D7.1. - Analysis of the legal issues and ethical aspects related to the creation of a pan-European information space

<table>
<thead>
<tr>
<th>Grant agreement number:</th>
<th>607078</th>
<th>Date of deliverable:</th>
<th>2014-10-30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of project start:</td>
<td>2014-06-01</td>
<td>Date of revised submission:</td>
<td>2015-11-13</td>
</tr>
<tr>
<td>Duration of project:</td>
<td>36</td>
<td>Deliverable approved by:</td>
<td>Georg Neubauer (AIT), Harold Linke (HITEC)</td>
</tr>
<tr>
<td>Lead Beneficiary:</td>
<td>KU Leuven (Lina Jasmonaite; Bjorn Coene; Anton Vedder)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Executive Summary

The aim of this deliverable is to provide a high level analysis of the legal requirements and ethical aspects related to the establishment of a pan-European information space to Enhance seCurity of Citizens, in other words, a Common Information Space.

This deliverable concludes that the EU data Protection Framework is applicable to the processing of personal data in the context of disaster management. The deliverable points out that the EU Data Protection Framework does not restrict the processing of personal data when providing disaster response. However, to be compliant with the EU data protection rules the data controller (i.e. an entity determining the purposes of processing) is required to follow certain legal, organisational and technical requirements.

The legal regimes on environmental information, spatial data and re-use of public sector information seem to facilitate access of data to first responders in the case of emergency situations. These regimes make a valuable contribution to clarifying the conditions and circumstances under which this data can be accessed, exchanged and used.

Contrary to the EU Data Protection Framework as well as the framework on the reuse of information held by public authorities, the intellectual property rights’ framework may impose limits on first responders’ legal use of data in the case of emergencies. Ordinary copyright, database copyright and the database sui generis right provide a broad protection to the rights of a right-holder about which first responders may not be aware while making use of incorporations of data subjected to the intellectual property rights’ framework. Consequently, first responders are prone to risks of infringing these rights. However, a number of exceptions to the categories of acts, which the intellectual property rights’ framework reserve to the right-holder, can offer first responders a cheap and immediate opportunity to use incorporations of data involving intellectual property protection without infringing the legal framework.

This deliverable not only points out ethical and legal obligations of the EPISSECC project when developing a Common Information Space, but it also describes measures taken to adhere to the EU Data Protection Framework in the context of WP 3 research activities (see Section 3.9). To ensure compliance with ethical and legal obligations, relevant ethics committees and regulatory authorities were approached. The EPISSECC project has obtained an approval of the interview procedure from the KU Leuven Social and Societal Ethics Committee (see Annex III). To meet the legal requirements related to the processing of personal data, the EPISSECC team developed an information notice (see Annex II) and notified the Austrian Data Protection Authority (see Annex IV).
# Table of Content

List of Tables ........................................................................................................................................ 5
List of Acronyms .................................................................................................................................. 6

1. **Introduction** ................................................................................................................................... 8
   1.1. The context of the EPISECC project .......................................................................................... 8
   1.2. Purpose and scope of the deliverable ...................................................................................... 8
   1.3. Document structure ................................................................................................................... 9
   1.4. Definitions .................................................................................................................................... 9
   1.5. Approach and methodology ....................................................................................................... 10

2. **Ethical Considerations** .................................................................................................................. 12
   2.1. Ethics added value to ICT ......................................................................................................... 12
   2.2. EPISECC ethical obligations ..................................................................................................... 12
   2.3. Research ethics .......................................................................................................................... 13
   2.4. Guidance on research output of the EU funded research projects ........................................... 13
   2.5. Guidance on information security ............................................................................................. 15
   2.6. Ethical concerns about the Common Information Space .......................................................... 17

3. **Relevance of the EU Data Protection Framework** ......................................................................... 19
   3.1. The background and scope of application ............................................................................... 20
   3.2. Responsibilities and identification of actors ............................................................................ 22
   3.3. General principles ..................................................................................................................... 22
   3.4. Conditions for lawful processing of personal data .................................................................... 23
      3.4.1. Legitimising the processing of personal data of affected people ...................................... 24
      3.4.2. Legitimising the processing of personal data of first responders ..................................... 25
   3.5. Data subjects’ rights ..................................................................................................................... 26
   3.6. Security requirements ............................................................................................................... 26
   3.7. Anticipating the adoption of the General Data Protection Regulation ..................................... 28
   3.8. Impact on exchanging and using personal data the context of disaster relief ...................... 29
   3.9. EPISECC compliance with the EU Data Protection Framework in WP 3 ................................ 30

4. **Relevance of Public Sector Data and its Regulation** ..................................................................... 33
   4.1. Aarhus Directive ....................................................................................................................... 33
      4.1.1. Scope of application ............................................................................................................. 33
      4.1.2. Access to environmental information upon request ......................................................... 34
      4.1.3. Active and systematic dissemination of environmental information .................................. 36
   4.2. Public Sector Information Directive ......................................................................................... 36
4.2.1. Scope of application ................................................................. 37
4.2.2. Rules on re-use ........................................................................ 38

4.3. **Inspire Directive** ......................................................................... 39

4.3.1. Scope of application ...................................................................... 40
4.3.2. The Infrastructure for Spatial Information in the European Community ............................................. 40
4.3.3. Public authorities within Inspire.................................................... 41
4.3.4. Making available and sharing of spatial data sets ............................... 42
4.3.5. The concept of ‘third parties’............................................................ 43
4.3.6. Enabling public access .................................................................. 44
4.3.7. Impact on exchanging and using data in the context of disaster relief ................................. 45

5. **Relevance of Intellectual Property Rights** ........................................ 47

5.1. **Ordinary copyright** ................................................................. 48
5.1.1. Requirements for the grant of an exclusive right................................ 49
5.1.2. Embodiments of the ‘work’ ................................................................ 49
5.1.3. Categories of acts subject to the authorisation of the right holder .................. 49
5.1.4. Relevant exceptions to the categories of restricted acts .......................... 50

5.2. **Intellectual property rights relating to databases** ......................... 51
5.2.1. Database copyright........................................................................... 51

5.3. **Database sui generis right** ......................................................... 53
5.3.1. Requirements for the grant of an exclusive right................................ 54
5.3.2. Whole or substantial part of the content of a database ......................... 54
5.3.3. Categories of acts subject to the authorisation of the right holder ................ 55
5.3.4. Relevant exceptions to the categories of restricted acts .......................... 55

5.4. Impact on exchanging and using data in the context of disaster relief ....... 56

6. **Summary** ....................................................................................... 59

**Bibliography** ...................................................................................... 61

Annex I – Questions related to the Common Information Space .................. 64
Annex II – Informed consent form for the EPISECC Inventory ...................... 66
Annex III – Ethical approval of the interview procedure .............................. 68
Annex IV – Notification to the Austrian Data Protection Authority ................. 77
List of Tables

Table 1: Mapping processing of personal data in a disaster relief..........................................................20
Table 2: Summary of relevant intellectual property rights..............................................................................48
## List of Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Network and Information Security</td>
</tr>
<tr>
<td>EPISECC</td>
<td>Establish Pan-European Information Space to Enhance seCurity of Citizens</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Union Agency for Network and Information Security</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>
Imprint

This document constitutes a formal deliverable 7.1 on legal requirements and ethical aspects and provides input to the associated deliverables in WP 2 and WP 3 of the EPISECC project. Use of any knowledge, information or data contained in this document shall be at the user’s sole risk. Neither the EPISECC Consortium nor any of its members, their officers, employees or agents shall be liable or responsible, in negligence or otherwise, for any loss, damage or expense whatever sustained by any person as a result of the use, in any manner or form, of any knowledge, information or data contained in this document, or due to any inaccuracy, omission or error therein contained. This document contains information that is protected by copyright.

© EPISECC Consortium 2014-2017
1. Introduction

1.1. The context of the EPISECC project

The overarching aim of the EC funded project, titled “Establish Pan-European information space to Enhance seCurity of Citizens” (hereinafter “EPISECC”), grant no. 607078, is to establish a pan-European information space to enhance security of citizens (hereinafter “Common Information Space”). The Common Information Space should improve data management practices and deployment of the European Union Mechanism for Civil Protection (hereinafter “EU Civil Protection Mechanism”) in case of a disaster situation. The activation of the EU Civil Protection Mechanism is not the only situation in which first responders from different EU Member States interact and cooperate to provide a disaster relief. The use of the Common Information Space could be triggered in cases of cross-border disaster involving teams from two or more Member States. Therefore, the main objective of the Common Information Space would be to serve as a tool enabling interaction and optimising coordination of civil protection assistance in disasters of various scale, including disasters that prompt activation of the EU Civil Protection Mechanism.

1.2. Purpose and scope of the deliverable

The aim of this deliverable is to provide a high level analysis of the legal requirements and ethical aspects related to the establishment of a pan-European information space to Enhance seCurity of Citizens (“Common Information Space”). The main focus of this deliverable is the identification of ethical and legal issues related to the creation of a Common Information Space. This report has been developed while following work undertaken in WP 2, titled “Analysis of the crisis management approaches applied in EU member states and beyond” and WP 3, titled “Pan European Inventory of events/disasters, considering time dimension”. This deliverable presents a high level analysis of the existing European regulatory frameworks that should be taken into account while developing a Common Information Space that would assist first responders during disaster relief.

Disasters can be categorised according to different dimensions, such as source (e.g. natural or human-made), scope (e.g. local or international) and impact (e.g. low and high). “International” disasters refer to situations either where disasters occur in cross-border areas and require a combined action by neighbouring countries, or where the impact overwhelms the response capacity of the affected country. An important indicator for the term cross-border disaster management is that it exceeds the daily-routine procedures of emergency services and requires additional capabilities. Cross-border cooperation is subject to international, national and cantonal treaties and/or agreements. The Council of Europe Convention on Transfrontier Co-operation between Territorial Communities or Authorities (no. 106) facilitates and encourages cross-border cooperation on civil protection and mutual aid in the event of disasters occurring in frontier areas on the basis of agreements between regions and local authorities. At the moment, because of the limitations of competencies imposed on the EU by the governing treaties, the European disaster relief framework is fragmented and includes regulatory measures developed by both the EU and its Member States.

---

1 Council of Europe, European Outline Convention on Transfrontier Co-operation between Territorial Communities or Authorities, 1980, [ETS No. 106].

Additionally, each member state has a discretion to conclude multilateral and bilateral agreements allowing cooperation in the field of civil protection with other countries.

1.3. Document structure

It has been pointed out in the deliverable 3.1, titled “Architecture of inventory” that, in general, there are no legal restrictions on the form of databases in the EU. Therefore, the architecture of the Common Information Space is not subject to any legal regulation. The efficient and reliable exchange of all available data in a disaster situation is the key to a successful disaster response. However, it should be noted that certain types of data processed in the Common Information Space may be subject to various restrictions and legal requirements. In particular, processing of personal data and data being subject to the intellectual rights while providing a disaster relief must be considered.

This deliverable is divided into six parts. The first part points out ethical considerations that have to be discussed by the project partners. It includes ethical guidance on research, development of new technology, and information security. The third part discusses the extent to which the EU data protection legal framework is applicable in public protection and disaster relief. The fourth part reflects on the challenges to re-use public sector information in a situation of a major disaster. The fifth part discusses the relevant legal framework from the intellectual property rights perspective. The sixth part summarizes the key findings of the report that have to be taken into account prior to developing the Common Information Space.

The Annex I of the deliverable includes a list of issues that have to be discussed and agreed upon by the project consortium prior to setting up the architecture for a Common Information Space to enhance security of citizens. Annex II includes a consent form that was developed in the context of work carried out by the WP 3. Annex III includes an application form regarding the interview procedure submitted to and approved by the KU Leuven Social and Societal Ethics Committee. Annex IV includes a letter from the Austrian Data Protection Authority confirming a notification about the processing of personal data in the context of WP 3.

The subsequent task of WP 7 is titled “Legal implementation for internal needs”. It will further build on the identified legal requirements in this report. Close cooperation with WP 4, titled “Taxonomy building” and WP 5, titled “Architecture of Common Information Space”. Work performed within the scope of the next deliverable will be prerequisite to evaluate the actual implications of identified legal concerns to the EPISECC project.

1.4. Definitions

In the context of the EPISECC project the following terms have been agreed:

- The word “disaster” indicates an alarming situation and may be used to refer to emergencies, crisis, critical events, terrorist attacks, technical accidents and alike events having adverse impact. A number of different definitions of disaster are available.\(^3\) The EU interconnection of electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

\(^3\) For example, the International Disaster Database EM-DAT, use specific criteria to qualify a situation as a disaster. To date the most elaborate definition has been proposed by the United Nations International Strategy for Disaster Reduction (UNISDR), which defines “a disaster” as “a serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources.” This
has developed a general definition for a disaster which is also followed in the EPISECC project. According to this definition, disaster “means any situation which has or may have a severe impact on people, the environment, or property, including cultural heritage.”

- Critical event has the same meaning as a disaster, but could also be considered as a situation that straightforwardly leads to a disaster.
- Data is defined as a “neutral or objective notion, relating to observations or representations of facts, concepts, or instructions that are suitable for interpretation or communication.”
- Personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”
- Sensitive data means special categories of data, as defined in Directive 95/46/EC. Sensitive data may include information about “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”
- Controller (or data controller) means “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.”
- Processor means “a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.”
- Response means “any action taken upon request for assistance under the Union Mechanism in the event of an imminent disaster, or during or after a disaster, to address its immediate adverse consequences.”

1.5. Approach and methodology

To achieve the overall objective of this deliverable (i.e. provide a high level analysis of the legal requirements and ethical aspects related to the establishment of a Common Information Space) the research methods included a desk based research and analysis of the relevant legislative measures. As a result of a desk based research, a number of data sources (e.g. scholarly articles, books, studies and reports) on domestic and the European Civil Protection mechanisms was collected. The examination of the most relevant materials to the EPISECC project resulted in an extensive literature review that not only allowed to develop a broader understanding of how different civil protection mechanisms function at various levels (a detailed report is included in the deliverable 3.2), but also helped to indicate relevant legal sources. The legal analysis in this deliverable focuses on the EU

---

*Decision No 1313/2013/EU Article 4.1.*
*Directive 95/46/EC, Article 8.*
*Directive 95/46/EC, Article 2 (c).*
*Directive 95/46/EC, Article 2(e).*
*Decision No 1313/2013/EU Article 4.1.*
*This is included in the deliverable 3.2.*
legislation and policy documents that are deemed to be of relevance to the EPISSECC project. The legal analysis goes beyond a mere description of the identified legal frameworks at EU level; it considers and points out practical aspects of these frameworks. It also takes into consideration opinions issued by the relevant regulatory bodies and agencies, such as the European Union Agency for Fundamental Rights and the Article 29 Working Party set up under Directive 95/46/EC.
2. Ethical Considerations

2.1. Ethics added value to ICT

Citizens, businesses and governments are empowered and make use of the Information and Communication Technology (ICT) on daily basis. ICT systems enhance effectiveness and efficiency of a vast number of their activities and services ranging from e-commerce to e-government. As the great benefits of the ICT are often assumed or taken for granted, and potential risks embodied in such technology are not always apparent. Also, the practice has shown that manufacturers as well as software developers are rather driven by the demand of new products and potential profits than implications of their innovations. Consequently, the current approach often results in systems that have a negative impact on individuals’ rights and freedoms. To mitigate the likeliness of such risks and undesirable situations, government agencies, civil society groups, as well a number of scholars encourage to carry out ethical analysis of a new products. Such analysis should be conducted at the time of designing new technologies as well as in the following product development stages. However, ethics is a hazy term. There is no one concept or definition for ethics. On the contrary, scholars representing different schools of thought suggest that ethics is based and entail different criteria and principles.

2.2. EPISECC ethical obligations

The EPISECC project has been developed in a response to the EC’s call for security research “FP7-SEC-2013-1”. The EPISECC project to a large extent is funded by the Seventh Framework Programme for research (hereinafter “FP7”). Consequently, all research and technological development, including demonstration activities, which are and will be carried out in the context of this project, are subject to Decision No. 1982/2006/EC of the European Parliament and of the Council concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (hereinafter “Decision”). According to Article 6 of this Decision, “all the research activities carried out under the Seventh Framework Programme shall be carried out in compliance with fundamental ethical principles.” Recital 30 supplementing Article 6 of the Decision provides a list of sources that have to be taken into account while considering ethical concerns. In particular, the recital refers to the Charter of Fundamental Rights of the EU, opinions adopted by the European Group on Ethics in Science and New Technologies, and the Protocol on the Protection and Welfare of Animals. Given the description of work of the EPISECC project, the latter is of no relevance to this project.

