier than to type a URL) e. g. to the internet page or app where citizen can find detailed information about the guidelines.

Figure 15: Motives of the posters for the campaign for alcohol prevention from the BZgA [BZgA16]

8.1.4 "Interactive" internet pages

Description: Interactive internet pages means a preparation of the full text guidelines for the use on internet pages. This preparation should include every information the full text document includes, but in a sorted and descriptive way.

Examples: Figure 16, Figure 17, Figure 18 and Figure 19 show how COSMIC [WWW23] present their guidelines on their website to the public. COSMIC split their guidelines in guidelines for public authorities and guidelines for citizens.

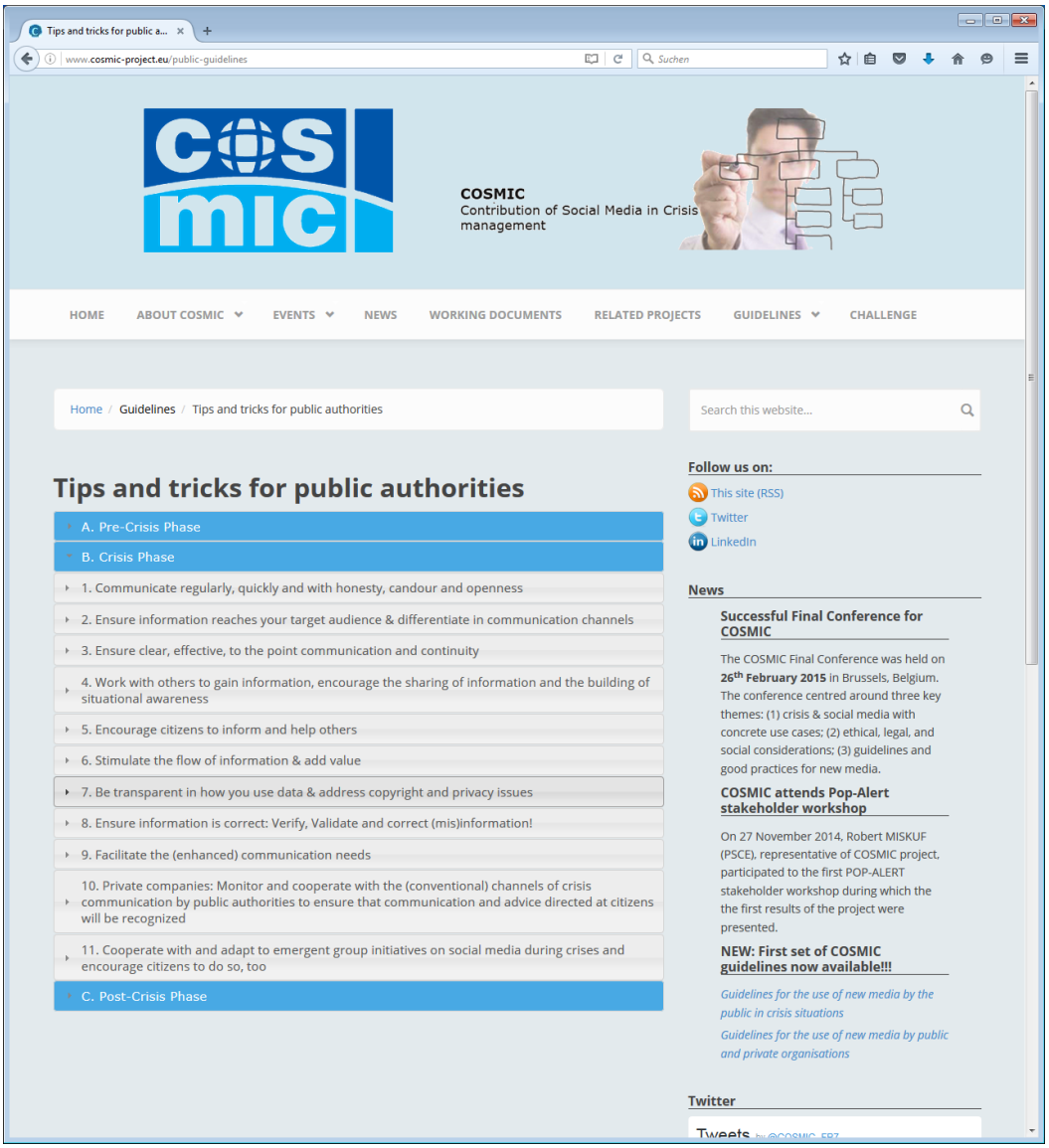


Figure 16: Overview COSMICs preparation of their guidelines for public authorities [COSM14a]

The guidelines for public authorities are divided into guidelines for the Pre-Crisis Phase, Crisis Phase and Post-Crisis Phase. Each of these categories includes different guidelines which are relevant for the corresponding phase (see Figure 16).

Figure 17: Detailed view on COSMICs preparation of their guidelines for public authorities [COSM14a]

The guidelines are constructed as drop-down menu so that the visitors of the internet page can read the guidelines selective (see Figure 17).