In addition to this obligation, the EPISECC project grant agreement includes a Special Clause no 15. According to this Special Clause, the parties to the EPISECC project grant agreement are required to “provide the REA with a written confirmation that it has received (a) favourable opinion(s) of the relevant ethics committee(s) and, if applicable, the regulatory approval(s) of the competent national

or local authority(ies) in the country in which the research is to be carried out before beginning any REA approved research requiring such opinions or approvals.”\textsuperscript{16} Copies of any official approvals from the relevant national or local ethics committees must be provided to the Research Executive Agency.\textsuperscript{17}

### 2.3. Research ethics

Research ethics includes guiding principles for the conduct of researchers. These principles are considered to be good practices that allow to avoid scientific misconduct. KU Leuven is a signatory to the European Charter for Researchers and invites the consortium partners to take into consideration these guidelines throughout the EPISECC project. This Charter provides the following basic guiding principles that can serve as good practices for all parties involved in the EPISECC project.\textsuperscript{18}

1) Adhere to ethical principles: to take into account the relevant ethical practices and fundamental ethical principles.

2) Take professional responsibility: engage in research activities that are relevant to the European society, do not plagiarize but further improve the existing knowledge. In cases of building on the research of others, provide acknowledgement.

3) Demonstrate professional attitude: be familiar with the context of the project (e.g. governing and funding schemes) as well as objectives and relevant legal framework.

4) Demonstrate accountability: be aware of accountability not only for the employers but also towards society as the project is funded by the public funds. Being accountable entails the principles of “sound, transparent and efficient financial management and cooperate with any authorised audits of their research”. Being accountable also means that research output includes research methods.

5) Undertake good practice in research: ensure compliance with relevant legal frameworks (e.g. protection of personal data), back-ups of information in cases of contingencies.

6) Ensure dissemination and exploitation of research results: disseminate research results as it is provided in the contract.

7) Engage with the general public: take effort to inform society about your research activities as this could both educate society and indicate research priorities and public interest.

8) Relation with supervisors: assist and guide researchers in their training phase.

9) Supervision and managerial duties: senior researchers should devote particular attention to their multifaceted role as supervisors, mentors, career advisors, leaders, project coordinators, managers or science communicators.

10) Continue professional development: take an effort to improve your knowledge and skills on a regular basis.

### 2.4. Guidance on research output of the EU funded research projects

The European Research Council, the European Commission and the European Group on Ethics in Science and New Technologies (hereinafter “EGE”) publish opinions providing guidance on how best

\textsuperscript{16} The EPISECC grant agreement No 607078, 6.
\textsuperscript{17} The EPISECC grant agreement No 607078, 6.
\textsuperscript{18} European Charter for Researchers, 11-15.
to address ethical concerns in the EU funded research projects. According to these opinions, research and innovation activities not only should be carried out with ethical principles in mind, but also should take into consideration relevant national, Union and international legislative measures.

According to the European Research Council, the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of a person, the right to non-discrimination and the need to ensure high levels of human health protection, are the key issues that have to be addressed prior to developing new technologies.19 The European Commission Directorate-General has also issued Research Guidelines on ethics for researchers subject to the EU funding, in particular FP7 program. This document requires researchers to “describe the measures taken to encode or anonymise [personal data] […]. Even where only anonymised data are used, adequate security for storage and handling of such data must be demonstrated.”20 This obligation has been meant to hold researchers accountable for their research activities that involve the processing of personal data.

Yet in the context of the EPISECC project, opinions of the EGE are considered to be of a greater relevance as they focus on the development and advancement of information and communications technologies. In particular, the EGE Opinions on “Ethics of Information and Communication Technologies” and “Ethics of Security and Surveillance Technologies” must be considered. Both opinions, alike Decision No. 1982/2006/EC, place a particular emphasis on principles enshrined in the Charter of Fundamental Rights of the European Union.

To ensure that ICT research and innovation addresses ethical concerns, the EGE recommends to avoid the unnecessary collection and use of personal data in case research and innovation activities require to process personal data. This group also suggests to indicate data sources (e.g. time and context when data was collected and for what purpose it was used) and consider issues of informed consent for any personal data being used.21 The EGE notes that the current use of internet, especially data mining capacity and the growing trends of cloud computing, social networks and mobile devices carry a promise of benefitting society at large and the same time it poses challenges to individuals’ fundamental rights. In this respect, a particular emphasis is placed on the fundamental rights to privacy and data protection as well as the freedom of information, as these rights are often affected by ICT systems.

The EGE provides recommendations of the general nature for entities engaged in the development of the ICT. The EGE suggests to take into consideration the following principles while developing new ICT products:

1) Human dignity: the concept of “human dignity” is the basis of the fundamental human rights framework. It is enshrined in the preamble of the Universal Declaration of Human Rights and the subsequent human rights’ instruments. The principle of human dignity is also integrated in the Charter of Fundamental Rights of the European Union (Article 1) and the Treaty on European Union (Articles 2 and 21.1). According to this principle, any action harming any individual is prohibited.

2) Respect of freedom: this includes freedom of thought, conscience and religion as well as freedom of expression and information. The newly developed applications should not impinge on these freedoms.

3) Respect for democracy, citizenship and participation: the developers should make sure that new products do not exclude society members or result in discriminatory actions.

4) Respect of privacy: the right to privacy is listed among the fundamental rights in the Charter of Fundamental Rights of the European Union (Article 7). According to this right, “[e]veryone has the right to respect for his or her private and family life, home and communications.” This right corresponds to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and it preceding case law, following which the concept of “privacy” includes relational privacy (e.g. sexual preferences), spatial privacy (e.g. home environment), medical privacy, and informational privacy (i.e. protection of one’s personal data).

5) Respect of autonomy and informed consent: these two principles constitute the cornerstone of the EU Data Protection Framework. To adhere to these principles, developers have to provide individuals with an information notice and obtain unambiguous consent prior to the processing of their personal data.

6) Justice: according to this principle, the entities are required to ensure the equal access to ICT, and a fair sharing of its benefits.

7) Solidarity among European citizens: this principle requires to ensure that different stakeholders can actively participate, make use of, and have access to the ICT system. Additionally, the EGE supports EU policies encouraging corporate social responsibility practices which result in applications that include privacy enhancing technologies, privacy impact assessment or the privacy by design principle.

2.5. Guidance on information security

While developing a Common Information Space, the EPISECC consortium should take into consideration the OECD Guidelines for the Security of Information Systems and Networks because data that may be shared via this space may include classified, confidential, or restricted information that is subject to legal, organisational or security requirements under laws of Member States. The OECD Guidelines provide the following principles:

1) Awareness: project partners when developing the final solution should be aware of the need for security of information systems and networks and what they can do to enhance security. Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Project partners should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Project partners should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility: project partners when developing the final solution are responsible for the security of information systems and networks. Project partners depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of
those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Project partners should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response: project partners should act in a timely and co-operative manner to prevent, detect and respond to security incidents. Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, project partners should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics: project partners should respect the legitimate interests of others. Given the pervasiveness of information systems and networks in our societies, project partners need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

5) Democracy: the security of information systems and networks should be compatible with essential values of a democratic society. Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment: project partners should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation: project partners should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation’s systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management: project partners should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic,
encompassing all levels of participants’ activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network, security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment: project partners should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Project partners when developing a Common Information Space should continually review, reassess and modify all aspects of security to deal with these evolving risks.

2.6. Ethical concerns about the Common Information Space

As said earlier, prior to setting a Common Information Space, one has to take into consideration not only the relevant EU legal frameworks, but also ethical issues that arise from the use of ICT. The ethical issues table in the description of work for the EPISODE project indicates that the project may process location data. In particular, the table indicates that personal data, which may include location or/and observation of people, will be processed in the context of this project. Provided this, it is expected that at the later stages of the project, in particular, while determining architecture of the Common Information Space, assessment of the measures ensuring integration of ethical and legal concerns, as well as security of the collected personal data should be provided. In addition to this, two specific questions seem to be of relevance while discussing the pan-European information space, namely:

1) How to find the right balance between the first responders’ need to obtain all available information (or could be made available) to information that is actually needed and absolutely necessary to provide a disaster response?
2) Could the Common Information Space run as a cloud application?

In response to the first question, one has to carry out a balancing exercise. This exercise should include assessment of interests and rights at stake of all actors involved in disaster management. After the list of interests and rights is completed, a certain priority could be assigned to each of the issue. For example, the use of location data of an affected person could be assigned higher priority than the right to spatial privacy of an affected person. At the same time, it should be noted that this evaluation could be very subjective if it is not based on some predefined criteria. Work carried out in the context of the inventory developed in WP 3 will make an important contribution to this discussion.

In response to the second question, one has to consider both advantages and disadvantages of the cloud use. While considering disadvantages one has to consider possibilities to mitigate risks associated with cloud computing. For this purpose, a detailed analysis of cloud specific risk analysis should be done. At this stage of the project, the agreement on the architecture on the Common
Information Space has not been reached. Therefore, project partners are invited to consider the list of cloud specific risks, as suggested by ENISA which could have an impact on the final decision:25

1. Loss of governance: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues that may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences.

2. Lock-in: there still is little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in house IT environment. This introduces a dependency on a particular CP for service provision, especially if data portability, as the most fundamental aspect, is not enabled.

3. Isolation failure: multi-tenancy and shared resources are defining characteristics of cloud computing. This risk category covers the failure of mechanisms separating storage, memory, routing and reputation between different tenants (e.g. so-called guest-hopping attacks). However, it should be considered that attacks on resource isolation mechanisms (e.g. against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional OSs.

4. Management interface compromise: customer management interfaces of a public cloud provider are accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.

5. Data protection: cloud computing poses several data protection risks for cloud customers and providers.

6. Insecure or incomplete data deletion: when a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible.

7. Malicious insider: while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include CP system administrators and managed security service providers.

8. Customers’ security expectations: the perception of Security levels by Customers might differentiate from the actual security (and availability) offered by the CP, or the actual temptation of the CP to reduce costs further by sacrificing on some security aspects.

9. Availability Chain: reliance on Internet Connectivity at Customer’s end creates a Single point of failure in many cases.

---

3. Relevance of the EU Data Protection Framework

Disaster response results in data exchange, including personal and sensitive data. In the context of the Common Information Space, the processing of personal data in the course of disaster management is essential and unavoidable. While providing disaster relief, first responders and volunteers exchange vast amounts of data to ensure effective response and distribution of resources. This data may include their own location, relevant observations to enhance situational awareness (e.g. geo-referenced data in form of maps), and data about affected persons.

This deliverable divides all actors involved in disaster management situations into three general groups — first responders, volunteers, and affected persons (Table 1). It should be noted that in practice this division is not crystal clear. There is a complex interdependency between the groups. In particular, distinguishing between first responders and volunteers may be difficult. In many European countries (e.g. Austria and Germany) teams of first responders are built from professional as well as trained and pre-registered volunteers.

The identified three general groups — despite representing intrinsically different roles in crisis management — are comprised of natural persons. Therefore, everyone within these groups can become a data subject within the meaning of Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereinafter “EU Data Protection Directive”, “Directive 95/46/EC”, or “the Directive”). Indeed, everyone within these groups is an identifiable person or can be identified “directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.”

Additionally, it can be argued that the processing of personal data in the field of civil protection falls within the scope of Directive 95/46/EC because as of the enforcement of the Lisbon Treaty, the EU has gained the supporting competences in this field. According to Article 3 (2) of Directive 95/46/EC only activities that fall outside the scope of Union law are not subject to Directive 95/46/EC. In practice, this means that EU data protection rules and principles apply to the processing of personal data while providing public protection and disaster relief.

Finally, the requirements to protect individuals’ privacy and personal data stem not only from the primary EU law namely, the Charter of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union (i.e. Article 16), as well Directive 95/46/EC, but also from the documents developed by the Council of Europe. In this respect, the core documents that set the states’ positive obligations to protect of individuals’ privacy and personal data include the European Convention on Human Rights and to the Convention no. 108 on data protection.

Provided this reasoning there is no doubt as to the relevance of the EU Data Protection Framework to the processing of data related to first responders, volunteers, and affected people in case of a disaster management. However, it should be noted, that there are significant differences in data processing of the identified groups. The processing of personal data of the identified groups, for example, may be subject to different legitimate basis. Also, types of personal data that are being processed as well as risk level associated to the processing operations may vary.

The following sections of this part will address requirements of the current EU Data Protection Framework that have to be considered prior to setting up a Common Information Space. In

---

26 Directive 95/46/EC, Article 2 (a).
anticipation of the adoption of the proposal for the General Data Protection Regulation, the report will identify relevant changes to the existing legal framework. The last section of this report will provide information about measures taken by the EPISECC to comply with the EU Data Protection Framework.

Table 1: Mapping processing of personal data in a disaster relief

<table>
<thead>
<tr>
<th>Categories of data subjects</th>
<th>Legal basis for data processing</th>
<th>Personal data being processed</th>
</tr>
</thead>
<tbody>
<tr>
<td>First responders</td>
<td>Legitimate interest of a data controller (e.g. employment contracts)</td>
<td>May include, but are not limited to name, surname; personal and business address, e-mail address, telephone and fax numbers; national identification number (ID), passport data, social security number; marital status, dependents, emergency contact information; demographic information, including nationality or citizenship, date and place of birth, gender, military status, residency status and work permits, driving license, a photograph, education, training and qualifications, and language skills.</td>
</tr>
</tbody>
</table>
| Volunteers (e.g. preregistered, trained) | Consent (e.g. signed forms)  
Legitimate interest of a data controller | May include similar information as of employed first responders. However, this is information may be limited to necessary contact details. |
| Affected people                  | Vital or essential interests of the data subject 
Necessity for the performance of the task carried in the public interest 
Legitimate interest of a data controller | May include various types of personal data, including sensitive information (e.g. information about affected person’s health). |

3.1. The background and scope of application

The underlying objectives of the EU Data Protection Directive, adopted in 1995, were to harmonise data protection regulation among the EU Member States and to enable the free flow of personal data within the EU. It should be noted that Directive 95/46/EC is not a directly applicable legal
instrument; it provides a minimum set of rules for the EU Member States. Similarly to other directives, Directive 95/46/EC is binding, “as to the result to be achieved” and leaves it to the discretion of the Member States to choose methods implementing legal requirements. All of the EU Member States have implemented rules set forth by the Directive into their national laws regulating data processing. However, due to different choices made while implementing the Directive, the EU Data Protection Framework is harmonised to a limited extent. Therefore, prior to setting up a processing operation of personal data, laws of the relevant Member State must be considered.

The EU Data Protection Directive applies to “the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.” The Directive assigns a very broad meaning to the processing. In the context of the Directive, the processing means “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.” In practice, this means that any operation performed upon personal data (e.g. entry of data about a person, location of a person, or description of person’s health condition) constitutes data processing.

Article 3 of the Directive delineates the scope of the Directive. According to this article, the Directive is not applicable, if data processing activities are undertaken in the context of law enforcement; if data processing falls under the so called “house hold exception”; or if data processing concerns public security, defence, and/or state security. Recital 16 specifies that in case the processing (e.g. video surveillance) “is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law”, the Data Protection Directive is not applicable. This means that Directive is not applicable in the following three situations:

- the processing of personal data “falls outside the scope of Community law”.
- the processing of personal data is part of law enforcement activities or concerns public security, defence, or national security. Typically, the content of definitions for public security, defence, and national security vary across the Member States. This leads to the situations where disaster management may fall under different concepts. Depending on the type of a crisis or a critical event (e.g. riots or flooding), the crisis management may fall within the scope of public security, defence, and national security.
- the processing of personal data is carried out by a natural person in the course of a household activity.

It is significant to note that the Directive entails a comprehensive approach and is applicable to all sectors and entities processing personal data. As a result of this comprehensive approach, the Directive does not specifically address data processing that is being performed in the context of

---

28 Note: the Directive has been implemented by the members of the European Economic Area that are not part of the EU, namely Iceland, Liechtenstein and Norway.
29 Directive 95/46/EC, Article 3.
30 Directive 95/46/EC, Article 2 (b).
31 Directive 95/46/EC, Recital 16.
32 Directive 95/46/EC, Article 3.
disaster relief. This opens a debate on the extent to which Directive 95/46/EC is applicable in the context of disaster relief.

3.2. Responsibilities and identification of actors

While considering application of the Directive it is important to identify roles of actors and agents involved in a particular data processing operation or set thereof. As pointed out by the European Union Agency for Fundamental Rights, “the most important consequence of being a controller or a processor is legal responsibility for complying with the respective obligations under data protection law.” While both controller and processor can be “a natural or legal person, public authority, agency or any other body”, in the EU Data Protection Framework, it is the data controller who carries the main responsibility for the processing of personal data. The controller defines purposes and means of any processing, it has to inform a data subject about the data processing at the time of collection, it has to notify the national data protection authority about the processing intent, and it is responsible for the integrity of collected data, even if that data is processed by a processor. Whereas a processor’s responsibility is limited to security of personal data; the processor processes personal data on the basis of instruction of the controller.

Additionally, identifying relevant actors and their responsibilities is of great assistance while determining the applicable law to the data processing. The Article 29 Working Party, representing views of European data protection authorities, is of opinion that “the main criteria in determining the applicable law are the location of the establishment of the controller, and the location of the means or equipment being used when the controller is established outside the EEA.” This means that neither the nationality or a place of habitual residence of data subjects (i.e. persons whose personal data are being processed), nor the physical location of the personal data, are decisive for this purpose.

Finally, it can be observed that application of new technologies in the field of disaster response poses the following challenges. First, assigning roles to agents providing disaster relief (i.e. determining who is a controller and who is a processor) is difficult as data exchange in a disaster response situation has become complex; often data are being processed via data maintenance tools over which first respondents as well as individual organisation have no influence. Second, due to the existing differences in Member States’ civil protection mechanisms identifying and categorizing data subjects whose data will be processed in a disaster situation requires contextual analysis.

3.3. General principles

To be compliant with the EU Data Protection Framework, the controller has to ensure adherence to the core principles of the EU Data Protection Framework. In particular, the controller has to ensure that personal data are being processed in a fair and lawful way. It is also required that personal data are “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.”

---

34 Directive 95/46/EC, Article 2 (d).
35 Directive 95/46/EC, Article 2 (e).
37 Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law (WP 179) 8.
The Article 29 Data Protection Working Party recommends that the controller identifies and documents the purposes of the data processing activities.\(^39\) The Working Party deems that “specification of the purpose in writing and production of adequate documentation” has a twofold aim.\(^40\) First, documenting the purposes of data purposes can provide evidence that the controller has complied with legal requirements, and second, it can facilitate an audit trail of accountability. The Working Party, also, suggests that in case controllers opt for legitimate interests as the legal ground ensuring lawfulness of the processing, controllers should carry out a balancing test. The balancing test should be carried out at the time of specifying purposes of data collection. The balancing test would allow determination of whether the controller has a legitimate interest to undertake foreseen data collection in a particular situation and whether that processing will not infringe on data subject’s rights.\(^41\)

In addition to the obligation to define purposes of data processing, a controller has to ensure that gathered personal data is “adequate, relevant and not excessive in relation to the purposes for which they are collected.”\(^42\) These three requirements form the core of so called “data minimisation principle”. Following the rationale of this principle, “needs based analysis” should be conducted. This analysis would allow to identify relevant personal data for a certain operation. Additionally, according to Article 6 (d), records of personal data should be accurate and, where necessary, kept up to date. When the processing of the personal data is no longer necessary for the defined purposes, the gathered data should be erased or deleted.

Finally, while applying above listed data quality principles, the controller has to consider the underlying principles of the EU Data Protection Framework — proportionality and transparency. For example, the controller has to question whether the collection of selected data sets is necessary for the purposes of that particular process and whether data subjects are informed and aware of the processing.

### 3.4. Conditions for lawful processing of personal data

To ensure compliance with the first data quality principle the controller has to ensure that personal data is being processed in a lawful way. The Directive foresees a list of conditions providing legitimate basis for the processing of personal data. In general, the processing of individual’s (i.e. data subject’s) personal data is lawful if unambiguous consent of the data subject is provided or if the processing of personal data is necessary in a particular situation. A particular situation may also include the performance of a contract, compliance with a legal obligation, protection of the vital interests of the data subject, the performance of a task carried out in the public interest, the exercise of official authority, and the legitimate interests of a controller.\(^43\)

It can be assumed that different legal basis would be used to legitimise the processing of personal data of the three general groups of actors (i.e. first responders, volunteers, and affected people) involved in disaster management. For example, while providing disaster relief the processing of first

---


\(^{40}\) Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203) 17.

\(^{41}\) Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217) 43-44.

\(^{42}\) Directive 95/46/EC, Article 7 (c).

\(^{43}\) Directive 95/46/EC, Article 7.
responders’ personal data could be legitimised via an employment contract. Whereas the processing of personal data of affected people could fall under the condition of vital interests of data subject. As the European Agency for Fundamental Rights explains, “interests which are closely related to the survival of the data subject, could be the basis for the legitimate use of health data or of data about missing persons.”

3.4.1. Legitimising the processing of personal data of affected people

It can be argued that first responders may invoke different legal bases to legitimise the processing of personal data of affected people. Presumably, first responders could rely on three different grounds while processing data of affected people.

First, they could consider Article 7 (d) and its accompanying Recital 31 to provide a condition under which processing of personal data could be legitimised – the vital or essential interests of the data subject. This wording can lead to a wide range of interpretations and only further comparative analysis of the Member States’ implementation of this wording could allow certain generalisations to be made on an EU level. The European Data Protection Authorities consider the application of this provision to be restricted to “questions of life and death, or at the very least, threats that pose a risk of injury or other damage to the health of the data subject.” As a result of this interpretation it can be questioned whether the processing of personal data of affected people would always fall under this ground (e.g. consider a flood rescue during which there is no direct danger to a data subject) and who would be competent to interpret these “questions of life and death”.

Second, it could be argued that the processing of personal data of affected people could fall within the scope of Article 7 (e). According to this paragraph, the processing of personal data is lawful if the “processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.” In practice, this would mean that the processing could be legitimised if it is essential for the performance of a task carried out in the public interest or if the data controller (i.e. the organisation providing first response) has authority to act in a particular field. The European Data Regulators explain that Article 7(e) “has potentially a very broad scope of application, which pleads for a strict interpretation and a clear identification, on a case by case basis, of the public interest at stake and the official authority justifying the processing.” Therefore, while there is no doubt that first responders providing public protection and disaster relief are subject to national laws and act in the public interest, they must carefully consider the ground legitimising the processing of personal data of affected people.

Third, first responders could claim that it is in their own legitimate interest to process personal data of affected people (Article 7 (f)). This claim, as suggested by European Data Protection Regulators, “may help prevent over-reliance on other legal grounds.” However, the ground of legitimate

---

45 On the basis of this analysis a note has been submitted to the ELSI workshop at ISCRAM 2015.
47 Directive 95/46/EC Article 7 (e).
interests “should not be automatically chosen, or its use unduly extended on the basis of a perception that it is less constraining than the other grounds.”\textsuperscript{50} In cases where first responders decide to rely on this legal ground, they should carry out a balancing test which would ponder on the legitimate interests of the controller and the interests or fundamental rights and freedoms of the data subject.\textsuperscript{51}

To conclude this part, it could be suggested that one, prior to setting up new databases and determining the legal ground for the processing of personal data of affected people, take into consideration recommendations made by the European Data Protection Regulations (i.e. Article 29 Working Party) and the case law developed by the Court of Justice of the EU (CJEU). Recently the CJEU has emphasised on several occasions that the interpretation of “Directive 95/46 is intended to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data.”\textsuperscript{52} Therefore, “the protection of the fundamental right to private life guaranteed under Article 7 of the Charter of Fundamental Rights of the European Union requires that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.”\textsuperscript{53} This implies that first responders should not rely on the exception of vital interests of data subjects to process personal data of affected persons.

3.4.2. Legitimising the processing of personal data of first responders\textsuperscript{54}

In case of a disaster European societies count on assistance of first responders, such as the Red Cross or firefighter units.\textsuperscript{55} Typically, one would deem that disaster response is provided by persons that are employed by specialised organisations. However, in reality first responses do not constitute a uniform group of employees. This group includes both employees and volunteers. Consequently, this means that data of first responders are processed in two different contexts – employment and voluntary participation.

Typically, the employment contract between the employer and employee addresses the use of personal data in the employment context. Provided the unequal balance of power in an employer-employee relationship, the controller (i.e. an employer or an organisation providing disaster relief) is not recommended to choose consent as a legal basis legitimising the processing of personal data. Consent should be “freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.”\textsuperscript{56} The exact type of consent depends on the personal data that is being processed (i.e. special or general categories of personal data). Consent may be required to be unambiguous or explicit. In case of processing special categories of data, such as data related to one’s health, consent must be explicit.\textsuperscript{57} Explicit consent is

\textsuperscript{50} Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 2014.
\textsuperscript{52} European Court of Justice, C-212/13 (Ryněš Case), paragraph 27. See also Google Spain case, C-131/12, EU:C:2014:317, paragraph 66.
\textsuperscript{53} European Court of Justice, C-212/13 (Ryněš Case), paragraph 28.
\textsuperscript{54} On the basis of this analysis a note has been submitted to the ISCRAM 2015.
\textsuperscript{55} “Disaster” means any situation which has or may have a severe impact on people, the environment, or property, including cultural heritage", from Decision No 1313/2013/EU Article 4.1.
\textsuperscript{56} Directive 95/46/EC, Article 2 (h).
\textsuperscript{57} Directive 95/46/EC, Article 8 (1). Special categories of data include so-called sensitive data, which relate to “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”
understood as “an affirmative action to express their desire to accept a form.”\(^{58}\) Therefore, in case of an app for first responders, the employers should consider the use of the other five possible grounds for legitimizing the processing of personal data, mentioned in the relevant laws. For example, a legitimate interest could be a reasonable ground for the processing of personal data. Since apps could be used to process sound and image and other data, e.g. their location, communication and performance, the collection of such data would result in employee monitoring.\(^{59}\) According to the Article 29 Working Party, employee monitoring is allowed only if necessary, legitimate, proportional and transparent. The processing of employee data falls within the scope of the EU Data Protection Framework.\(^{60}\) For this reason, the organisations opting for the use of apps during the disaster relief should take into consideration possible implications of such system on employees’ rights.

Volunteers often assist first responders providing disaster response. The involvement of volunteers consequently results in processing of their personal data. The organisations providing disaster relief should consider the most appropriate legal ground legitimising processing volunteers’ personal data. Differently from the employed first responders, volunteers are not subordinates of the specialised organisation. Consequently, volunteers have more freedom and choice as to providing their consent. However, relying on consent as a legitimate ground for the data processing may not be desirable. A volunteer can withdraw his or her consent at any time. As a result of consent withdrawal, first responders may be asked to delete all the data about a volunteer. Yet the immediate action may be not possible because in some countries data about operations has to be kept to the reporting purposes. Therefore, it is not recommended to rely on consent for the processing of volunteers’ personal data.

3.5. Data subjects’ rights

Under the EU Data Protection Framework every data subjects are awarded a number of rights provided in the Directive. These rights include general and specific rights. General rights include individuals’ right to the processing of their personal data that is fair, lawful, and has a legitimate purpose. Specific rights include the right to information about the processing operations, the right to the right to object to the processing on legitimate grounds, and the rights to access, rectification and erasure.

The right to information requires the controller to provide a data subject with a notification which would include the following information items, the identity of the controller; the purpose of the processing; the recipients (third parties if any of the data); and the rights of the data subjects.\(^{61}\)

3.6. Security requirements

Directive 95/46/EC requires organisations, or in other words, data controllers to ensure the integrity of personal data and take “appropriate technical and organisational measures” to prevent

---


\(^{59}\) Location data is understood as a geospatial data; it “may refer to the latitude, longitude and altitude of the user’s terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded”, as provided in the E-Privacy Directive.

\(^{60}\) Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 3.

\(^{61}\) Directive 95/46/EC, Article 10.
unauthorised disclosure or access to collected personal data. In practice, this implies that the controller has the discretion (i.e. an organisation defining the purposes of the processing) to select these measures. Technical and organisational measures may include but are not limited to governance and risk management, human resources security, security of systems and facilities, operations management, incident management, business continuity management, monitoring, auditing and testing. The guidance provided by the Directive is limited to requiring data controllers to take into account the state of the art of available technologies and the cost of their implementation. The Directive requires that any measures undertaken by the controller will result in an appropriate level of security provided the risks associated to the processing. To illustrate the particular examples of technical and organisational measures, the use of cryptography (e.g. encryption) and establishment of access control to the information systems could be considered. More specific technical requirements were addressed in the report for Task 3.1.

It is significant to note, that the controller in case of outsourcing the processing of personal data to a third party remains the key agent responsible for the processing. The outsourcing should be documented (e.g. by a contract or legal act binding the processor). The document should explicitly state that the processor will act only on the controller’s instructions and that it will take “appropriate technical and organisational measures” to ensure integrity of the collected personal data.  

Directive 2002/58/EC as amended by Directive 2009/136/EC (hereinafter “E-privacy Directive” or “Directive”) on privacy and electronic communications reiterates above described security requirements for communication data. E-Privacy Directive sets requirements for the providers of publicly available electronic communications services and the providers of public communications networks. This Directive also foresees an obligation for providers of a publicly available electronic communications service to inform affected data subjects in case of a data breach. However, the applicability of this law to the Common Information Space can be questioned. E-privacy Directive is applicable to the processing of personal data in context of publicly available electronic communications services in public communications networks. Therefore, to decide on the application of the Directive, a particular interface that is used for data processing has to be considered. If the processing of personal data in a disaster management situation falls within the scope of the E-Privacy Directive, then it should be applied with the Commission Regulation No 611/2013. The Commission Regulation No 611/2013 provides measures applicable to the notification of personal data breaches under E-Privacy Directive.

In case of disaster management and response, data processing takes place via communication networks and tools that many times are developed for exclusive use of first responders. A good indication as to the types of communication data has been provided by the European Union Agency for Network and Information Security (hereinafter “ENISA”). The ENISA has identified the typical communications systems used in an emergency situation, namely: Terrestrial Trunked Radio (i.e. emergency radio), data services, often on commercial networks and public networks. Provided this, it may be of relevance to consider provisions introduced by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services.

62 Directive 95/46/EC, Article 17.
63 Directive 95/46/EC, Article 17
3.7. Anticipating the adoption of the General Data Protection Regulation

The current EU Data Protection Framework is under revision. The European Commission published a proposal for the General Data Protection Regulation in January 2012. The legislative proposal has been in the first reading of the EU legislative process since 2012. On March 12, 2014 the European Parliament in its plenary vote confirmed the amendments to the General Data Protection Regulation made by the Committee in charge. The Council of the EU adopted a common position on the proposed legislative act in June 2015. Currently, it is speculated that the EU legislative actors (i.e. the Commission, the Parliament and the Council) will close the trilogue negotiations and agree on the final text in late 2015. Yet the outcome of the negotiations is rather uncertain.

The proposed General Data Protection Regulation (GDPR) includes terms of “natural or man made disasters” in the proposed Recital 59. Recital 59 states that the EU Member States can adopt provisions in their national laws limiting data subjects’ rights that are “necessary and proportionate in a democratic society to safeguard public security, including the protection of human life especially in response to natural or man made disasters, the prevention, investigation and prosecution of criminal offences or of breaches of ethics for regulated professions, other specific and well-defined public interests of the Union or of a Member State.” The Council has proposed to expand the scope of the situations in which certain restrictions can be imposed on the processing of personal data and to include “social protection, public health and humanitarian purposes, such as the performance of a task incumbent upon the International Red Cross and Red Crescent Movement.” It seems that the EU legislators agree that any restrictions imposed on data protection rights must be in compliance with requirements set out by the Charter of Fundamental Rights of the European Union and by the European Convention on Human Rights.

While due to the limitations imposed by the subsidiarity principle the EU does not provide for more extensive guidance on the processing of personal data in the field of public protection and disaster relief, the GDPR will have an impact on the processing on personal data in the context public protection and disaster relief.

It is important to note that data processing of first responders (e.g. employees or trained volunteers) and volunteers would occur in a different context than data processing of people affected by a disaster. Consequently, this would mean that controllers, that is organisations defining purposes of the processing, should take into consideration new principles that will be introduced in the EU Data Protection Framework. In particular, it should be pointed out that seems that once the GDPR is

---

69 Note: the EU capacity to develop policies in various domains is limited to the competences conferred by the Member States upon the founding treaties; the field of civil protection is not an exception. The EU, as set forth in Article 6 of the Treaty on the Functioning of the European Union (TFEU) has so called “supporting competences” in the civil protection matters; the EU can only intervene to support, coordinate or complement actions of Member States.
adopted, public authorities no longer will be allowed to rely on the legitimate interest of the controller as a legal basis legitimising the processing of personal data.\textsuperscript{70}

During the discussion on the architecture of future Common Information Space a particular attention should be paid to the general accountability article.\textsuperscript{71} This article would require data controllers to develop policies addressing the management of personal data and to implement measures allowing demonstration of compliance with the EU Data Protection Framework. To achieve these objectives, according to the general accountability article, the controllers would be required to keep relevant documentation of all processing operations under its responsibility (Article 28). Controllers would be also required to take appropriate technical and organisational measures that would ensure security of the processing operations (Article 30).\textsuperscript{72}

Prior to launching a data processing operation controllers would have an obligation to conduct a data protection impact assessment (hereinafter “PDIA”) in situations when processing may “present risks to the rights and freedoms of data subjects” (Article 33). Then, controllers would be obliged to obtain an authorisation from the DPA prior to the processing operations in cases where the PDIA is required or the DPA deems it to be necessary (Article 34). Lastly, data controllers may be required to designate a data protection officer who would ensure an entity’s compliance with the EU Data Protection Framework (Article 35).

In addition to the general accountability provision, prior to setting up the Common Information Space one needs to consider the data protection by design and by default principles. According to these principles set for in Article 23 of the proposed General Data Protection Regulations, the controller is required to consider the purpose of the data processing at the time of setting up the system and ensure that only relevant data to the processing is collected. However, as the text of the proposed Regulation is subject to change, it is hard to measure the impact of these provisions on the processing of personal data in disaster management situations.