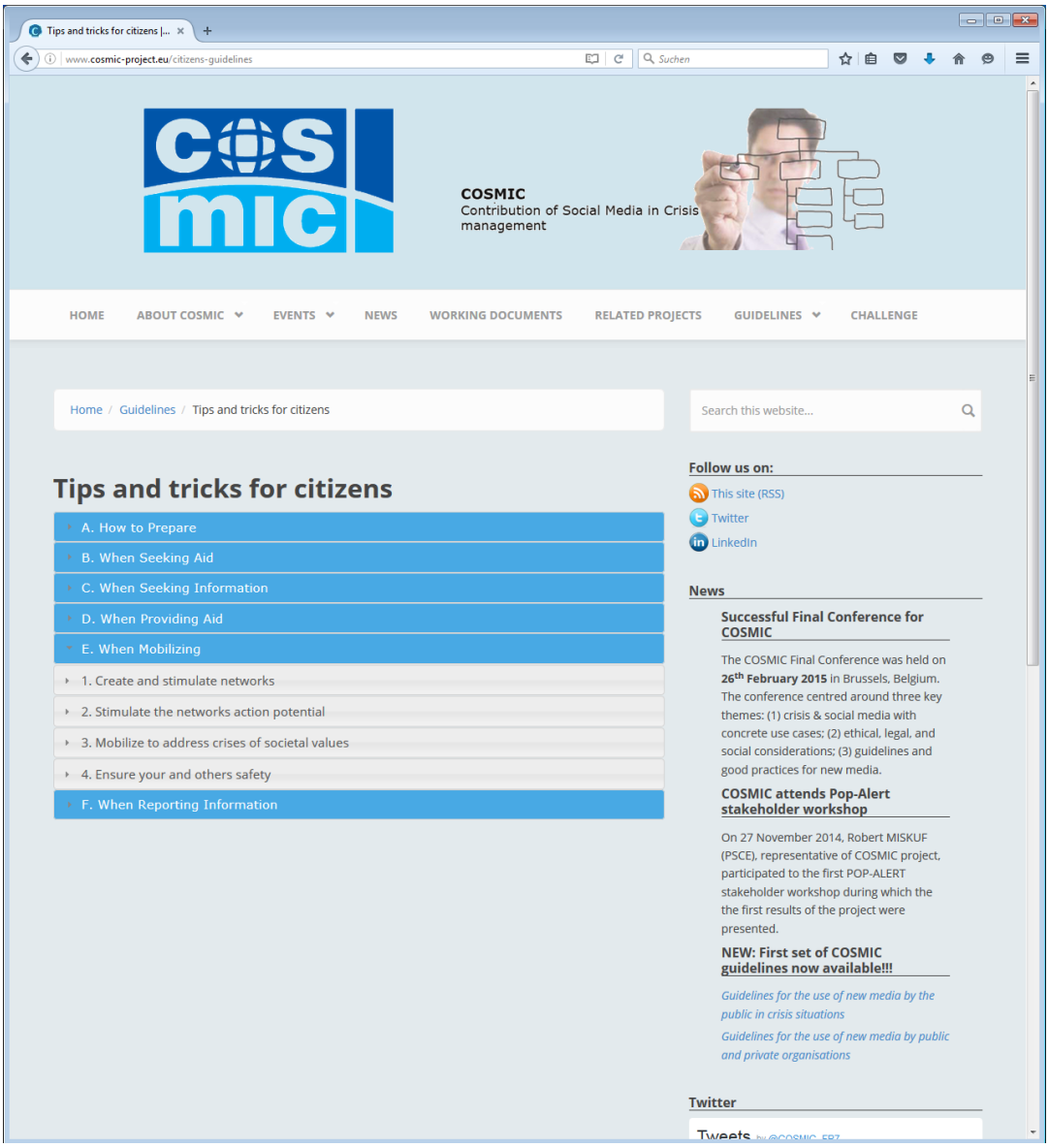


Figure 18: Overview COSMICs preparation of their guidelines for citizens [COSM14b]

The guidelines for citizens have a similar structure. They are split into six sections with the single guidelines as sub-categories of each sections (see Figure 18). Here were used a drop-down structure as well (see Figure 19).

Figure 19: Detailed view on COSMICs preparation of their guidelines for citizens [COSM14b]

Guidelines for emergency services and public authorities: Emergency services and public authorities shouldn't need a preparation of the guidelines in this way because they should know the content of the full text document.

Guidelines for citizens: For the preparation of guidelines for citizens this kind of presentation seems to be very helpful. So citizen don't get an overloaded text document but get a structured version of the guidelines, which still contains the whole content. It should be ensured that the guidelines are retrievable with multiple end devices like tablets or smartphones.

8.1.5 Creating videos

Description: Videos can help to present the content of the guidelines in a short and descriptive way [AuMe16]. Videos should illustrate the gist of the social media guidelines, maybe in a funny way, so that the target group can remember the content easily.

Examples: "Tchibo", a german chain of coffee retailers, published a video with the title "Mr. Bean goes online" (original title "Herr Bohne geht ins Netz", see Figure 20) [Tchi11]. This video shows employees how they should act in social media in a descriptive way.

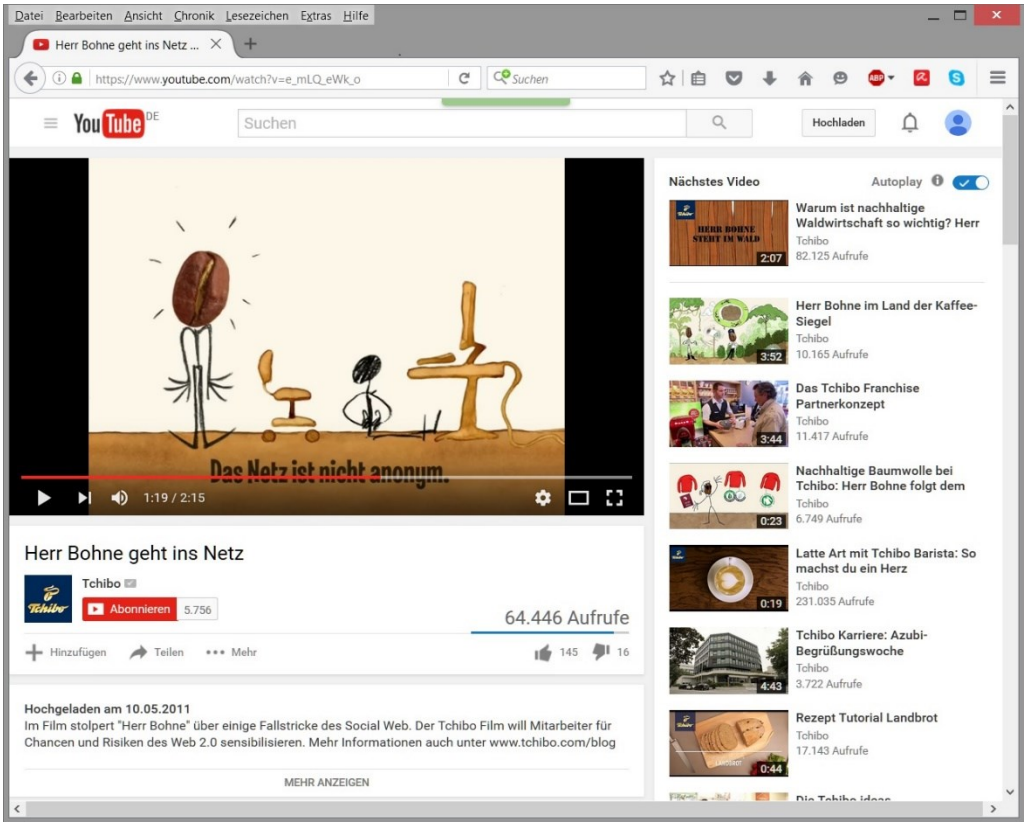


Figure 20: YouTube-Video "Mr. Bean goes online" by Tchibo [Tchi11]

Many other organisations published such videos too. For example, Great-West Life (see Figure 21), a Canadian insurer, and the Linde Group (see Figure 22), a global engineering company.