3.8. Impact on exchanging and using personal data the context of disaster relief

It can be concluded that the EU Data Protection Framework is applicable to the processing of personal data in the context of public protection and disaster relief. It was demonstrated that this framework does not restrict the processing of personal data while providing disaster response. However, to be compliant with EU data protection rules, the data controller (i.e. an entity determining purposes of the processing) is required to follow certain requirements, general and data quality principles. Following the rationale of the EU data protection framework, it is possible to identify three general categories of data subjects involved in a disaster relief, namely, first responders, volunteers, and affected people. The processing of personal data related to individuals within these three groups — despite their different roles in disaster management—should be based on different legitimate grounds. This legitimate ground has to be considered prior to setting up the Common Information Space. For the processing of personal data to be lawful, the controller has to define these purposes at the inception of the information system and a data subject should be informed about such purposes prior of at the time of obtaining personal data. It is essential to understand that because of the broad scope of the EU definition for ‘personal data’, many different types of information that can be directly or indirectly linked with an identifiable individual.

\textsuperscript{70} General Data Protection Regulation, Article 6. 1(f).
\textsuperscript{71} General Data Protection Regulation, Article 22.
\textsuperscript{72} Directive 95/46/EC includes the same obligation.
The current EU Data Protection Framework is set by Directive 95/46/EC which is of general scope and does not address a specific situation of disaster management in which processing of personal data of affected person may occur. It leaves an open interpretation as to the grounds legitimising data processing of affected people. Article 7 (d) — on the vital or essential interests of the data subject — or (e) — necessity for the performance of the task carried in the public interest — as well as Article 7 (f) — legitimate interests of the controller — could be used to legitimize the processing of personal data of affected people. The processing of personal data of first responders should adhere to the EU Data Protection Framework. It seems that in the revised EU Data Protection Framework fragmentation of regulatory approaches will remain present. If the proposed Regulation text is adopted, the Member States would maintain competency to enact national rules that are deemed to be necessary and proportionate to the intended aims.

3.9. EPISECC compliance with the EU Data Protection Framework in WP 3

The EU Data Protection Framework was considered in the context of WP 3. To meet the objectives of WP 3, the EPISECC has developed an inventory that indicates similarities, differences, weaknesses and strengths of the most commonly used international standards for information management as well procedures, practices developed by first responders. The inventory was a follow-up of a desk research on publicly available information (e.g. sources accessible online) performed in WP 2.

While the inventory aims at pointing out technical information that would be subsequently used when developing a Common Information Space, it includes several types of personal data (e.g. a name and an email address). After carefully considering the necessity of personal data elements, the technical committee concluded that in order to ensure quality check of information entered into the inventory, contact details of volunteers (i.e. interviewees of the questionnaire) were necessary. Therefore, in addition to information about disasters or critical events, volunteers were requested to provide their first names, surnames, and addresses of their email accounts affiliated with the employment place. Provided that first names, surnames, and addresses of email accounts allow establishing direct or indirect link to an identified or identifiable natural person, these types of data are considered to be personal data.73 As indicated above, in the EU, for the processing of personal data to be legitimate, it has to adhere to the rules set forth by Data Protection Directive (Directive 95/46/EC). Directive 95/46/EC is transposed by the EU Member States, and thus every Member State has a national law implementing the Directive. Provided that the questionnaire of the inventory is on the AIT servers in Austria, the consortium has consulted the Austrian Data Protection Act implementing the Directive - Datenschutzgesetz 2000.74

Even though, the Austrian Data Protection Law also foresees exemptions for the processing of personal data that has been published, the EPISECC consortium following up on the requirements outlined in Directive 95/46/EC, the Austrian Data Protection Act, and Consent Guidance for FP7 projects has developed a consent form (see Annex II).75 The developed consent form includes an information notice. The consent form indicates the AIT as a data controller who is responsible for the handling of personal data.

---

According to the Austrian Data Protection Act, a data subject’s consent means [“Zustimmung”]: the valid declaration of intention of the data subject, given without constraint, that he agrees to the use of data relating to him in a given case, after having been informed about the prevalent circumstances.\(^{76}\)

This means that to be valid consent has to meet the following criteria:

- the data subject must be provided with all relevant information about the data to be processed, the purpose of the respective data processing and any potential data recipients;
- the consent must be given without any restraints; and
- the data subject has to receive explicit information about his right to revoke his consent at anytime, without giving reason for such revocation.

To adhere to the EU Data Protection Framework in the context of WP 3, the consortium partners took the following measures:

- Developed an information notice that is provided to participants (i.e. volunteers) of the EPISECC inventory, in other words, data subjects (see Annex II). According to the requirements listed in Articles 24 and 26 of the Datenschutzgesetz 2000, the information notice describes the purposes of the data application for which the data is collected, the name and contact details of the data controller, the purpose of the use of data and the legal basis of the processing intelligible form (see Annex II). Additionally, the information notice, requests data subjects to alert the controller about the data that may be qualified as classified, confidential, restricted information or as a special category of data, as defined in Directive 95/46/EC.\(^{77}\)

- The AIT, assisted by its legal department, took measures to notify the national data protection authority about the processing of personal data, as required in Article 17 of the Austrian Data Protection Act. A letter confirming the notification is included in Annex IV.

- According to Article 14 of the Datenschutzgesetz 2000, data controllers (i.e., entities defining the purposes of data collection) are required to ensure security of the processing. Data controllers carry responsibility for implementing appropriate technical and organizational measures safeguarding the integrity of collected personal data. Safeguarding integrity include measures preventing accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The AIT implemented organisational, technical and physical security measures that include the storage of the information in the database and the application server which is located in a closed server room in Seibersdorf (AIT) and encryption of communications between client and server via the “https” link. Also, the AIT deployed an access control mechanism, which permits only certain users to access, process, or alter data, and at the same time, introduced limitations on users’ actions.


\(^{77}\) According to Article 2 of Directive 95/46/EC, personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity,” special categories of data (sometimes referred to as sensitive data) include information about “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”
More specifically, the AIT access control scheme awards Administrator and Expert users with full access to raw data and differentiates among the 4 groups of users:

- **Administrator**: the AIT appointed a representative who takes responsibility for the questionnaire and the collected data. The main characteristics of the administrator’s profile are:
  - Full access to all data (Read/Write/Update/Delete, Alter structure)
  - Administration of metadata and users
  - Administration of questionnaires
  - Held only by AIT employees who work on the EPSECC project

- **Expert user**:
  - Read/Write access to all data (includes also raw data)
  - Report generation (statistic summary, anonymous results of raw data)
  - Held by key partners (like DLR, AIT, HITEC, UNIST) involved in developing indicators.

- **Guest user**:
  - Read access to generated reports (statistic summary, anonymous results of raw data)
  - Held by all partners and stakeholders

- **Respondent**:
  - Can read/write/Update only the own content

In addition to the above listed measures, the EPSECC consortium has consulted the KU Leuven Social and Societal Ethics Committee regarding the procedure of contacting and collecting information from the participants. The EPSECC internal ethics task force decided to consult the KU Leuven Social and Societal Ethics Committee because it is responsible for evaluating research on human subjects that is not related to health science practices or includes medical or pharmacological procedures. It includes a multidisciplinary panel of experts for ethical review of research in the humanities and the behavioural or social science research traditions. While preparing the application form to the KU Leuven Social and Societal Ethics Committee, the consortium partners held debates about the procedure and necessary types of data that are needed to meet the purposes of the inventory. The application form as well as its approval are included in Annex III of this deliverable.

---

78 More information about the composition and responsibilities of the Committee is available at: https://admin.kuleuven.be/raden/en/sme#section-0.
4. Relevance of Public Sector Data and its Regulation

Public sector is known for holding the wealth of data, yet one needs skills and knowledge to make use of this data. To facilitate use, access, and subsequent innovation, several directives promoting the availability of data held by the public sector have been developed. The directives aim at enhancing availability of public sector data and therefore they could be of great value to first responders providing disaster relief. Therefore, the use of public sector data has to be considered in the context of the Common Information Space.

At the moment, the following EU Directives could be of importance to the EPISCC project:


In order to provide an overview of how these legal measures could possibly provide first responders with more opportunities to exchange or use public sector data originating in the EU Member States, an analysis of the above listed directives follows in the subsequent sections.

4.1. Aarhus Directive

The Aarhus Directive aims to enhance the availability of environmental information that is held by or for public authorities of the Member States. It introduces obligations for public authorities to make such information available to the public, both upon a request of applicants and on their own initiative.

4.1.1. Scope of application

The obligations of the Aarhus Directive relate only to environmental information that is held by or for public authorities of the Member States. This makes “environmental information” and “public authority” the two most important concepts while delineating the scope of application of this directive.

The notion of environmental information in the Aarhus Directive refers to information on a specific list of topics; be it in written, visual, aural, electronic or any other material form. First of all, such environmental information can refer to information on the state of the elements of the environment.

---

80 Note: it addresses an important pillar of the Aarhus Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters.
82 See: Aarhus Directive, Articles 3 and 7.
83 Aarhus Directive, Article 2.1.
such as air, water or landscape. This includes information on factors (e.g. noise, radiation and waste) and measures (e.g. legislation, plans and programs) that are likely to affect the state of these elements. Secondly, environmental information can also refer to reports on the implementation of environmental legislation, as well as to economic analyses and assumptions related to measures that are likely to affect the state of the elements of the environment. Finally, environmental information can also refer to the state of human health and safety, inasmuch as they may be affected by the state of the elements of the environment or by the factors and measures relating to these elements.

The notion of a public authority is also provided in the Aarhus Directive. This directive regards the notion of public authority as:

1) a government or other public administration;
2) a natural or legal person who performs public administrative functions under national law; or
3) a natural or legal person who under control of one of the previous bodies or persons qualifying as a public authority has public responsibilities or functions relating to the environment or provides public services relating to the environment.

This broad definition means that, for example, a private company can qualify as a public authority in the sense of the Aarhus directive if it is found to have a public responsibility or function that relates to the environment and that is controlled by a government or public administration.

4.1.2. Access to environmental information upon request

The Aarhus Directive obliges public authorities to make their environmental information available upon request. The Directive specifies several aspects of this obligation.

First of all, the Aarhus Directive determines on what grounds a public authority could grant or refuse a request to make environmental information available. In this regard, the directive stipulates the principle that a public authority is required to make its environmental information available to all applicants, at their request and without these applicants having to state an interest.

The directive foresees derogations from this principle in two lists of possible valid reasons for a public authority to refuse an applicant’s request to access its environmental information. The first list enumerates formal grounds reasons to refuse access to information. This list, in particular, states that Member State may allow public authorities to refuse a request for environmental information: 1) if the information requested is not held by or for that public authority; 2) if the request is too general or manifestly unreasonable; or 3) if the request concerns internal communications or unfinished documents or data.

The second list enumerates reasons that relate to a specific protected interest. This list, in essence, states that Member State may allow public authorities to refuse a request for environmental information if disclosure of the information would adversely affect: 1) the confidentiality of the proceedings of public authorities; 2) international relations, public security or national defence; 3) the course of justice; 4) the confidentiality of commercial or

---

84 Aarhus Directive, Article 2.1 (a).
85 Aarhus Directive, Article 2.1.
86 Aarhus Directive, Article 2.1 (e).
87 Aarhus Directive, Article 2.1 (f).
88 Aarhus Directive, Article 2.2.
89 Aarhus Directive, Article 3.
90 Aarhus Directive, Article 3.1.
92 Aarhus Directive, Article 4.1. The valid reasons listed in the Directive are not mandatory. The Member States are therefore free to choose which of them to implement into their domestic laws. In addition, the actual decision about calling upon such a valid reason to refuse access is in the discretion of the public authority. The public authority can refuse access on these grounds, but it does not have to.
industrial information; 5) intellectual property rights; 6) the confidentiality of personal data 7) the protection of the environment. The Aarhus Directive stipulates that the valid reasons to refuse a request for access are all to be interpreted in a restrictive way, taking into account the relevant interests. The directive specifically requires that, in every case, the public interest served by disclosure is weighed against the interest served by limiting or conditioning the access.

Second, the directive gives instructions on the form or format in which a public authority is to make environmental information available, upon granting a request to access this information. As a rule, the directive requires a public authority to make the environmental information available in the specific form or format requested by the applicant. The public authority can, however, derogate from this rule if the information is already available in another, easily accessible form or format or if it is reasonable for the public authority to make it available in another form or format. In addition the directive also requires public authorities to make all reasonable efforts to keep their environmental information in forms or formats that are readily reproducible and accessible by computer telecommunications or by other electronic means.

Thirdly, the directive lays down rules on the opportunity for public authorities to make access to environmental information dependent on payment. The directive in particular stipulates that public authorities may not charge for examination in situ of the information requested. It also forbids charging for access to specified public registers and lists that hold information on the public authorities holding environmental information. In contrast to what is the case for examination in situ, the Directive does allow public authorities to charge for supplying environmental information, provided that the charge does exceed a reasonable amount. The directive does, however, require public authorities to inform applicants on the charges made.

Fourthly, the directive sets public authorities a time frame to handle an applicant’s request for environmental information. Having regard to any timescale specified by the applicant the directive requires public authorities to handle requests of the applicant, as a rule, as soon as possible or, at the latest, within one month after having received the request. This timeframe can be extend to two months if the volume and the complexity of the information requested makes it impossible to handle the request within one month after the request was made.

Fifthly, the directive requires that a public authority’s decision on granting access to environmental information can be subjected to review. In particular, the directive requires Member States to ensure a possibility of an administrative and judicial review of submitted requests. The directive also allows Member States to give access to legal recourse to third parties incriminated by the disclosure of information.

---

93 See: Aarhus Directive, Article 4.2 deals with the non-validity of some of these reasons when it comes to refusing requests that relate to information on emissions into the environment.
94 Aarhus Directive, Article 4.2.
95 Aarhus Directive, Article 3.4.
96 Aarhus Directive, Article 3.4.
97 Aarhus Directive, Article 5.
98 Aarhus Directive, Article 5.1.
99 Aarhus Directive, Articles 5.1 and 3.5.
100 Aarhus Directive, Article 5.2.
101 Aarhus Directive, Article 5.3.
102 Aarhus Directive, Article 3.2 (a).
103 Aarhus Directive, Article 5.2 (b).
Finally, the directive instructs Member States to support the public in seeking and requesting environmental information. The directive, in essence, requires Member States to inform the public on its rights to request environmental information and to help it locate particular environmental information. This last aspect includes, for example, making available registers or lists of the environmental information held by public authorities.

### 4.1.3. Active and systematic dissemination of environmental information

The Aarhus directive also provides an obligation for public authorities to disseminate their environmental information on their own initiative. First of all, the directive specifies to which environmental information this dissemination obligation applies. On the one hand, the directive specifies a list of the minimum of information to be actively disseminated and stipulates an obligation to make periodic reports. On the other hand, the directive clarifies that there is no obligation to actively disseminate environmental information in relation to which a public authority could call upon a valid reason to refuse access upon request.

Secondly, the directive specifies the way in which the required environmental information is to be made available to meet its active dissemination obligation. In this regard, the directive requires the information to be made available in an appropriately updated version and preferably by means of computer telecommunication or electronic technology. It also requires Member States to ensure that environmental information progressively becomes available in electronic databases that are easily accessible to the public through public telecommunication networks. However, the directive also stipulates that Member States can meet its dissemination obligation by creating links to Internet sites where the required information can be found.

Finally, the directive stipulates that in the event of an imminent threat to human health or the environment, whether caused by human activities or due to natural causes, a broad dissemination obligation applies. In case of such an event, the directive requires an immediate dissemination of all information held by or for public authorities which could enable the potentially affected public to take measures against this threat. In formulating this broad dissemination obligation, the directive does not make an exception for environmental information in relation to which a public authority could refuse access upon request on the grounds of a valid reason. It does however stipulate that this broad dissemination obligation in the event of imminent threats to human health or the environment is without prejudice to any specific obligation laid down by Community (i.e. meaning the EU) legislation.

### 4.2. Public Sector Information Directive

---

105 Aarhus Directive, Article 3.5.
108 Aarhus Directive, Article 7.5.
110 Aarhus Directive, Article 7.1.
111 Aarhus Directive, Article 7.6.
112 Aarhus Directive, Article 7.4.
114 Aarhus Directive, Article 7.4.
The PSI Directive (i.e. Public Sector Information Directive) as amended in 2013, requires Member States to ensure that documents held by public authorities are made available for re-use for commercial or non-commercial purposes. According to this directive a term “re-use” refers to the use which persons or legal entities make of such documents for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced. The directive also explicitly states that exchange of documents between public sector bodies, purely in pursuit of their public tasks does not constitute re-use.

The directive’s definition of re-use immediately indicates that the following does not qualify as such re-use: use for the initial purpose within the public task for which the document was created, and the exchange of documents between public sector bodies purely for public task purposes. In addition, literature defends that the notion of re-use should be taken not to extend to the further use of documents within the public sector body in which they were created, for purposes different than the original one, but still for the performance of the public task.

According to the directive’s definition there is re-use, however, in case of use by private persons and in case of use by sector bodies outside of their public tasks. So, if documents are made available to other public sector bodies but for activities different than the performance of their public task, this qualifies as such re-use. It also constitutes re-use when a public sector body is using its own documents for purposes other than its public task, for example for creating commercial or value added products on the market.

4.2.1. Scope of application

As a general rule, the PSI Directive stipulates that its provisions on re-use, apply to existing documents that are held by public sector bodies of the Member States. In addition to the notion of re-use, the notion of document and the notion of public sector body are key to delimiting the scope of application of the PSI Directive. Within the scope of the directive, both the notion of documents as well as the notion of public sector bodies are interpreted in a broad way. A document refers to any content or part of it, whatever it’s medium. This includes, for example, data written on paper, data stored in electronic form and data incorporated in sound, visual or audio-visual recordings. A public sector body refers to the State, regional and local authorities and different sorts of bodies governed by public law.

However, the PSI Directive also explicitly excludes certain types of documents from its scope of application. Among the list of excluded types of documents, the directive mentions: documents supplied outside the scope of a body’s public task; documents over which a third party holds intellectual property rights; documents to which the access regimes in the Member States apply access limitations on the grounds of protecting national or public security, statistical or commercial confidentiality and personal data, or on the ground of access being dependent on proving a particular interest; documents held by public service broadcasters and documents held by

116 PSI Directive, Article 2.4.
117 PSI Directive, Article 2.4.
119 PSI Directive, Article 3.1.
120 PSI Directive, Article 2.3.
121 PSI Directive, Article 2.1.
educational, research and cultural establishment. This list shows that the PSI Directive builds on the existing access regimes in the Member States and does not change the national rules for access to documents. The amended directive emphasises that documents to which access is restricted by virtue in the Member States are not subject to the directive.

4.2.2. Rules on re-use

The PSI Directive formulates rules which public sector bodies have to adhere while deciding upon an applicant’s request to re-use their documents. Again, these rules touch upon different aspects of a submitted request.

First of all, the directive determines the elements on which a public sector body can base its grant or refusal of the request to re-use documents. In general, if a public sector body holds a document that is not explicitly excluded from the scope of application of the PSI Directive, this public body has to allow the re-use of this document in accordance with the rules set out by this Directive. The general rule is that if a public sector body finds its document to come within the scope of application of the PSI Directive this body is compelled to grant requests to re-use it. The exception to this rule is the case in which libraries, including university libraries, museums and archives hold intellectual property rights in relation to documents not explicitly excluded from the scope of application of the PSI Directive. With regard to this particular case, the directive does not make re-use mandatory, but it does stipulate that if re-use is indeed allowed the allowed re-use of this documents is then to comply with the provisions of the PSI Directive.

Secondly, the PSI Directive also ensures that a public sector body that decides to allow the re-use of a document, has to observe certain minimum rules when it comes to determining the conditions under which this re-use is possible. These minimum rules touch upon different aspects.

A first aspect covered by these rules is the format in which public sector bodies are to make their documents available when allowing their re-use. The directive requires these bodies to make these documents available in any pre-existing format or language and, where possible and appropriate, in open and machine-readable format together with their metadata.

A second aspect relates to the charges that sector bodies make for the re-use of documents. The directive requires public sector bodies to be transparent about these charges. The directive, in principle, does not allow these charges to exceed the marginal costs incurred for their reproduction, provision and dissemination.

A third aspect concerns imposing conditions on the allowed re-use of documents. The directive permits public sector bodies to impose such conditions, where appropriate by means of a licence. However, the directive also stipulates that such conditions may not unnecessarily restrict possibilities for re-use and may not be used to restrict competition. In relation to licences, the directive

---

122 PSI Directive, Article 1.2.
124 PSI Directive, Article 1 (iii) ca.
125 PSI Directive, Article 3.1.
126 PSI Directive, Article 3.2.
127 Directive, Article 5.
129 PSI Directive, Article 8.1.
encourages to make standard licences available that can be adapted to meet particular licence applications and that can be processed electronically.\footnote{PSI Directive, Article 8.2.}

Two final aspects relate to non-discrimination and the prohibition of exclusive agreements. According to the directive, any applicable conditions for the re-use of documents shall be non-discriminatory for comparable categories of re-use.\footnote{PSI Directive, Article 10.} The directive’s prohibition of exclusive agreements holds that the re-use of documents shall, in principle, be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents.\footnote{PSI Directive, Article 11.}

Thirdly, the directive compels Member States to make practical arrangements that facilitate the search for documents available for re-use. As examples of such practical arrangements the directive mentions online and machine-readable asset lists of documents combined with relevant metadata and portal sites that are linked to the asset lists.\footnote{PSI Directive, Article 9.}

Finally, the PSI Directive also gives public sector bodies instructions on how to handle an applicant’s request to re-use a document.\footnote{PSI Directive, Article 4.} In this regard, the directive, most importantly, sets a timeframe for a public body to process the request and to make the document available or finalise a license offer, in case it decides to allow the requested re-use. This timeframe is set consistent with the timeframe used in national access regimes, if the document concerned is covered by such an access regime.\footnote{PSI Directive, Article 4.1 \.; K. Janssen, The availability of spatial and environmental data in the European Union: at the crossroads between public and economic interests (Alphen aan den Rijn Kluwer Law International 2010) 143.} This timeframe is in principle, set at a maximum of 20 working days, if the document concerned is not covered by a national access regime.\footnote{PSI Directive, Article 4.2.} The directive also imposes requirements on the public sector body, in case it decides to refuse the requested re-use. In that case the public sector body should communicate the grounds for refusal to the applicant.\footnote{PSI Directive, Article 4.3.} If the refusal is based on a third party holding intellectual property rights, the public sector body should normally also include a reference to the right holder or licensor from which it has obtained the relevant material.\footnote{PSI Directive, Article 4.3.} In addition, any decision on re-use shall contain a reference to the means of redress in case the applicant wishes to appeal the decision.\footnote{PSI Directive, Article 4.4.}

### 4.3. Inspire Directive

The Inspire Directive lays down rules to establish the Infrastructure for Spatial Information in the European Community (hereinafter “Inspire”).\footnote{Inspire Directive, Article 1.1.} The Inspire Directive covers Community policies and activities relating to the environment. There are three objectives that the Inspire Directive seeks to achieve in this domain by establishing the Inspire infrastructure for spatial information. The first and most important objective is to make it facilitate access, sharing and use of spatial data sets and services for public authorities while performing their public tasks regarding the environment.\footnote{Inspire Directive, Article 17.} In this regard the Inspire Directive uses the same broad notion of a public authority as the Aarhus
Directive does. A second, minor objective is to create an opportunity for third parties to link their spatial data and services to the Inspire infrastructure. Such a third party refers to any natural or legal person, other than a public authority. A third objective is to give citizens appropriate, public access to the spatial data sets and services that public authorities and third parties make available within this Inspire infrastructure. The Inspire Directive explicitly stipulates that its provisions are without prejudice to the Aarhus Directive and without prejudice to the PSI Directive.

4.3.1. Scope of application

The rules that the Inspire Directive introduces on spatial data sets and services, only apply if the actual spatial data set involved fulfils specific conditions. The first condition is that the spatial data set has to relate to an area or location where a Member State has jurisdiction rights. The second condition is that regarding this area or location, this data set must touch upon one of the 34 spatial data themes explicitly listed in the annexes to this directive. These themes listed include, for example: geographical grid systems, elevation, soil, human health and safety, population distribution, Utility and governmental services, etc. The third condition is that the data set has to be in an electronic format. The fourth condition is that the data set has to be held by, or on behalf of: 1) either a public authority acting within the scope of its public tasks, or 2) a third party who fulfils the requirements to link to the network of services specified by the directive. The fifth condition is that the data set has to constitute the reference version. This means that, in cases where multiple identical copies of the same spatial data set are held by or on behalf of various public authorities, the directive applies only to this reference version from which the various copies are derived. The sixth condition relates specifically to the case in which the data set is held by or on behalf of a public authority operating at the lowest level of government within a Member State. In such a case the directive only applies, if the Member State has laws or regulations requiring this public authority to collect or disseminate such a data set. Noteworthy, the Inspire Directive does not require collection of new spatial data.

4.3.2. The Infrastructure for Spatial Information in the European Community

To reach its objectives relating to the access, exchange and use of spatial data sets and services, the Inspire Directive creates the Infrastructure for Spatial Information in the European Community. Its approach to creating this Community infrastructure is to determine specifications that are to be met by the infrastructures for spatial information operated by the Member States. The directive determines these specifications through a combination of certain general rules laying down a framework and timetable to decide on more detailed, common Implementing Rules. These common
Implementing Rules are adopted by the European Commission, assisted by a committee of representatives of the Member States (i.e. “Comitology Procedure”). The roadmap for the full implementation of the Inspire Infrastructure currently stretches to 2020.¹⁵⁵

In giving the specifications of the Infrastructure for Spatial Information in the European Community, the Inspire Directive and the Implementing Rules cover five areas. The first area concerns the metadata to be used to describe the spatial data sets and services to which the Inspire Directive applies.¹⁵⁶ The second area relates to the technical arrangements for the interoperability of these spatial data sets and services.¹⁵⁷ A third area concerns the network of services which Member States are to establish and operate for the spatial data sets covered by the directive.¹⁵⁸ More in particular, the Inspire Directive leads to specifications on creating:

- Discovery services that make it possible to search for spatial data sets and services by means of the metadata describing them;
- View services that make it possible, in essence, to visualise spatial data sets, legend information and any relevant content of metadata;
- Download services that make it possible to download copies of spatial data sets and to access the downloaded copies directly;
- Transformation services enabling spatial data sets to be transformed with a view to achieving interoperability; and
- Services allowing spatial data services to be invoked.

A fourth area covered by the specifications of the Inspire Directive and the Implementing Rules, relates to agreements on accessing and sharing the spatial data sets and services to which the Inspire Directive applies.¹⁵⁹ A fifth area concerns coordination, monitoring and reporting obligations of the Member States in relation to the implementation of their infrastructures for spatial information.¹⁶⁰

Finally, the Infrastructure for Spatial Information in the European Community, established by the Inspire Directive, also has the Commission operate an Inspire geo-portal.¹⁶¹ This Internet portal, which is operated at the Community level, provides access to the services that EU Member States operate for the spatial data sets under this directive.¹⁶²

### 4.3.3. Public authorities within Inspire

The Inspire Directive, first of all, lays down rules that affect public authorities. In formulating these rules, this directive, as mentioned, uses the same broad notion of a public authority as the Aarhus Directive does. The Inspire Directive also uses the notion public authority as referring to: 1) a government or other public administration; 2) a natural or legal person who performs public administrative functions under national law; or 3) a natural or legal person who, under control of one

---

¹⁵⁶ Inspire Directive, Article 5.
¹⁵⁸ Inspire Directive, Article 11.
¹⁵⁹ Inspire Directive, Article 17.
¹⁶¹ Inspire Directive, Article 15.
of the previous bodies or persons qualifying as a public authority, has public responsibilities or functions relating to the environment or provides public services relating to the environment.\textsuperscript{163}

4.3.4. Making available and sharing of spatial data sets

First of all, the provisions of the Inspire Directive result in an obligation for public authorities of the Member States to make spatial data sets and services available. This obligation more in particular holds that if all relevant conditions are fulfilled a public authority is compelled to make available its spatial data sets and services in a particular way.\textsuperscript{164}

In essence, the directive results in compelling a public authority to make spatial data sets and services available if the spatial data sets and services held by or for this public authority are covered by the directive.\textsuperscript{165} This means that a public authority only faces this obligation if the spatial data sets and services concerned indeed fulfil all of the abovementioned conditions for the Inspire Directive to apply. Provided this, a public authority is not obliged to make its spatial data sets and services available, solely because these data sets and services involve electronic data sets that, in relation to an area or location within a Member State, touch upon a spatial data theme listed by the Inspire Directive.\textsuperscript{166} Facing this obligation also requires two additional conditions to be fulfilled. Firstly, this public authority has to manage the reference version of these spatial data sets and do so within the scope of its public task.\textsuperscript{167} Secondly, in case this public authority operates at the lowest level of government within a Member State, the laws or regulations of the Member State have to require it to collect or disseminate these data sets.\textsuperscript{168}

With regard to the appropriate method for public authorities to meet their obligation on making spatial data sets and services available, the directive results in requirements that reflect its goal of establishing an Infrastructure for Spatial Information in the European Community. The directive more in particular results in compelling the public authorities concerned to make the required data sets and services available, in accordance with the directive’s specifications on metadata, interoperability and network services within this infrastructure.\textsuperscript{169} The directive also explicitly stipulates that Member States have to ensure that any information needed to comply with these specifications is made available to public authorities.\textsuperscript{170}

The Inspire Directive also results in ensuring certain public authorities a possibility to share each other’s spatial data sets and services, for the purposes of public tasks that may have an impact on the environment.\textsuperscript{171} This directive does so by requiring measures that enable these public authorities to gain access to spatial data sets and services, and to exchange and use those sets and services, for those purposes.\textsuperscript{172}

A specific group of public authorities may be subjected to the requirements of the Inspire Directive on sharing spatial data sets and services in view of their public tasks (e.g. environmental agencies). The directive only requires to enable such sharing between the public authorities of a Member state.

\textsuperscript{163} Inspire Directive, Article 3.9.
\textsuperscript{164} Inspire Directive, Article 7.3.
\textsuperscript{165} Inspire Directive, Article 4.
\textsuperscript{166} Inspire Directive, Article 4.
\textsuperscript{167} Inspire Directive, Article 4.2
\textsuperscript{168} Inspire Directive, Article 4.6.
\textsuperscript{169} Inspire Directive, Article 7.3.
\textsuperscript{170} Inspire Directive, Article 10.1.
\textsuperscript{171} Inspire Directive, Article 17.
\textsuperscript{172} Inspire Directive, Article 17.1.
that qualify either, as the government or other public administration, or as a natural or legal person performing public administrative functions under national law.\textsuperscript{173}

In addition, the Inspire Directive does not result in an absolute obligation for the affected public authorities to share relevant spatial data sets and services, for environment related public tasks, nor to do so for free and without imposing conditions. In principle, the directive requires that, at the point of use, there are no practical obstacles to prevent the affected public authorities from sharing the relevant spatial data sets and services.\textsuperscript{174} However, with regard to most cases, the directive’s requirements on enabling sharing do not prohibit public authorities from making the supply of data sets and services dependent upon payment or accepting licences.\textsuperscript{175} As a general rule, the directive merely requires that such charges and licenses be kept to the minimum required to ensure quality and supply, a reasonable return on investment, and possible self-financing requirements of public authorities.\textsuperscript{176} In addition, the directive does not require any sharing of spatial data sets and services, if such sharing compromises the course of justice, public security, national defence or international relations.\textsuperscript{177}

4.3.5. The concept of ‘third parties’

The Inspire Directive also affects third parties. This notion of third parties refers to natural or legal persons who do not qualify as a public authority.\textsuperscript{178}

The directive ensures that, upon their request, third parties are given the technical possibility to link their spatial data sets and services to the network services within the Infrastructure for Spatial Information in the European Community, provided that their data sets and services meet the specifications of this Infrastructure.\textsuperscript{179} More in particular, the directive only ensures this possibility to third parties whose spatial data sets and services comply with the relevant specifications in relation to metadata, network services and interoperability. In this regard, the directive explicitly stipulates that Member States are to provide third parties any information needed to comply with these specifications.\textsuperscript{180}

The consequence of a third party linking their spatial data sets and services to the Inspire network services, is that they become available both to the public at large and public authorities. Public access to these spatial data sets and services comes with a limited opportunity for the third party to make this access dependent on payment or accepting a licence.\textsuperscript{181} The limits to this opportunity are discussed in the following part that deals specifically with public access. With regard to public authorities, the directive stipulates that, if the third party holds intellectual property rights to the data sets, the public authority may only access, exchange or use these data sets, with the consent of

\textsuperscript{173} Inspire Directive, Article 17.1.


\textsuperscript{175} Inspire Directive, Article 17.3 stipulates an exception relating to Community institutions and bodies.

\textsuperscript{176} See: Inspire Directive, Article 17.

\textsuperscript{177} Inspire Directive, Article 17.7.

\textsuperscript{178} Inspire Directive, Article 2.10.

\textsuperscript{179} Inspire Directive, Article 12.

\textsuperscript{180} Inspire Directive, Article 10.

\textsuperscript{181} Inspire Directive, Article 14.
that third party. Noteworthy, in the Inspire Directive, the abovementioned rules on sharing spatial data sets and services apply only to certain public authorities and not to third parties.

4.3.6. Enabling public access

Finally, the Inspire Directive also affects the public at large, by ensuring public access to the spatial data sets and services that public authorities and third parties make available within the Inspire infrastructure. The directive in particular requires that the public have access to these spatial data sets and services through the network services within the Inspire Infrastructure.

The Inspire Directive laid down a principle according to which the network services within the Inspire Infrastructure should be available to the public, in a user friendly way, via the Internet or any other appropriate means of telecommunication. As these services have to be made available for all the spatial data sets to which the directive applies, public access to the services automatically entails public access to these data sets.