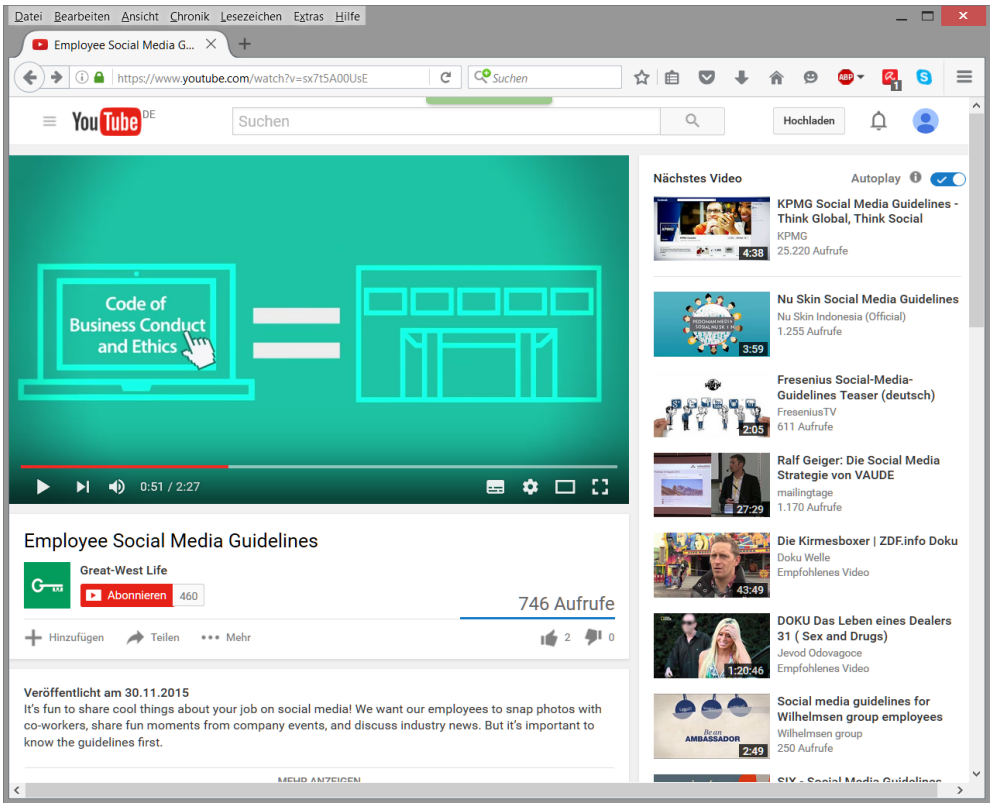


Figure 21: YouTube-Video "Employee Social Media Guidelines" by Great-West Life [GWL15]

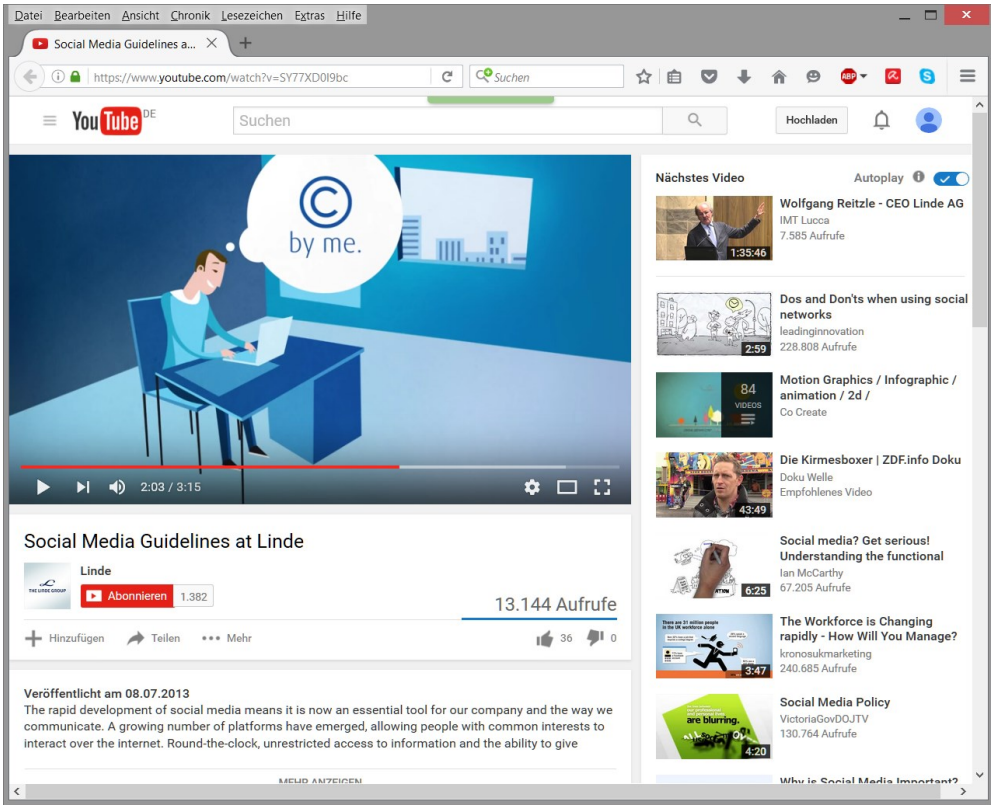


Figure 22: YouTube-Video "Social Media Guidelines at Linde" by Linde [Lind13]

Guidelines for emergency services and public authorities: Videos are limited suitable to present guidelines for emergency services and public authorities. With videos you can't transfer information in detail as it is necessary. Videos could be used for employees who are not regularly using social media. But the employees who are responsible for the different social media channels, who are regularly writing on them and who shall look after them in times of crisis need more detailed information. By publishing videos for public authorities you also have to think about the accessibility (concerning computer access or sound) for your employees [AuMe16]. Additional you need to note that in general changes are not as easy implemented as in text documents [AuMe16].

Guidelines for citizens: Videos could be used to provide the content of the guidelines to the public in a short and attractive way. The content should be short and simple and the video should include a reference where to find further information. Citizen usually have access to a computer or smartphone which can display the video. But the integration of changes might be also a problem. By creating the video, it should be ensured that the video is playable with multiple devices like computer, smartphones or tablets.

8.1.6 Including guidelines in existing "emergency apps"

Some organisations like the "Federal Office for Civil Protection and Disaster Assistance" ("Bundesamt für Bevölkerungsschutz und Katastrophenhilfe" BBK, Germany [WWW24]) or the "Federal Emergency Management Agency" (FEMA, USA [WWW25]) are using "emergency apps" to usually warn people if there is a danger near them or give prevention tips to prepare for possible risks. Examples of such apps are:

- NINA (original title "Notfall-Informations- und Nachrichten-App" – emergency information and news app [WWW26]) is a free app, published by the German "Federal Office for Civil Protection and Disaster Assistance" to warn the public in Germany about risks in their neighbourhood. [BBK16]
- KATWARN is a free warning app for Germany and was published by different organisations [KATW15, p. 5]. KATWARN provides information that there is an incident and how to react [KATW15, p. 3]
- The Federal Emergency Management Agency also published an app for the USA. The FEMA Mobile App focusses on prevention tips and helps citizens to prepare for possible emergency situations.