In derogation of this principle of public access, however, the Inspire Directive enumerates the valid reasons to restrict public access to those spatial data sets and services to which its rules apply. A first list of such reasons applies specifically to discovery services. In this list, the directive stipulates that public access to spatial data sets and services through discovery services may be limited, if granting such access would adversely affect international relations, public security or national defence. A second list of reasons applies to all other network services. In this second list the directive states that public access to spatial data sets and services through these services may be limited, in essence, if such access would adversely affect any of the following: 1) the confidentiality of the proceedings of public authorities; 2) international relations, public security or national defence; 3) the course of justice; 4) the confidentiality of commercial or industrial information; 5) intellectual property rights; 6) the confidentiality of personal data 7) the interests or protection of a person voluntarily supplying information; and 8) the protection of the environment. The Inspire Directive stipulates that the valid reasons to refuse a request for access, are all to be interpreted in a restrictive way, taking into account the relevant interests. The directive specifically requires that, in every case, the public interest served by disclosure be weighed against the interest served by limiting or conditioning the access. In its provisions on the valid reasons to refuse public access to spatial data and services, the Inspire Directive deliberately mirrors the provisions of the Aarhus Directive on refusing requests for access to environmental information.

In addition, the Inspire Directive also stipulates rules on making the public access to spatial data and services through the Inspire network services dependent upon payment or upon accepting a licence agreement. The directive stipulates that all discovery services have to be provided to the public free of charge. With regard to view service, the directive, in principle, requires them to be offered for

---

182 Inspire Directive, Article 4.5.
183 Inspire Directive, Article 17.
free, but allows public authorities supplying such a service to apply charges in view of securing the maintenance of spatial data sets and corresponding data services. 192 Relating to the other services within the Inspire network, the directive does not limit the possibility to make public access dependent on payment. On the topic of licences, the directive stipulates that, with exception of discovery services, it is allowed to make public access to the Inspire network services dependent on accepting a licence. 193 Finally, the directive explicitly states that view services may make data available in a form that prevents their re-use for commercial purposes. 194

4.3.7. Impact on exchanging and using data in the context of disaster relief

It can be concluded that Aarhus, PSI and Inspire Directives aim at enhancing the availability of particular public sector data, which in turn could benefit first responders. A first, obvious benefit is that first responders can enjoy the rights to access to certain information held by public sector. This is beneficial given that “environmental information”; “spatial data” and “documents” held by the public sector can be very valuable when it comes to providing response to various emergencies in the most efficient and effective way. A second benefit is that the Aarhus, PSI and Inspire Directives provide first responders with more clarity about the conditions under which they are allowed to access, exchange or use the public sector data covered by these directives. A third benefit relates specifically to the Inspire Directive resulting in mandatory technical specifications for data sets and services included within the Inspire Infrastructure. These known technical specifications make it possible to ensure that, across the EU Member States, first responders are capable of accessing, exchanging and using the spatial data sets and services included in the Inspire Infrastructure with a minimum of technical difficulties.

A two-step analysis should be performed to establish whether a first respondent’s intended action concerning public sector data (e.g. accessing, exchanging or using the public sector data) is governed by the rules resulting from the Aarhus Directive, PSI Directive or Inspire Directive. The first step should analysing the nature of the data to which the intended action of the first respondent relates. In this step it is important to assess whether this data qualifies as a “document” covered by the PSI Directive, as “environmental information” covered by the Aarhus Directive or as an electronic “spatial data set” covered by the Inspire Directive. The second step is to analyse the intended action of the first respondent concerning the data. This step in particular is about analysing whether this action constitutes “accessing”, “sharing” or “re-use” as defined by the relevant directives and whether the first responder is going to perform this action as a private person or, on the contrary, as a public authority or a public sector body as defined by the relevant directives. Performing this two-step analysis, as said, will clarify whether the rules resulting from the Aarhus Directive, PSI Directive or Inspire Directive govern the intended action of the first respondent concerning public sector data held by a public body. This two-step analysis will especially clarify which of these rules governs the opportunity for the public body to refuse its permission for the intended action, and to make granting this permission dependent upon conditions such as payment or accepting a licence agreement.

Finally, two observations are important to assess the true relevance for first responders of the rules resulting from the Aarhus Directive, PSI Directive and Inspire Directive. These observations both

194 Inspire Directive, Article 14.3.
relate to the opportunity, in practice, for first responders reacting to an emergency to access, exchange and use the public sector data covered by these directives.

A first observation is that in promoting the availability of particular public sector data the Aarhus Directive, PSI Directive and Inspire Directive do not push aside intellectual property rights nor the legal framework protecting the processing of personal data. This has clear consequences in case intellectual property rights and data protection frameworks apply to public sector data covered by these directives. In such a case the opportunity for first responders to access, exchange or use this public sector data will also be governed by the rules on intellectual property rights and protection of personal data.

A second observation relates to the timeframe in which the Aarhus Directive, PSI Directive and Inspire Directive allows public bodies to decide whether to make public sector data available. Depending on the circumstances, these time frames can exceed the time frame in which the public sector data can really contribute to emergency relief. Again, this time issue arises, in particular, if the need for certain data becomes apparent only in light of the actual emergency and could not be remedied by collecting the data in advance. However, the timeframes outlined by the Aarhus Directive, the PSI Directive and the Inspire Directive do not have to be an insurmountable obstacle to the practical relevance of their rules in emergency situations. First of all, these directives do not forbid national rules requiring that in case of emergencies public bodies are to decide immediately on making data available or are to do so within a much shorter time frame. Secondly, in case the availability of data is dependent upon concluding a licence, this data can be made available much faster by introducing a quick possibility to conclude pre-existing licences that apply specifically to emergency situations. Another possible measure is to introduce a principle that if there is really no time to conclude a licence in an emergency the data is simply made available immediately and potential licencing issues are solved afterwards.195

5. Relevance of Intellectual Property Rights

In the context of the Common Information Space it is also important to take into consideration intellectual property rights, such as copyright and the database *sui generis* right. While providing an efficient response to emergencies, first responders may exchange and use of incorporations of data that are covered by intellectual property rights. For example, text files, photos, maps, renditions of weather reports and extracts from databases all are very likely to be covered by intellectual property rights.

An intellectual property right grants a right holder an exclusive right over a particular result of human efforts that can be embodied in more than one perceptible thing at the same time. Copyright, for example, will grant a map maker (i.e. a right holder) an exclusive right over their intellectual creation, their ‘work’, that relates to developing symbols that allow maps to express a distinction between various types of industrial sites. Different intellectual property rights grant exclusive rights over different types of results of efforts that can all be embodied in more than one perceptible thing at the same time. For example, copyright grants exclusive rights over such results of efforts that qualify as a ‘work’. Patent law, on the other hand, only does so in relation to such results of efforts that constitute an ‘invention’.

The consequence of an intellectual property right granting a right holder an exclusive right over a result of efforts (e.g. over the devised wording of a report) is that the right holder, in principle, has the exclusive power to perform certain categories of acts concerning embodiments of this result of efforts (e.g. to ‘communicate’ copies of the report ‘to the public’). A person other than the right holder has only limited options to perform these categories of acts concerning these embodiments in a legal, non-infringing way. A first option is that this person obtains the permission from the right holder, a licence, to perform these categories of acts that are subject to the authorisation of the right holder. A second option is that this person has the right holder transfer him all or part of the exclusive right granted by the intellectual property right. A third option is that this person can enjoy an exception which the intellectual property right explicitly stipulates in relation to these categories of acts that are subject to the authorisation of the right holder. Such exceptions describe specific circumstances in which performing these categories of acts in a legal way does not require the permission of the right holder.

In the scenario of first responders exchanging and using data to provide emergency relief, it is typically relevant to analyse the legality of these actions in light of ordinary copyright, database copyright and the database *sui generis* right. In view of performing such an analysis the following gives an overview of the rules governing these intellectual property rights.

---

196 Such a licence does not make this person the new right holder of the exclusive right granted by the intellectual property right. The licence merely entails that the right holder gives this person a permission to perform a category of acts that is subject to the authorisation of the right holder.

197 To the extent that this exclusive right was transferred this person becomes the new right holder of the exclusive right granted by the intellectual property right.

198 This statement is based on the assumption of a scenario in which first responders, for the purpose of reacting to an emergency, exchange and use incorporations of data which as such do not constitute a computer program and which, at the most, are meant to be processed by a computer program that operates a computer. In this scenario it is indeed most relevant to analyse the legality of these actions of the first responders in light of ordinary copyright, database copyright and the database *sui generis* right. In this scenario it is in fact unlikely that their exchange and use of the incorporations of data infringes other intellectual property rights such as computer program copyright, patent law or trade mark law. Absolute certainty, however, whether an act of a first responder infringes any intellectual property right requires taking into account the rules laid down by ordinary copyright, database copyright, computer program copyright,
Table 2: Summary of relevant intellectual property rights

<table>
<thead>
<tr>
<th>Exclusive right</th>
<th>Ordinary copyright</th>
<th>Database copyright</th>
<th>Database sui generis right</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object</td>
<td>A ‘work’</td>
<td>A ‘work’ relating to the selection or arrangement of the elements of a ‘database’</td>
<td>The substantial investment in obtaining, verifying or presenting the content of a ‘database’</td>
</tr>
<tr>
<td></td>
<td>(i.e. a person’s own intellectual creation that relates to expressing an idea in perceptible features that are not dictated by their function)</td>
<td>(i.e. a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means)</td>
<td>(i.e. a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means)</td>
</tr>
<tr>
<td>Restricted acts</td>
<td>The acts of</td>
<td>The acts of</td>
<td>The acts of</td>
</tr>
<tr>
<td>(i.e. acts subject to authorisation of the right holder)</td>
<td>- ‘reproducing’,</td>
<td>- ‘reproducing’,</td>
<td>- ‘extracting’ and</td>
</tr>
<tr>
<td></td>
<td>- ‘communicating to</td>
<td>- ‘communicating to</td>
<td>- ‘re-utilising’</td>
</tr>
<tr>
<td></td>
<td>the public’,</td>
<td>the public’,</td>
<td>in relation to the whole or substantial parts of the content of the ‘database’</td>
</tr>
<tr>
<td></td>
<td>- ‘distributing’,</td>
<td>- ‘distributing’,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ‘lending’ and</td>
<td>- ‘communicating to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- ‘renting’</td>
<td>the public’,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>in relation to</td>
<td>- ‘lending’ and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>embodiments of</td>
<td>- ‘renting’</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the ‘work’</td>
<td>in relation to the</td>
<td></td>
</tr>
<tr>
<td>Relevant</td>
<td>- Temporary technical reproductions</td>
<td>- Access and normal use (only for the lawful user)</td>
<td>- Use of insubstantial parts</td>
</tr>
<tr>
<td>exceptions</td>
<td></td>
<td></td>
<td>- Public security</td>
</tr>
<tr>
<td>(i.e. acts are not subject to the authorisation of the right holder)</td>
<td>- Public security (differences across EU Member states)</td>
<td>- Public security</td>
<td></td>
</tr>
</tbody>
</table>

5.1. Ordinary copyright

Ordinary copyright grants the right holder an exclusive right over a ‘work’. Such a ‘work’ is generally taken to refer to a person’s own intellectual creation that relates to expressing an idea in perceptible features that are not dictated by their function.© Copyright initially grants this exclusive right to the author of the ‘work’ that is to the person who actually made the effort of thinking up the intellectual
creation. However, this exclusive right can be transferred to a new right holder or licensed to a licensee.\textsuperscript{200}

The exclusive right which copyright grants the right holder in relation to a ‘work’ results in giving the right holder an exclusive power to control certain categories of acts concerning embodiments of the ‘work’. The duration of this exclusive right is limited to the lifetime of the author of the ‘work’ plus an additional 70 years.\textsuperscript{201}

5.1.1. Requirements for the grant of an exclusive right

In order to grant an exclusive right copyright requires that an embodiment of a person’s efforts (e.g. a symbol on the map which he made) demonstrate that these efforts resulted in a ‘work’ (e.g. in devising that the features of this symbol are apt to express a particular meaning). As mentioned, such a ‘work’ is generally taken to refer to a person’s own intellectual creation that relates to expressing an idea in perceptible features that are not dictated by their function. In this regard, a very modest intellectual creation can already qualify as such a ‘work’.\textsuperscript{202} However, a person’s creation will not qualify as a ‘work’ to the extent that it is directed at developing perceptible features that are solely dictated by their function\textsuperscript{203}. For example, the features of a bathymetric chart that are dictated by giving an accurate description of a submerged terrain cannot be taken to result from a ‘work’.

5.1.2. Embodiments of the ‘work’

The exclusive right granted by copyright results in an exclusive power of the right holder over embodiments of the ‘work’. To be considered such an embodiment of the ‘work’, a perceptible item has to meet two requirements. The first requirement is that the perceptible item has to display substantial similarities to those specific features of the author’s initial embodiment of the ‘work’ that demonstrate his creation of the ‘work’. The second requirement is that the perceptible item has to display these substantial similarities as a result of copying an embodiment of the ‘work’ and not as a result of an independent creation made without knowledge of the existence of an embodiment of the ‘work’.\textsuperscript{204} From these requirements it follows, for example, that it is not possible to substantiate that two maps of the same area are embodying the same ‘work’ merely on the basis of their similarities, which are dictated by giving an accurate description of the area.

5.1.3. Categories of acts subject to the authorisation of the right holder

Copyright results in giving a right holder an exclusive power over performing the following categories of acts in relation to embodiments of his ‘work’: ‘reproducing’, ‘communicating to the public’, ‘distributing’, ‘lending’ and ‘renting’.

\textsuperscript{200} See: Information Society Directive, Recital 30.
\textsuperscript{204} See: A. Strowel, "La contrefaçon et droit d’auteur: conditions et preuve ou pas de contrefaçon sans ‘plagiat’" (Auteurs & Media 2006) 268.
In copyright ‘reproducing’ refers to any direct or indirect, temporary or permanent reproduction, in whole or in part and by any means and in any form. This broad notion of ‘reproducing’, in principle, also covers the often short-lived duplications that computers need to make in order to technically allow them to perform a task. Examples of such duplications are the ones that a computer makes in its working memory and screen buffer when asked to display a video file stored on its hard disk. In addition, ‘reproducing’ is usually taken to cover ‘adapting’ and ‘translating’.

The notion of ‘communicating to the public’ in the context of copyright covers any communication, by any means, directed at people who are not connected by family or quasi-family ties. This notion also covers making available to the public in such a way that members of the public get access from a place and at a time individually chosen by them. Making embodiments of a ‘work’ available to the public via the Internet therefore also qualifies as ‘communicating to the public’.

In copyright ‘distributing’ refers to any form of distribution to the public by sale or otherwise of copies of the ‘work’. Note however, that if an embodiment of a ‘work’ is sold for the first time in an EU Member State with the consent of the right holder this fact entails the following: the right holder has exhausted their possibility to call upon copyright to control ‘distributing’ that particular embodiment within the EU Member States.

Copyright also makes ‘renting’ and ‘lending’ subject to the authorisation of the right holder. ‘Renting’ covers making available for use, for a limited period of time and for direct or indirect economic or commercial advantage. ‘Lending’ refers to making available for use, for a limited period of time and not for direct or indirect economic or commercial advantage, when it is made through establishments which are accessible to the public.

5.1.4. Relevant exceptions to the categories of restricted acts

Finally, it is necessary to take into account that copyright also stipulates several exceptions in relation to the categories of acts subject to the authorisation of the right holder. Discussing all of these exceptions is beyond the scope of this deliverable. Many of these exceptions have a very specific scope of application (e.g. the exception relating to religious celebrations) that makes them of little relevance to a first responder acting in the context of an emergency. However, this does not apply to all these exceptions.

The first exception of relevance in the context of emergency relief is the mandatory exception that the Information Society Directive stipulates in relation to temporary technical reproductions. This exception states that, under certain circumstances, the right holder cannot prohibit temporary acts of reproduction that constitute an integral and essential part of a technological process that is being applied with the sole purpose of either enabling the transmission in a network between third parties by an intermediary, or enabling a lawful use of a protected ‘work’. According to this exception this is the case if these temporary acts of reproduction are transient or incidental and have no independent

---

206 Information Society Directive, Article 3.
211 Information Society Directive, Article 5.3 (g).
economic significance. The exact scope of this exception has given rise to debate. However, it is clear that this exception can be relevant for first responders who perform acts in relation to a digital embodiment of a ‘work’ that technically require temporary reproductions of this embodiment in a computer (e.g. the temporary reproductions made in the working memory of a computer while browsing the Internet). To the extent that this exception for temporary technical reproductions applies, these first responders can perform those acts legally, even without permission of the right holder.

The second exception that can be relevant in the context of emergency relief relates to public security. The Information Society Directive has made it optional for EU Member States to introduce an exception that limits the opportunity of a right holder to forbid reproductions or communications to the public made for the purpose of public security. Some Member States have made use of this option. In these states the notion of ‘public security’ is sometimes taken to also cover for example the health of citizens. Note however, that even in the Member States that have introduced such an exception relating to ‘public security’ it remains important to take into account the exact wording and scope of this exception.