These apps provide prevention tips, information about how to prepare and react in emergencies, checklists with preparation actions, maps with active warnings, functionality to send textual information or pictures to the authorities, and allow the user to enter locations to receive related warnings. Besides this information, emergency apps could include information from the citizen guidelines to encourage the expected use of social media in emergency situations.

8.1.7 Seminars, information events and workshops

Description: Seminars, information events and workshops are intended for learning the right use of social media. So people may learn in a dialogue with experienced social media users how to write and act in social web.

Examples: On the internet there are many offers for organisations to book different social media seminars and trainings. Also, experienced users may organise them itself and share their knowledge.

Guidelines for emergency services and public authorities: For organisations it could be beneficial to organise seminars about the right use of social media [AuMe16]. So it is possible to convey the content better than just with a brochure [AuMe16]. Especially for organisations where social media was not used until now, in the beginning the focus should be on train the employees and explain the new environment (especially to users who are not using social media until now) and not just on distribute guidelines.

Guidelines for citizens: It is not suitable to organise workshops for citizens because it would be an inappropriate effort to train all interested social media users. Conceivable could be in certain circumstances for organisations to organise workshops which interested people can book. This may work in smaller cities but rather not in a big city.

8.1.8 Final view on the publication of guidelines

There are many possibilities to publish guidelines in which every organisation need to choose the best one depending on kind of work and organisational structures. Not every organisation needs to prepare each of the options above. In general, two points should be considered for choosing possibilities to publish guidelines. At first it is necessary to draw attention to the guidelines. So it is useful to choose one preparation method with maybe lower content but visually appealing. The second point is the transmission of content. Is attention called, the entire content must be taught with detailed documents. For example, it is better to prepare posters (visually appealing) and “interactive” internet pages (detailed content) than just to publish posters and videos (both visually appealing) or full text documents and “interactive” internet pages (both detailed content). The right mix of the suggestions above brings the success.

8.2 Where to publish guidelines

Next to the correct preparation of guidelines it is necessary to choose the right medium to publish guidelines. In dependence on the way of preparation there are different possibilities to share the guidelines with the public. Figure 23 shows suggestions where social media guidelines could be published. There is a distinction in guidelines for public authorities and guidelines for citizens as well as the different possibilities of preparation as they were discussed in the previous subsections.

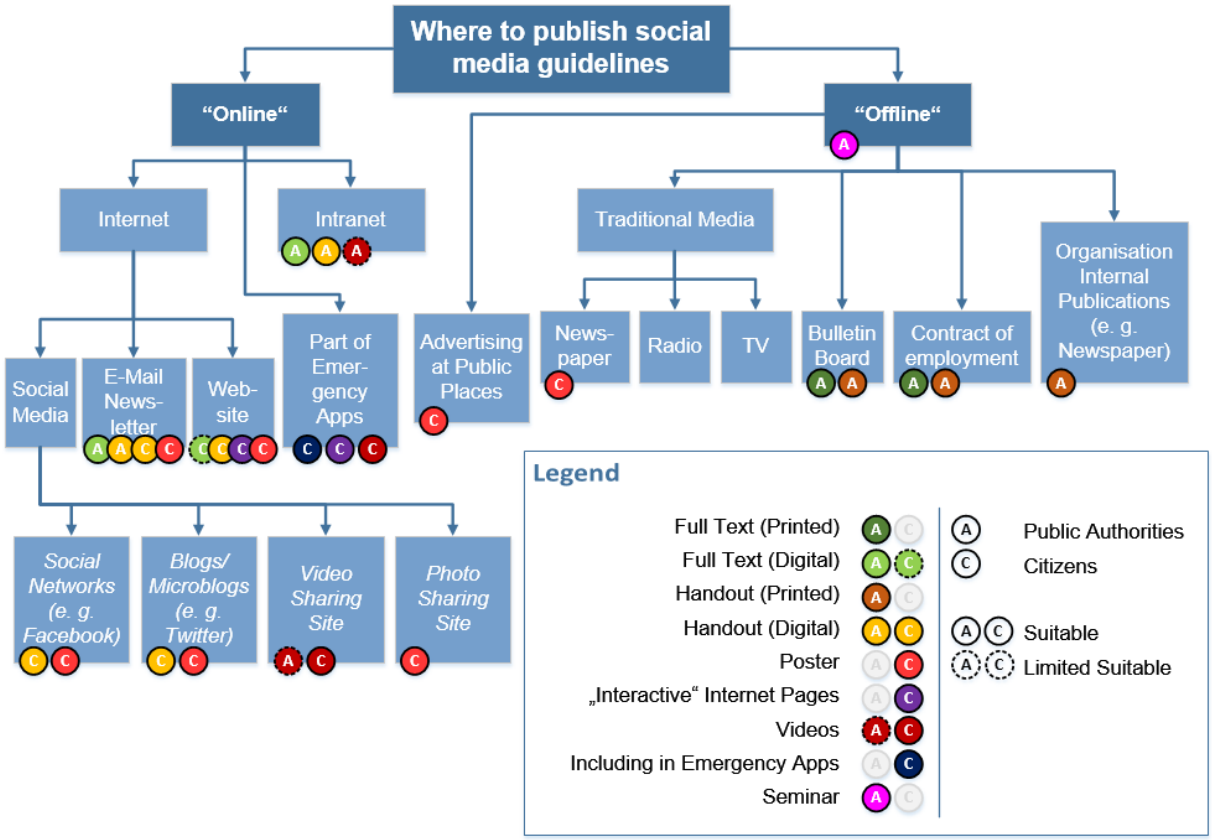


Figure 23: Overview how to disseminate guidelines

The figure only shows suggestions where guidelines could be published. The channels have to be adjusted depending on the organisational structures and target group. Additionally, not every organisation should use any opportunity. If an organisation has no Video-Sharing-Channel yet it shouldn't be set up just for publishing the guidelines. Similarly, not every organisation needs to produce a video to publish their guidelines.

References

[ACTG12] ACT Government: *„ACT Government Social Media Policy Guidelines“*; March 2012; Version 1.0; online available at: http://www.cmd.act.gov.au/__data/assets/pdf_file/0020/312581/Social_Media_Guidelines_-_May_2012.pdf; access: 06.05.2015.