5.2. Intellectual property rights relating to databases

Database copyright and the database sui generis right grant exclusive rights over certain results of efforts that relate to ‘databases’. Both database copyright and the database sui generis right take a ‘database’ to refer to a collection of independent works, data or other materials that are arranged in a systematic or methodical way and that are individually accessible by electronic or other means. The database copyright focuses on the intellectual creation involved in the selection or arrangement of the elements of the ‘database’. The database sui generis right concentrates on the substantial investment that went into obtaining, verifying or presenting the elements of the ‘database’.

5.2.1. Database copyright

Database copyright grants a right holder an exclusive right over an intellectual creation, a ‘work’ that relates to devising the selection or arrangement of the elements of a ‘database’. The exclusive right which database copyright grants the right holder over this intellectual creation results in giving the right holder an exclusive power to control certain categories of acts concerning embodiments of this intellectual creation. The database copyright initially grants this exclusive right to the author of this ‘work’, which is to the person who actually made the intellectual creation relating to such a selection or arrangement. However, again, this exclusive right can be transferred to a new right.

---

212 Information Society Directive, Article 5.1.
213 See: S. Clark, “Just browsing? An analysis of the reasoning underlying the Court of Appeal’s decision on the temporary copies exemption in Newspaper Licensing Agency Ltd v Meltwater Holding BV” (E.I.P.R. 2011) 727.
215 Information Society Directive, Article 5.3 (e).
216 See: §45, 2) German Copyright Law and art. 22 Dutch Copyright Law. Contrary Belgian Copyright Law does not contain such an exception.
218 See: §45, 2 German Copyright Law.
220 Database Directive, Article 3.
221 Database Directive, Article 7.
222 Database Directive, Article 3.
holder or licensed to a licensee. As in ordinary copyright the duration of this exclusive right is limited to the lifetime of the author plus an additional 70 years.

5.2.1.1. Requirements for the grant of an exclusive right

In order to grant an exclusive right, database copyright requires that the selection or arrangement of the elements of a ‘database’ demonstrates to result from a ‘work’, a person’s own intellectual creation.\(^{223}\) In this connection, the database copyright does not require the selection or arrangement to demonstrate a high level of intellectual creation. However, a person’s efforts will not qualify as the required intellectual creation if they result in a selection or arrangement that is dictated by its function (e.g. achieving exhaustiveness) or that is based on commonplace criteria (e.g. arranging elements alphabetically).\(^{224}\) Finally, as is the case for ordinary copyright, obtaining database copyright protection does not require any formalities or registration.

5.2.1.2. Embodiments of the intellectual creation relating to the structure of a database

The exclusive right granted by database copyright results in an exclusive power of the right holder over embodiments of the intellectual creation, the ‘work’, related to selecting or arranging the elements of a ‘database’. To be considered such an embodiment of this intellectual creation a perceptible item has to meet two requirements. The first requirement is that the perceptible item has to display substantial similarities to those features of the author’s initial selection or arrangement of the elements of the ‘database’ that indeed result from the intellectual creation in selecting or arranging them. The second requirement is that the perceptible item has to display these substantial similarities as a result of copying this initial selection or arrangement and not as a result of an independent creation made without knowledge of the existence of this initial selection or arrangement. These requirements imply, for example, that similarities relating to the commonplace characteristics of the arrangement of the elements of a ‘database’ are irrelevant for tracing embodiments of the right holder’s intellectual creation related to arranging these elements. In fact, others are free to give these same elements an arrangement with the same commonplace characteristics. In addition, the requirements just mentioned imply that only copying and arranging multiple elements of a ‘database’ – as opposed to copying an individual element – can result in an embodiment of right holder’s intellectual creation related to selecting or arranging these elements. Note however, that the database copyright does not influence the fact that an individual element of the database can be covered by, for example, ordinary copyright.\(^{225}\)

5.2.1.3. Categories of acts subject to the authorisation of the right holder

Database copyright results in reserving a right holder the following categories of acts concerning embodiments of his intellectual creation in selecting or arranging the elements of a ‘database’: ‘reproducing’, ‘adapting’, ‘distributing’, ‘communicating to the public’, ‘lending’ and ‘renting’. These categories of acts basically refer to the same types of acts as the corresponding categories of acts do

\(^{223}\) Database Directive, Article 3.


\(^{225}\) Database Directive, Article 3.2.
in ordinary copyright. However, specific to database copyright is precisely that these categories refer to these types of acts performed concerning an embodiment of the right holder’s intellectual creation in selecting or arranging the elements of a ‘database’. This implies that, in practice, these categories only refer to these types of acts performed in relation to a whole of elements found in that ‘database’ that is a sufficiently large whole to indeed embody that right holder’s intellectual creation in selecting or arranging the elements of the ‘database’.

5.2.1.4. Relevant exceptions to the categories of restricted acts

Database copyright also stipulates several exceptions to the categories of acts that, in principle, are subject to the authorisation of the right holder. Again, many of these exceptions will be of little relevance to a first responder acting in the context of an emergency due to their specific scope of application. However, this is not the case for all these exceptions.

The first exception that is relevant in the context of emergency relief is the mandatory exception, which the Database Directive stipulates in relation to normal use. This exception, in essence, states that the lawful user of a database does not need any permission of the right holder to perform acts that are necessary for the purposes of access to and normal use of the contents of the database.226 This exception implies that database copyright does not prevent first responders from accessing a database and using it in normal way, provided that they qualify as ‘lawful users’ of this database. This condition of qualifying as a lawful user gives rise to uncertainty. The reason is the ongoing debate whether such a ‘lawful user’ refers 1) only to persons granted a licence by the right holder; 2) also to anyone who lawfully acquired an embodiment of the ‘database’ (e.g. an embodiment once sold by the right holder); or 3) also to everyone acting within the limits of a normal use of an embodiment of the ‘database’ regardless whether this embodiment was acquired lawfully.227

The second exception that can be relevant in emergency situations again relates to public security. The Database Directive has allowed legislation of the EU Member States to provide that, for the purpose of public security, the categories of acts which database copyright normally subjects to the authorisation of the right holder may be performed without his permission.228 Most Member States have chosen to implement this exception quasi word for word. In case of such an implementation, the reference to ‘public security’ can arguably be taken to cover activities of first responders reacting to an emergency.

5.3. Database sui generis right

The database sui generis right grants a right holder an exclusive right in relation to a ‘database’ that demonstrates that there has been a qualitatively or quantitatively substantial investment in obtaining, verifying or presenting its content.229 This exclusive right results in an exclusive power for this right holder to control the extraction and the re-utilisation of the whole or of qualitatively or quantitatively substantial parts of the content of that ‘database’.230 The database sui generis right can in fact be analysed as granting an exclusive right over the substantial investment in obtaining,

228 Database Directive, Article 6.2 (c). Note: this directive does not stipulate that only a ‘lawful user’ of the ‘database’ is able to call upon this exception.
verifying or presenting the content of a ‘database’ as embodied in the whole and substantial parts of this content.\textsuperscript{231} Initially, the database \textit{sui generis} right grants this exclusive right to the maker of the ‘database’, that is to the person who took the initiative and the risk of investing in it.\textsuperscript{232} However, again, this exclusive right can be transferred to a new right holder or licensed to a licensee.\textsuperscript{233} The duration of the exclusive right is, in principle, limited to 15 years counting from the date of completion of the ‘database’.\textsuperscript{234} Yet any change to the contents of a ‘database’ that demonstrates a qualitatively or quantitatively substantial investment has the ‘database’ resulting from that investment enjoy its own term of protection of 15 years.\textsuperscript{235}

\section*{5.3.1. Requirements for the grant of an exclusive right}

In order to grant an exclusive right the database \textit{sui generis} right requires that a ‘database’ demonstrates that obtaining, verifying or presenting its content involved a qualitatively or quantitatively substantial investment.\textsuperscript{236} Investments relating to the creation of the elements included in the ‘database’ are not relevant to substantiate the required substantial investment.\textsuperscript{237} In this regard, it is usually accepted that the requirement of the investment being ‘substantial’ is to be interpreted as a \textit{de minimis} criterion that merely excludes insignificant investments.\textsuperscript{238} The qualitative assessment of the investment refers to an assessment of quantifiable resources involved whereas the qualitative assessment of the investment refers to an assessment of the efforts involved that cannot be quantified.\textsuperscript{239} Obtaining the protection offered by the database \textit{sui generis} right does not require any formalities or registration.

\section*{5.3.2. Whole or substantial part of the content of a database}

The exclusive right granted by the database \textit{sui generis} right results in an exclusive power of the right holder over the whole and qualitatively or quantitatively substantial parts of the content of his ‘database’.\textsuperscript{240} As mentioned, the object of this exclusive right can be analysed as the substantial investment in obtaining, verifying or presenting the content of a ‘database’ as embodied in the whole and substantial parts of this content. This means that whether a part of the content of a ‘database’ is a ‘substantial part’ in quantitative or qualitative terms, in essence, depends on this part embodying enough of the substantial investment involved in obtaining, verifying or presenting the content of the database.\textsuperscript{241}

In this regard, it is accepted that an individual element of a ‘database’ cannot qualify as a qualitatively or quantitatively substantial part of the ‘database’ in terms of the database \textit{sui generis}

\begin{thebibliography}{99}
\bibitem{232} Database Directive, Recital 41.
\bibitem{233} Database Directive, Article 7.3.
\bibitem{234} Database Directive, Article 10.1.
\bibitem{235} Database Directive, Article 10.3.
\bibitem{236} Database Directive, Article 7.1.
\bibitem{237} See: European Court of Justice 9 November 2004, C-46/02 (Fixtures Marketing t. Oy Veikkaus), para 49.
\bibitem{239} European Court of Justice 9 November 2004, C-444/02 (OPAP v. Fixtures Marketing), para 44.
\bibitem{240} Database Directive, Article 7.1.
\bibitem{241} See: European Court of Justice 9 November 2004, C-203/02 (BHB v. William Hill), para 69.
\end{thebibliography}
right. The database *sui generis* right therefore does not give the right holder an exclusive power over individual elements of a ‘database’.

It is also accepted that a person’s collection of the same elements as the ones included in the right holder’s ‘database’ can only constitute the whole or a substantial part of the content of that ‘database’, in terms of the database *sui generis* right, if the following holds true: this person’s collection came about by appropriating the substantial investment in obtaining, verifying or presenting the content of that ‘database’. If however, that person’s collection is based on his independent efforts this collection does not involve infringing the exclusive right, which the database *sui generis* right grants the right holder. In this regard, it is accepted that the person’s mere knowledge of the existence of the right holder’s ‘database’ does not prevent him from making his similar collection based on such independent efforts. On this point, the database *sui generis* right differs from ordinary copyright and database copyright.

5.3.3. Categories of acts subject to the authorisation of the right holder

The database *sui generis* right subjects two categories of acts to the authorisation of the right holder: ‘extracting’ and ‘re-utilising’. ‘Extracting’ refers to the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form. This broad notion of ‘extracting’, in principle, also covers such short-lived transfers to another medium which computers need to make to technically allow them to perform a task concerning a ‘database’. ‘Re-utilising’ is defined as any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by on-line or other forms of transmission. In this regard, however, the database *sui generis* right explicitly indicates that the first sale of a copy of a database within an EU Member State by the right holder or with his consent shall exhaust the right to control resale of that copy within the EU Member States.

Both ‘extracting’ and ‘re-utilising’ only refer to types of acts concerning the whole or a qualitatively or quantitatively substantial part of the content of a ‘database’. In principle, the database *sui generis* right does not give the right holder an exclusive power over these same types of acts performed concerning individual elements of the ‘database’ or performed concerning insubstantial parts of the content of the ‘database’. However, ‘extracting’ and ‘re-utilising’ does cover the repeated and systematic performance of these types of acts concerning such individual elements and insubstantial parts, in essence, as soon as the cumulative effect of these acts results in ‘extracting’ or ‘re-utilising’ a substantial part.

5.3.4. Relevant exceptions to the categories of restricted acts

The database *sui generis* right also stipulates several exceptions to the categories of acts that, in principle, are subject to the authorisation of the right holder. Once more, many of these exceptions

---

242 See: European Court of Justice 9 November 2004, C-203/02 (BHB v. William Hill), para 72 and Database Directive, Recital 46.
243 See: European Court of Justice 9 November 2004, C-203/02 (BHB v. William Hill), para 67.
246 Database Directive, Article 7.2 (a).
247 Database Directive, Article 7.2 (b).
248 Database Directive, Article 7.2 (b).
249 Database Directive, Article 7.5; European Court of Justice 9 November 2004, C-203/02 (BHB v. William Hill), para 89.
will be of little relevance to a first responder acting in the context of an emergency due to their specific scope of application. Again, this is not the case for all these exceptions.

The first exception that is relevant in case of emergency situations is the mandatory exception that the Database Directive stipulates in relation to insubstantial parts. This exception states that in relation to a ‘database’ which is made available to the public the right holder may not prevent a lawful user from ‘extracting’ or ‘re-utilising’, for any purpose whatsoever, qualitatively or quantitatively insubstantial parts of its contents.\textsuperscript{250} This exception is somewhat stating the obvious given that, as a rule, the database \textit{sui generis} right does not grant a right holder an exclusive right over acts that merely concern insubstantial parts of a ‘database’.\textsuperscript{251} In any case, it is to be accepted that, in principle, the database \textit{sui generis} right does not prevent first responders from legally ‘extracting’ or ‘re-utilising’ insubstantial parts of a ‘database’ that has been made available to the public.

The second exception that can be relevant in the context of emergency relief, again, relates to public security. The Database Directive has allowed legislation of the EU Member States to provide that concerning a ‘database’ that is made available to the public its lawful user may, for the purpose of public security, ‘extract’ or ‘re-utilise’ a substantial part of its contents without the authorization of the relevant right holder.\textsuperscript{252} Again, most Member States have chosen to implement this exception quasi word for word. In case of such an implementation, the reference to ‘public security’ can arguably be taken to cover activities of first responders reacting to an emergency, provided that they qualify as ‘lawful users’.\textsuperscript{253} This condition of qualifying as ‘lawful users’ again gives rise to uncertainty. The abovementioned discussion on the possible interpretations of the notion of a ‘lawful user’ in the context of database copyright is also found in the context the database \textit{sui generis} right.

5.4. Impact on exchanging and using data in the context of disaster relief

First responders wanting to exchange and use data in the context of emergency situations often face the risk of infringing intellectual property rights. Their exchange and use of incorporations of data is very likely to infringe ordinary copyright and can, under circumstances, also infringe database copyright or the database \textit{sui generis} right.

Intellectual property rights limit the opportunity for first responders to exchange and use incorporations of data that are covered by intellectual property rights. Intellectual property rights do so because exchanging and using these incorporations often involves performing categories of acts that are subject to the authorisation of a right holder. For example, displaying a copyrighted map to first responders by means of a digital platform is very likely to involve two such categories of acts, namely ‘communicating to the public’ and ‘reproducing’. Even in an emergency, the legal options for first responders to perform such categories of acts are limited. For these first responders as well, these options are limited to performing them within the scope of an explicit exception or performing them after the right holder has agreed to licence or transfer his exclusive right granted by the intellectual property right.

\textsuperscript{250} Database Directive, Article 8.1.
\textsuperscript{252} Database Directive, Article 9 (c).
The explanation why first responders often face this risk is twofold. The first reason is that ordinary copyright, database copyright and the database sui generis right cover many incorporations of data. For example, many texts, photographs, maps and databases are likely to be covered by one of these intellectual property rights. After all, ordinary copyright, database copyright and the database sui generis right, respectively, do not require a high level of intellectual creation nor a high level of investment in order to grant exclusive rights. In relation to this first reason, it is to be noted that first responders cannot rely on official registries of ‘works’ or ‘databases’ to assess whether an incorporation of data is covered by ordinary copyright, database copyright or the database sui generis right.

The second reason for the high risk of infringement is that ordinary copyright, database copyright and the database sui generis right give right holders an exclusive power over very broad categories of acts with only limited exceptions. If an incorporation of data is covered by these intellectual property rights, a wide variety of acts concerning it can be subject to the authorisation of the relevant right holder (e.g. merely displaying it to other first responders). In case of digital incorporations of data this is even more the case. Virtually every act concerning such a digital incorporation technically requires duplicating this incorporation in parts of a computer. Making these duplications can be subject to the authorisation of the right holder.

If first responders want to exchange and use incorporations of data covered by intellectual property rights without infringing these rights they can basically opt for two approaches. Both approaches, however, are likely to take time and efforts.

A first approach is that the first responders limit themselves to those acts concerning the incorporations of data covered by intellectual property rights that these intellectual property rights do not make subject to the authorisation of the right holder. In this approach, first responders can still perform acts that, from the outset, do not qualify as categories of acts subject to the authorisation of the right holder. In this approach, they can also perform categories of acts subject to the authorisation of the right holder, provided that they do so in the circumstances described by one of the explicit exceptions to these categories of acts. Nevertheless, this first approach has considerable disadvantages. First of all, first responders applying this approach will find themselves significantly limited in what they can actually do concerning the incorporations of data. This results from the fact that the categories of acts subject to the authorisation of the right holder are defined in a very broad way whereas the few exceptions to these categories of acts are to be interpreted in a restrictive way. Secondly, it can prove to be time-consuming and difficult to map the exact scope of the categories of acts subject to the authorisation of the right holder in combination with the exact scope of the relevant exceptions to these categories of acts. This mapping exercise is difficult because of ongoing legal debates and, especially in case of the exceptions, because of differences between the relevant provisions in the national legislation of the EU Member States.