[AFA16] Akerkar, R., Friberg, T., Amelunxen, C., User Requirements, Version 2, Project EmerGent, February 2016, available at: http://www.fp7-emergent.eu/wp-content/uploads/2016/03/20160229_D3.5_RequirementsVersion2_EmerGent_final2.pdf

[ARC10] Austrian Red Cross: „Rotkreuz-Social-Media-Policy“; 26.11.2010; online available at: https://www.roteskreuz.at/fileadmin/user_upload/PDF/Was_wir_tun/Social-Media-Policy.pdf; access: 01.07.2016.

[ARC2.0] American Red Cross, Social Media Engagement Handbook, version 2.0, available at: http://redcrosschat.org/wp-content/uploads/2012/06/SocialEngagementHandbookv2.pdf

[AuMe16] AUSSCHNITT Medienbeobachtung: *“Das Geheimnis erfolgreicher Social Media Guidelines“*; online available at: https://www.ausschnitt.de/sites/default/files/emct/downloads/som_booklet_2013_web.pdf; access: 09.05.2016.

[BBK16] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; *„Warn-App NINA“*; online available at: http://www.bbk.bund.de/DE/NINA/Warn-App_NINA.html; access: 01.07.2016.

[BFW12] Berliner Feuerwehr: *„Social-Media-Guideline – Empfehlungen für einen sicheren Umgang mit sozialen Medien“*; 26.10.2012; online available at: http://www.berliner-feuerwehr.de/fileadmin/bfw/dokumente/Download/2012/2012_01_SM-Guideline.pdf; access: 06.05.2015.

[BITK10] BITKOM: *„Social Media Guidelines – Tipps für Unternehmen“*; 2010; online available at: https://www.bitkom.org/Publikationen/2010/Leitfaden/Social-Media-Guidelines-Tipps-fuer-Unternehmen/BITKOM-SocialMediaGuidelines.pdf; access: 15.06.2016.

[BlKa11] Blank-Gorki, Verena; Karutz, Prof. Dr. Harald: *„Web 2.0: Neue Perspektiven für den Bevölkerungsschutz?“*; in: *„Bevölkerungsschutzmagazin - Geoinformationen – Daten für einen modernen Bevölkerungsschutz“*, 1/2011, p. 24-27, publisher: BBK; online available at:

http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_1_11.pdf?__blob=publicationFile; access: 14.11.2014.

[BMI14] Bundesministerium des Innern: *„Leitfaden Krisenkommunikation“*; August 2014; online available at: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2014/leitfaden-krisenkommunikation.pdf?__blob=publicationFile; access: 14.11.2014.

[BTHW11] Bundesanstalt Technisches Hilfswerk: *„Verhalten in sozialen Netzwerken“*; December 2011; online available at: http://thw-eisenach.de/uploads/media/social_Media_guidelines_final_02_03_2012.pdf; access: 06.05.2015.

[BZgA16] Bundeszentrale für gesundheitliche Aufklärung (BZgA); set of posters fort he campaign: *“Alkohol? Kenne dein Limit.“*; online available at: http://www.kenn-dein-limit.de/alkohol/infomaterial/allgemeine-informationen/; access: 28.06.2016; motive “Birgit” (top left): http://www.kenn-dein-limit.de/alkohol/infomaterial/allgemeine-informationen/detail/?tx_bzgashop_pi2%5BarticleNumber%5D=1924&tx_bzgashop_pi2%5BparentArticles%5D=0&cHash=c6e55dc5e393640645ad15a5c26ced32; motive “Mai” (top middle): http://www.kenn-dein-limit.de/alkohol/infomaterial/allgemeine-informationen/detail/?tx_bzgashop_pi2%5BarticleNumber%5D=1925&tx_bzgashop_pi2%5BparentArticles%5D=0&cHash=d8b9f35f01aaa90e3335ac9e80dab3af; motive “Markus” (top right): http://www.kenn-dein-limit.de/alkohol/infomaterial/allgemeine-informationen/detail/?tx_bzgashop_pi2%5BarticleNumber%5D=1926&tx_bzgashop_pi2%5BparentArticles%5D=0&cHash=5ce94ddffb2274227a1a19c0c4294310; motive “Knut” (bottom left): http://www.kenn-dein-limit.de/alkohol/infomaterial/allgemeine-informationen/detail/?tx_bzgashop_pi2%5BarticleNumber%5D=1927&tx_bzgashop_pi2%5BparentArticles%5D=0&cHash=32102016e77b177e5c8d70e90cc73d36; motive “Jörn” (bottom middle): http://www.kenn-dein-limit.de/alkohol/infomaterial/allgemeine-informationen/detail/?tx_bzgashop_pi2%5BarticleNumber%5D=1928&tx_bzgashop_pi2%5BparentArticles%5D=0&cHash=2b612b4c88c27e719369d7c1befc6a89; motive “Verantwortung Schwangerschaft” (bottom right): http://www.kenn-dein-limit.de/alkohol/infomaterial/allgemeine-informationen/detail/?tx_bzgashop_pi2%5BarticleNumber%5D=2580&tx_bzgashop_pi2%5BparentArticles%5D=0&cHash=29cd13a86aac724bd8aaca49d88093b4.

[CDC11a] Centers for Disease Control and Prevention (CDC) (Hg.): *„Social Media Guidelines and Best Practices – CDC Twitter Profiles“*; Stand: 14.02.2011; online verfügbar

unter: http://www.cdc.gov/socialmedia/tools/guidelines/pdf/twitterguidelines.pdf; Zugriff: 28.06.2015.

[CDC11b] Centers for Disease Control and Prevention (CDC): *„The Health Communicator's Social Media Toolkit"*; July 2011; online available at: http://www.cdc.gov/healthcommunication/ToolsTemplates/SocialMediaToolkit_BM.pdf; access: 06.05.2015.

[CDC12a] Centers for Disease Control and Prevention (CDC) (Ed.): *„CDC's Guide to Writing for Social Media"*; April 2012; online available at: http://www.cdc.gov/socialmedia/tools/guidelines/pdf/GuidetoWritingforSocialMedia.pdf; access: 28.06.2015.

[CDC12b] Centers for Disease Control and Prevention (CDC) (Ed.): *„Social Media Guidelines and Best Practices - Facebook"*; 16.05.2012; online available at: http://www.cdc.gov/socialmedia/tools/guidelines/pdf/facebookguidelines.pdf; access: 28.06.2015.

[COSM14a] COSMIC Project: *"Tips and tricks for public authorities"*; online available at: http://www.cosmic-project.eu/public-guidelines; access: 28.06.2016.

[COSM14b] COSMIC Project: *"Tips and tricks for citizens"*; online available at: http://www.cosmic-project.eu/citizens-guidelines; access: 28.06.2016.

[CRC13] Canadian Red Cross (Ed.): *„Social Media – Guidelines for Canadian Red Cross Staff and Volunteers"*; online available at: http://www.redcross.ca/crc/documents/What-We-Do/Violence-Bullying/partners/social-media-guidelines-2013.pdf; access: 06.05.2015.

[CSJD+14] Cullen, Joe; Spielhofer, Thomas; Junge, Kerstin; Drabble, David; Ludwig, Thomas; Reuter, Christian: *"Deliverable 2.1 - Concept for impact assessment"*; Project EmerGent; July 2014; online available at: http://www.fp7-emergent.eu/wp-content/uploads/2014/09/D2.1_ConceptforImpactAssessment.pdf.

[Daim12] Daimler AG: *„Social Media Leitfaden – 10 Tipps zum Umgang mit Social Media"*; Stand: July 2012; online available at: https://www.daimler.com/Projects/c2c/channel/documents/1895106_Social_Media_Leitfaden_Final.pdf; access: 06.05.2015.

[DCV11] Deutscher Caritasverband: *„Das Soziale ins Netz bringen – die Caritas und soziale Medien"*; Stand: December 2011; online available at: http://www.caritas.de/diecaritas/fuermitarbeiter/caritaswebfamilie/social_media_leitlinien_caritas/guidelines; access: 06.05.2015.

[DRK11] Deutsches Rotes Kreuz (DRK): *„Ein Leitfaden zum Umgang mit Social Media im DRK“*; online available at: http://lv-saarland.drk.de/fileadmin/user_upload/PDF-Dateien/Soz_Medien_Internet/LeitfadenSozMedien.PDF; access: 06.05.2015.

[DSTL12] Defence Science and Technology Laboratory (dstl): *„Using social media in emergencies: Smart Practices – Smart tips for category 1 responders using social media in emergency management“*; March 2012; online available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/85946/Using-social-media-in-emergencies-smart-tips.pdf; access: 06.05.2015.

[FEMA16a] Emergency App *“FEMA”* for Android; Version 2.8.2 (last update: 30.06.2016); Federal Emergency Management Agency (FEMA); USA; Download available at: https://play.google.com/store/apps/details?id=gov.fema.mobile.android&hl=en; access: 01.07.2016.

[FEMA16b] Federal Emergency Management Agency; online available at: http://www.fema.gov/mobile-app; access: 07.07.2016.

[FHH12] Freie und Hansestadt Hamburg: *„Social Media in der Hamburgischen Verwaltung - Hinweise, Rahmenbedingungen und Beispiele“*; 06.03.2012; online available at: http://www.hamburg.de/contentblob/2882174/data/social-media-in-der-hamburgischen-verwaltung.pdf; access: 06.05.2015.

[GIS11] Government Information Services, New Zealand Department of Internal Affairs, Social Media in Government – High Level guidance, November 2011, available at: https://webtoolkit.govt.nz/guidance/social-media/high-level-guidance/

[GWL15] Great-West Life; YouTube-Video *“Employee Social Media Guidelines”*; 30.11.2015; online available at: https://www.youtube.com/watch?v=sx7t5A00UsE; access: 30.06.2016.

[HSGM+14] Helsloot, Ira; Scholtens, Astrid; Groenendaal, Jelle; Melssen, Nivine; Watson, Hayley; Hagen, Kim; Wadhwa, Kush; Kalemaki, Eirini; Papadimitriou, Alex; Vontas, Apostolos: *„Deliverable D6.2.1: Guidelines for the use of new media by public and private organisations”*; Project „Cosmic – The Contribution of Social Media In Crisis management”; 2014; online available at: http://www.cosmic-project.eu/sites/default/files/deliverables/Deliverable%20D6.2.1%20final%20version.pdf.

[HVGS+14] Helsloot, Ira; de Vries, David; Groenendaal, Jelle; Scholtens, Astrid; Günel, Zeynep; Baruh, Lemi; Scifo, Salvatore; Watson, Hayley; Hagen, Kim; Kalemaki, Eirini; Papadimitriou, Alex; Vontas, Apostolos: *„Deliverable D6.1: Guidelines for the use of new media by the public in crisis situations”*; Project „Cosmic – The COntribution of Social Media In Crisis management”; 2014; online available at: http://www.cosmic-

project.eu/sites/default/files/deliverables/D6.1.pdf.

[HVGS+15] Helsloot, Ira; de Vries, David; Groenendaal, Jelle; Scholtens, Astrid; in 't Veld, Michiel; van Melick, Gaby; Baruh, Lemi; Scifo, Salvatore; Günel, Zeynep; Watson, Hayley; Wadhwa, Kush; Hagen, Kim; Kalemaki, Eirini; Papadimitriou, Alex; Vontas, Apostolos; Bonnamour, Marie-Christine; Blaha, Manfred: *„Deliverable D6.1 & D6.2: Guidelines for the use of new media in crisis situations"*; Project „Cosmic – The COntribution of Social Media In Crisis management"; 2015; online available at: http://www.cosmic-project.eu/sites/default/files/Deliverables_D6.1.2_and_D6.2.2_Final_Guidelines_April_2015.pdf.

[IATA14] International Air Transport Association (IATA) (Ed.): *„Crisis Communications and Social Media: A best Practice Guide to Communicating in an Emergency"*; December 2014; online available at: http://www.iata.org/publications/documents/social-media-crisis-guidelines.pdf; access: 06.05.2015.

[IFRC09] International Federation of Red Cross and Red Crescent Societies (IFRC) (Ed.): *„Social media guidelines for IFRC staff"*; online available at: http://sm4good.com/wp-content/uploads/2009/11/Red-Cross-Red-Crescent-SocialMedia-Guidelines.pdf; access: 06.05.2015.

[KaRe2016] Kaufhold, M.-A., Reuter, C., The Self-Organization of Digital Volunteers across Social Media: The Case of the 2013 European Floods in Germany, 2016, Journal of Homeland Security and Emergency Management, 13(1), 137–166

[KATW15] Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS, Verband Öffentlicher Versicherer (VöV), CombiRisk GmbH: *"Nutzerhandbuch KATWARN – Fragen und Antworten"*; June 2015; online available at: https://www.katwarn.de/wp-content/uploads/KATWARN-Nutzerhandbuch_Juni2015_Web.pdf; access: 04.07.2016.

[KATW16a] Emergency App *"KATWARN"* for Android; Version 2.0.17 (last update: 01.06.2016); CombiRisk GmbH; Germany; Download available at: https://play.google.com/store/apps/details?id=de.combirisk.katwarn; access: 01.07.2016.

[KATW16b] KATWARN; online available at: https://www.katwarn.de/unterstuetzte-orte/; access: 04.07.2016.

[Lind13] The Linde Group; YouTube-Video *"Social Media Guidelines at Linde"*; 08.07.2013; online available at: https://www.youtube.com/watch?v=SY77XD0I9bc; access: 30.06.2016.

[Neil15] Neild, G., Social Media Policy and Guidance, Leeds Community Healthcare, NHS Trust, 23 February 2015, available at: www.leedscommunityhealthcare.nhs.uk/seecmsfile/?id=415

[NINA16] Emergency App *"NINA"* for Android; Version 2.0.1 (last update: 21.06.2016); Bundesamt für Bevölkerungsschutz und Katastrophenhilfe; Germany; Download available at: https://play.google.com/store/apps/details?id=de.materna.bbk.mobile.app; access: 01.07.2016.

[PYKI+13] Papadimitriou, Alex; Yannopoulos, Angelos; Kotsiopoulos, Ioannis; Finn, Rachel; Wadhwa, Kush; Watson, Hayley; Baruh, Lemi: *„Deliverable D2.2 – Case studies of communication media and their use in crisis situations"*; Project „Cosmic – The COntribution of Social Media In Crisis management"; 2013; online available at: http://www.cosmic-project.eu/sites/default/files/deliverables/D2.2.pdf.

[QPS1.0] Queensland Police Service, Disaster Management and Social Media - a case study, version 1.0, available at: https://www.police.qld.gov.au/corporatedocs/reportsPublications/other/Documents/QPSSocialMediaCaseStudy.pdf , [accessed: 2016/09/13]

[RFMB+14] Reuter, C., Friberg, T., Moi, M., Bizjak, G., Nuessler, D., Sangiorgio, F., Toscano, F., Gizikis, A., Guidelines for Social Media integration into existing EMS systems, Project EmerGent, July 2014, available at: http://www.fp7-emergent.eu/wp-content/uploads/2014/09/D3.2_GuidelinesForSocialMediaIntegrationIntoExistingEMSSystems.pdf

[RLKS16] Reuter, C., Ludwig, T., Kaufhold, M.-A., & Spielhofer, T., Emergency Services Attitudes towards Social Media: A Quantitative and Qualitative Survey across Europe, 2016, International Journal on Human-Computer Studies (IJHCS), 95, 96–111

[RLFM+14] Reuter, Christian; Ludwig, Thomas; Friberg, Therese; Moi, Matthias; Akerkar, Rajendra; Pratzler-Wanczura, Sylvia; Gizikis, Alexis; O'Brien, Tony: "Deliverable 3.1 - Usage Patterns of Social Media in Emergencies"; Project EmerGent; June 2014; online available at: http://www.fp7-emergent.eu/wp-content/uploads/2014/09/D3.1_UsagePatternsOfSocialMediaInEmergencies.pdf.

[RPSD14] Reuter, C., Pratzler-Wanczura, S., Spielhofer, T., Drabble, D., End-User Based View on Potentials of Social Media Usage for ES and Citizens' Involvement in the EMC, October 2014, Project EmerGent

[ReSp16] Reuter, C., & Spielhofer, T., Towards Social Resilience: A Quantitative and Qualitative Survey on Citizens' Perception of Social Media in Emergencies in

Europe, 2016, Journal Technological Forecasting and Social Change (TFSC)

[ScGo12] Scottish Government: *„Warning and Informing Scotland - Using Social Media in Emergencies“*; 2012; online available at: http://www.gov.scot/Resource/0041/00411704.pdf; access: 06.05.2015.

[SJCD+16] Spielhofer, T., Junge, k., Cullen, J., Drabble, D., Hahne, A.S., Bizjak, G., Akerkar, R., Reuter C., Kaufman, M.A., Plasota, T., Wenarski, G., Gizikis, A., Impact of social media on Emergency Services and Citizens, Project EmerGent, May 2016, available at: http://www.fp7-emergent.eu/wp-content/uploads/2016/06/20160526_D2-3_Impact-of-social-media-on-ES-and-citizensFINAL.pdf

[SpGa16] Gabler Wirtschaftslexikon: *“Social-Media-Richtlinien”*; Springer Fachmedien Wiesbaden GmbH; online available at: http://wirtschaftslexikon.gabler.de/Definition/social-media-richtlinien.html; access: 15.06.2016.

[SSG14] Steiger, Dr. Saskia; Schiller, Prof. Dr.-Ing. Jochen; Gerhold, Dr. Lars: *„Aktive Risiko- und Krisenkommunikation in Social Media“*; in: *„Bevölkerungsschutzmagazin - Social Media“*, 3/2014, p. 14-16, publisher: BBK; online available at: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_3_14.pdf?__blob=publicationFile.

[Tchi11] Tchibo; YouTube-Video *“Herr Bohne geht ins Netz”*; May 2011; online available at: https://www.youtube.com/watch?v=e_mLQ_eWk_o; access: 09.05.2016.

[Tril15] Trilateral Research & Consulting, Comparative Review of Social Media Analysis Tools for Preparedness, 31 July 2015

[Unic12] UNICEF: *„Social Media in Emergencies: UNICEF Guidelines for Communication and Public Advocacy“*; 16.05.2012; online available at: http://www.unicefinemergencies.com/downloads/eresource/docs/3.1%20Media%20and%20Communications/socialmediainemergencies-communicationsguidelines-120518144234-phpapp02.pdf; access: 06.05.2015.

[USDV16] United States Department of Veterans Affairs: *“Glossary”*; online available at: http://www.va.gov/trm/TRMGlossaryPage.asp; access: 15.06.2016.

[Vand16] Vanderbiest, N., False information during attacks. How do they spread online during attacks?, Oct 2013, EENA event: Social Media & Public Warning, available at: https://www.dropbox.com/sh/6eyjse79ot3zbg0/AADS4GSspqIr1ZMAety5C8nia?dl=0&preview=5.False+information+during+attacks.+How+do+they+spread+online+during+attacks.pdf

[WREM14] Wellington Region Emergency Management Office: *„Social Media for emergency*

management - A good practice guide"; May 2014; online available at: http://www.getprepared.org.nz/sites/default/files/uploads/Social%20media%20for%20emergency%20management%20-%20a%20good%20practice%20guide%20-%20July%202014.pdf; access: 06.05.2015.

[WWW01] Social-Media-Guidelines.com: *"Was sind Social Media Guidelines?"*; online available at: http://www.social-media-guidelines.com/einfuehrung/; access: 15.06.2016.

[WWW02] Alike.ch; *"15 'Dos' for Pinterest"*; online available at: http://alike.ch/15-dos-fuer-pinterest/; access: 22.06.2016.

[WWW03] Technologyrocksseriously.com; *"Before You Post: THINK"*; online available at: http://www.technologyrocksseriously.com/2014/10/before-you-post-think.html#.VMP7XDTF-Sp; access: 22.06.2016.

[WWW04] QR-Code-Generator; online available at: http://www.qrcode-generator.de/; inserted URL: http://www.fp7-emergent.eu/; access: 19.07.2016.

[WWW05] European Journalism Centre (EJC), Verification Handbook, http://verificationhandbook.com/ [accessed: 2016/06/06]

[WWW06] Creative Commons, About Licenses, https://creativecommons.org/licenses/ [accessed: 2016/09/12]

[WWW07] Creative Commons, Best practices for attribution, https://wiki.creativecommons.org/wiki/best_practices_for_attribution [accessed: 2016/09/12]

[WWW08] Centers for Disease Control and Prevention, Social Media Public Comment Policy, http://www.cdc.gov/SocialMedia/Tools/CommentPolicy.html [accessed: 2016/10/26]

[WWW09] Reputation Lab, Nicolas Vanderbiest, Attentats de Bruxelles: regards croisés entre recherche et réalité (in French), http://www.reputatiolab.com/2016/10/attentats-de-bruxelles-regards-croises-entre-recherche-realite/ [accessed: 2016/11/03]

[WWW10] Twitter, Twitter for Good, https://about.twitter.com/company/twitter-for-good [accessed: 2016/11/03]

[WWW11] Twitter Account of Queensland Police Service, #mythbuster hashtag, https://twitter.com/search?q=%23mythbuster%20from%3Aqpsmedia&src=typd&lang=en [accessed: 2016/11/03]

[WWW12] UK Information Commissioner's Office Blog, What you need to know about ICO Privacy Seals, https://iconewsblog.wordpress.com/2015/01/28/what-you-need-to-know-about-ico-privacy-seals/ [accessed: 2016/12/14]

[WWW13] UK West Midlands Police, Social and digital media policy, http://www.west-midlands.police.uk/csimages/files/Social_and_Digital_Media_policy_V1_3_-_FINAL.pdf [accessed: 2016/12/16]

[WWW14] EENA Case Study, Nicolas Vanderbiest, Brussels Attacks Crossover between research and reality, http://eena.org/publications/brussels-attacks-twitter-reactions [accessed: 2016/12/16]

[WWW15] EENA Operations Document, Media in Authority-to-Citizen (A2C) Communications, http://www.eena.org/download.asp?item_id=161 [accessed: 2016/12/16]

[WWW16] RallyEngine, The Rise of the Virtual Operations Support Team (VOST), http://rallyengine.com/vost-virtual-operations-support-teams/ [accessed: 2016/12/16]

[WWW17] Irekia, El Departamento de Seguridad suscribe un convenio de colaboración con la asociación de voluntarios digitales de emergencias VOST Euskadi, http://www.irekia.euskadi.eus/es/news/24810-segurtasun-sailak-lankidetza-hitzarmena-larrialdien-boluntario-digitalen-elkartearekin [accessed: 2016/12/16]

[WWW18] Twitter VISOV, https://twitter.com/VISOV1/status/803008126744002561 [accessed: 2016/12/16]

[WWW19] Ibz Crisiscentrum, Team D5 : Un renfort en communication de crise, http://centredecrise.be/fr/content/team-d5-un-renfort-en-communication-de-crise [accessed: 2016/12/16]

[WWW20] VOST Spain, https://www.vost.es/ accessed: 2016/12/16]

[WWW21] VOST Europe website (under construction), https://www.vosteurope.eu/ accessed: 2016/12/16]

[WWW22] VOST Leadership Coallition, http://vosg.us/blog/2012/05/24/what-is-the-vost-leadership-coalition/ [accessed: 2016/12/16]

[WWW23] COSMIC Project, http://www.cosmic-project.eu/ [accessed: 2016/12/16]

[WWW24] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, http://www.bbk.bund.de/DE/Home/home_node.html [accessed: 2016/12/16]

[WWW25] Federal Emergency Management Agency, http://www.fema.gov/

[WWW26] Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Warn-App NINA, http://www.bbk.bund.de/DE/NINA/Warn-App_NINA.html [accessed: 2016/12/16]

[WWW27] KATWARN< https://www.katwarn.de/ [accessed: 2016/12/16]

[WWW28] FEMA Mobile App, http://www.fema.gov/mobile-app [accessed: 2016/12/16]

[WWW29] Emergency 2.0 Wiki, http://emergency20wiki.org/wiki/index.php/Main_Page [accessed: 2015/09/16]

[WWW30] VOST Americas Twitter Account, https://twitter.com/vostamericas [accessed:

2016/12/22]

[WWW31] VOST Oceania Twitter Account, https://twitter.com/vostoceania [accessed: 2016/12/22]

[WWW32] VOST Spain #StopBulos, https://www.vost.es/stopbulos [accessed: 2016/12/22]

[WWW33] Twitter Account of Police in Spain – example use of the #StopBulos hashtag, https://twitter.com/policia/status/809085298286141440 [accessed: 2016/12/22]

[WWW34] ENA, 112 Smartphones Apps, 2014, http://www.eena.org/uploads/gallery/files/operations_documents/2014_02_25_112smartphoneapps.pdf [accessed: 2017/01/12]

[WWW35] Eurostat, Digital economy and society statistics - households and individuals, http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access [accessed: 2017/01/12]

[WWW36] Statista, Smartphone users worldwide 2014-2020 https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ [accessed: 2017/01/12]

[WWW37] Twitter, Tweet by Polizeipräsidium Oberbayern Süd (Germany), https://twitter.com/polizeiOBS/status/816213910487527424 [accessed: 2017/05/09]

[WWW38] Twitter, Tweet by Policía Nacional (Spain), https://twitter.com/policia/status/813689383345790976 [accessed: 2017/05/09]

[WWW39] Twitter, Tweet of the French Ministry of Interior, https://twitter.com/Place_Beauvau/status/753720082413547520 [accessed: 2017/05/09]

[WWW40] Twitter, Tweet of the French government, https://twitter.com/gouvernementFR/status/753719504807534592 [accessed: 2017/05/09]

[WWW41] EENA, European 112 day, http://112day.eu/ [accessed: 2017/05/09]

[WWW42] EENA, Infographic “Social media & emergencies: the basics of how your smartphone can help you”, https://www.dropbox.com/s/cxghkdq8od1dgo4/112Day2017_factsheet.pdf?dl=0 [accessed: 2017/05/09]