A second approach is that the first responders avoid infringing intellectually property rights by concluding the necessary agreements with the right holders. In this approach, first responders ensure that their acts concerning incorporations of data covered by intellectual property rights do not infringe the exclusive rights of the right holders by having these right holders agree to licensing or transferring them these exclusive rights. In practice, concluding a mere licence agreement will mostly suffice to cover the needs of first responders reacting to an emergency. After all, this licence agreement already gives first responders the permission of the right holder to perform the categories of acts subject to his authorisation. For the purpose of emergency relief a first responder normally has little interest in a transfer of rights making him the new right holder.
This second approach, concluding agreements with the right holders, of course has a significant advantage. Concluding such agreements can provide first responders with a legal possibility to perform whatever categories of acts that are subject to the authorisation of the right holder that helps them respond more efficiently to an emergency.

This second approach has disadvantages though. A first disadvantage is that right holders can of course make agreements dependent upon payment. Obtaining a licence, for example, can be made dependent on paying the right holder a licence fee. A second disadvantage is that concluding agreements with the right holders takes time and efforts. If an incorporation of data is covered by an intellectual property right simply tracing the right holder of the exclusive right can already prove to be time-consuming. After all, ‘databases’ and incorporations of ‘works’ do not always come with information that makes it easy to identify and contact the relevant right holder. As mentioned, it is also impossible to rely on official registries of ‘works’ or ‘databases’ to obtain this information about the relevant right holder. The extent to which the time needed to conclude agreements with the right holders becomes a problem depends on the circumstances. If first responders can assess in advance that they will need certain data in light of future emergency situations this time issue is not very problematic. In that case, they can negotiate the necessary agreements before the emergency arises. However, if the need for certain data becomes apparent only in light of an acute emergency valuable time can indeed be lost in negotiating and concluding agreements with the right holders.
6. Summary

While this deliverable focuses on ethical and legal obligations of the EPISECC consortium with respect to the development of a Common Information Space, issues arising from the processing of personal data were considered in the context of WP 3 (see Section 3.9). To meet the legal requirements related to the processing of personal data, the EPISECC developed an information notice (see Annex II) and notified the Austrian Data Protection Authority (see Annex IV). The EPISECC partners consulted and obtained an approval of the interview procedure from the KU Leuven Social and Societal Ethics Committee (see Annex III). The EPISECC partners followed this procedure when contacting volunteers and requesting them to populate the EPISECC inventory.

The deliverable distinguished two groups of ethical principles that have to be considered by the consortium partners. The first group of principles relates to the researchers conduct, whereas the second group focuses on the outcomes of newly developed applications. The deliverable also points out ethical concerns related to the security of information systems.

As a result of the legal analysis of the EU data protection and intellectual property rights’ frameworks and the discussion on the re-use of public sector information in a situation of a major disaster, the following conclusions can be made:

- The EU Data Protection Framework does not restrict the processing of personal data while providing disaster response. However, to be compliant with EU data protection rules the data controller (i.e. an entity determining purposes of the processing) is required to follow certain requirements, general and data quality principles. The processing of personal data of first responders, volunteers, and affected people should be based on different legitimate grounds. These legitimate grounds have to be considered prior to setting up the Common Information Space. The current EU Data Protection Framework is set by Directive 95/46/EC which is of general scope and does not address a specific situation of disaster management in which processing of personal data of first responders and affected persons may occur. There is no doubt as to the relevance of this legal framework. However, more contextual analysis has to be conducted to determine the grounds legitimising data processing of affected people. It has been suggested that assigning roles to agents providing disaster relief (i.e. determining who is a controller and who is a processor) is difficult as data exchange in a disaster response situation has become complex; often data are being processed via data maintenance tools over which first respondents as well as individual organisation have no influence. Additionally, it is reasonable to expect that the fragmented approach to the processing of personal data by the first responders will remain because the revised EU Data Protection Framework does not address the civil protection mechanisms developed by the Member States. The General Data Protection Regulation awards Member States with a possibility to enact national rules that are deemed to be necessary and proportionate to the intended aims (e.g. security of citizens).

- The legal regimes on environmental information, spatial data and re-use of documents held by the public sector increase the amount of data available to first responders in case of emergency situations. These regimes make a valuable contribution to clarifying the conditions and
circumstances under which this data can be accessed, exchanged and used. However, the true practical relevance of these regimes in the context of emergencies is highly dependent on the timeframe in which they result in data being available to first responders. From that perspective it is advisable to consider way to integrate data made available by these regimes prior to setting up the information space.

- Contrary to the EU Data Protection Framework and the legal framework facilitating reuse of public sector information, the intellectual property rights’ framework limits the opportunity for first responders to legally use data in case of emergencies. The broad protection offered by ordinary copyright, database copyright and the database sui generis right often puts first responders in a position that their use of incorporations of data in an emergency risks constituting infringement. The opportunity for first responders to avoid such infringement by concluding the necessary licencing agreements can be time-consuming and dependent upon payment. On the contrary, exceptions to the categories of acts which these intellectual property rights reserve the right holder can offer first responders a cheap, immediate opportunity to use incorporations of data involving intellectual property protection without involving infringement. However, because the relevant provisions tend to differ across the Member States it is not always clear whether a first responder’s actual use of an incorporation of data in emergencies is indeed covered by such an exception. Therefore, in view of promoting the use of data in the context of emergency relief it would be advisable to have all Member States introduce an identical, specific exception relating to emergencies in their legislation on intellectual property rights.
Bibliography

Legislation:


[15] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011 (COD) (General Data Protection Regulation).
Policy documents:


Literature:


[12] C. Matlack, Germans Battle Floods with Sandbags, Facebook, and Twitter (Bloomberg Business, June 12, 2013),

concept for volunteer management in disaster relief” (Springer-Verlag Berlin Heidelberg 2011).


project.


Case law:
[1] European Court of Justice, C-145/10 (Painer).
[5] European Court of Justice, C-131/12 (Google Spain).
Annex I – Questions related to the Common Information Space

This annex includes a list of questions that should be discussed within the EPisecc consortium when setting up the architecture for the Common Information Space. This appendix has been prepared following the guidance provided by Pat Jeselon and Anita Fineberg in their work titled “A Foundational Framework for a PbD – PIA” and published in November, 2011. Answering these questions will provide output for tasks 7.2 and 7.3. To provide elaborate answers to these questions, the project partners have to agree upon the architecture of a Common Information Space.

General questions:

1. What types of data the Common Information Space will include?
2. What will be the main sources of data for the Common Information Space?
3. Will the Common Information Space process any data that can be qualified as personal data or as special category of data?
4. Who will be the controller of the processing operations? (i.e., who will decide on types of personal to be collected and who will decide on the use to which the personal data will be put?)
5. Who will manage data uploaded on the system?
6. In what situations and under what circumstances will the Common Information Space collect data?
7. Will the controller outsource data processing to the processor?

Questions for data controller:

8. Has the controller conducted a mapping and developed an inventory of personal data that he collects?
9. Has the controller developed privacy management policies for internal and external use?
10. Has the controller determined the purposes of the data processing?
11. Has the controller evaluated proportionality of the surveillance system to set objectives?
12. Does the controller know the physical location of the collected data that may include personal data?
13. Has the controller implemented appropriate organizational and technical measures that would address the level of risks associated with data processing?
14. Has the controller set up a training program for employees that have access to the obtained data?
15. Has the controller implemented appropriate organizational and technical measures to facilitate access to the system only for the authorized personnel?
16. Has the controller set up measures to mitigate third party risk?
17. Has the controller identified and evaluated external and internal risks and threats associated with the processing of personal data in this particular context?
18. Has the controller implemented appropriate organizational and technical measures that would prevent access and manipulation of the collected data, for example, via social engineering attacks or installation of the malware?
19. Has the controller set up a process to review and re-evaluate risk and threats associated to the processing?
20. Has the controller implemented appropriate organizational and technical measures that would allow to check reliability of the warrant/third party access request to obtain relative personal data?

21. Has the controller implemented appropriate organizational and technical measures that would prevent negative impact on the data subject in case the collected data are manipulated?

22. Has the controller implemented appropriate organizational and technical measures that would allow to prevent third party’s searches in the archive that would go beyond what has been foreseen in the authorization to access such personal data?

Questions allowing determination whether an act of a first responder infringes an intellectual property right.

23. Does the act of the first responder relate to anything that is covered by the protection of an intellectual property right?
   - **Ordinary Copyright**: does it involve an embodiment of a person’s own intellectual creation?
   - **Database copyright**: does it involve an embodiment of a person’s own intellectual creation in selecting or arranging the elements of a ‘database’?
   - **Database sui generis right**: does it involve the whole or a substantial part of the contents of a ‘database’ that shows the required substantial investment?
   - If not, the act does not infringe an intellectual property right.
   - If yes, question (23) needs to be answered.

24. Does the intellectual property right make the act subject to the authorisation of the right holder?
   - **Ordinary and database copyright**: does the act qualify as ‘reproducing’, ‘communicating to the public’, ‘distributing’, ‘lending’ or ‘renting’?
   - **Database sui generis right**: does the act qualify as ‘extracting’ or ‘re-utilising’?
   - If not, the act does not infringe an intellectual property right.
   - If yes, question (24) needs to be answered.

25. Is the act covered by an exception stipulated by the intellectual property right?
   - **E.g. ordinary copyright**: is the act covered by the exception relating to temporary technical reproductions or by an exception relating to public security?
   - **Database copyright**: is the act covered by the exception relating to normal use or by an exception relating to public security?
   - **Database sui generis right**: is the act covered by the exception relating to insubstantial parts or an exception relating to public security?
   - If yes, the act does not infringe an intellectual property right.
   - If not, question (31) needs to be answered.

26. Did the right holder give permission to perform the act (e.g.: by way of granting a licence)?
   - If yes, the act does not infringe an intellectual property right.
   - If not, the act infringes an intellectual property right.

***
Annex II – Informed consent form for the EPISECC Inventory

This annex includes the information notice discussed in Section 3.8, titled “EPISECC compliance with the EU Data Protection Framework”. The information notice includes a consent form, which was provided to volunteers in the context of WP 3 research activities. The information notice and the consent form follow requirements outlined in Directive 95/46/EC, the Austrian Data Protection Act, and Consent Guidance for FP7 projects.

Information Notice

This information notice is an accompanying document to a request to provide information for the research purposes related to the EC funded project, titled “Establish Common Information Space to Enhance seCurity of Citizens” (hereinafter “EPISECC”), grant no. 607078. The EPISECC project was launched on the 1st June, 2014. The Austrian Institute of Technology is the managing partner of the project and is responsible (i.e., data controller) for the processing of data within the scope of the questionnaire.

Purpose of the questionnaire

The EPISECC project aims at creating a Common Information Space for public safety services. In the current stage of the project, the participating partners seek to obtain information from organizations providing Public Protection and Disaster Relief (hereinafter “PPDR”) that would allow to develop a pan-European inventory of past critical events and disasters. This inventory has been designed to focus on the performance of processes, the data exchange and the organizational boundaries. The inventory aims at pointing out similarities, differences, weakness and strengths of the most commonly used international standards, procedures, practices in the field of PPDR. As a follow up of a desk research on publicly available information (e.g. sources accessible online), some of the project partners will reach out to organizations for additional information that is necessary to complete their analysis.

Requested information

For the purposes of developing the inventory we do not intend to process any other personal data apart from the information related to your official capacity. The EPISECC project has no intentions to obtain special categories of data, as defined in Directive 95/46/EC. 254 Also, we do not intend to process confidential data. We kindly ask you to identify, whether data you share are considered to be classified, confidential, or restricted information that is subject to legal, organisational or security requirements under your governing law. In case, you identify that you provide us with classified, confidential, or restricted information, we will take appropriate security measures to protect it against unauthorized access and misuse.

254 According to Article 2 of Directive 95/46/EC, personal data means “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity,” special categories of data (sometimes referred to as sensitive data) include information about “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”
Use of obtained information

The EPISECC partners will not distribute data obtained from you to third parties outside the scope of the EPISECC project. However, please note, the obtained information, with an exception of personal data, which is not identified as restricted or classified information, will be used to prepare output related to the deliverables of the EPISECC project. Consequently, this means that the obtained data may be published and become available to the general public.

All data you provide in the EPISECC Pan-European inventory of disasters and business models for emergency management services will be only processed for scientific research purpose in an aggregated and anonymized format. Single persons will not be distinguishable from the data.

Contact details

For more information about the EPISECC project and its partners please visit: https://www.episecc.eu.
For more information about the EPISECC inventory contact: Dr. Georg Neubauer, AIT Austrian Institute of Technology, georg.neubauer@ait.ac.at.

Participant’s consent

I volunteer to participate in the EPISECC inventory of past critical events and disasters. I am informed and take note that I have a right to access, update, rectify and delete my personal data provided to the EPISECC project.

Name: ___________________
Date: ___________________ 
Signature: ________________
Annex III – Ethical approval of the interview procedure

This annex includes three documents related to the ethical approval of interview procedure used in the context of WP 3. The first document includes a statement from the Vienna ethics committee declaring that the EPISECC project falls out of the scope of its work. Following up on the opinion of the Vienna ethics committee, the EPISECC project submitted an application form to the KU Leuven Social and Societal Ethics Committee regarding the procedure of contacting and collecting information from volunteers for the EPISECC inventory. This application form, which is discussed in Section 3.8, titled “EPISECC compliance with the EU Data Protection Framework,” is included as the second document in this annex. The KU Leuven Social and Societal Ethics Committee approved the suggested interview procedure. The approval of the KU Leuven Social and Societal Ethics Committee follows the application form and is the last document in this annex.
Sehr geehrte Frau Jager!

Anlässlich Ihres Ansuchens zur Beurteilung der Studie mit dem Titel:

“EPISECC (Establish Pan-European Information Space to Enhance seCurity of Citizens)”


Eine Zuständigkeit der Ethikkommission der Stadt Wien zur Beurteilung eines Projektes ist nur dann gegeben, wenn entweder eine Prüfung von Arzneimitteln oder Medizinprodukten oder die Anwendung neuer medizinischer Methoden am Menschen vorgesehen ist. Keines der genannten Kriterien trifft auf das gegenständliche Projekt zu.

Mit freundlichen Grüßen
Der Geschäftsführer:

Reinhard Undeutsch
Document may be completed in Dutch or English.

Send complete document (+ annexes) to: smec@kuleuven.be

Date: January 16  
Research Unit: ICRI/CIR  
Faculty / department: Law Faculty

Responsible coordinator(s), supervisor(s) - names & e-mail addresses:
Anton Vedder, Anton.Vedder@law.kuleuven.be

Researcher(s) & experimenter(s) - names & e-mail addresses:
Lina Jasmonaita, lina.jasmonaita@law.kuleuven.be

Signature of coordinator: ___________________________

To be completed by SMEC Board

Advise by SMEC Board:
☐ favorable - allotted SMEC number:
☐ recommended revision before start of project:
☐ unfavorable - required revisions:

☐ Evaluation by Medical Review Board recommended (ORANGE code)
Specific topics of attention:
S number: _______________________________ 
M number: _______________________________

☐ Evaluation by Medical Review Board required for following reasons (RED code):
S number: _______________________________ 
M number: _______________________________

Starting date of project: June 1, 2014
Type of dossier:
☐ New project
☐ Extension: (SMEC or S/ML number)
☐ Modification: (SMEC or S/ML number)
☐ General approval for grant application (applications for subparts of the project might still be required at a later date)

Title: Establish Pan-European Information space to Enhance seCurity of Citizens (hereinafter "EPISECC"), grant no. 607028.

Korte beschrijving van het onderzoeksthema & belangrijkste onderzoeksvragen / Brief description of research topic & main research questions:

The EPISECC aims at creating a common information space for public safety services. In the current stage of the project, the participating partners seek to obtain information from organizations providing Public Protection and Disaster Relief (PPDR) that would allow to develop a pan-European inventory of past critical events and disasters. This inventory has been designed to focus on the performance of processes, the data exchange and the organizational boundaries. The inventory aims at pointing out similarities, differences, weaknesses and strengths of the most commonly used international standards, procedures, practices in the field of PPDR. As a follow up of a desk research on publicly available information (e.g., sources accessible online), some of the project partners will reach out to organizations for additional information that is necessary to complete their analysis. Some of the questions include:

- Which information system does your organization use for disaster management and civil
research techniques & methods (may involve more than one):
☑ questionnaire (validated, published) - specify: the questionnaire will contain a list of questions that will have been approved by the consortium members. The questionnaire will be accessible via an online link provided in the email or letter inviting to participate in the inventory. Questionnaire system, including the answers, will be stored on the Austrian Institute of Technology (AIT) physical server. The AIT is the managing partner of the project. The AIT server is located in Selbersdorf, Lower Austria. The access to the obtained information will be limited to authorised AIT personnel associated with the EPISECC project.

☑ questionnaire (non validated): included as annex
☑ electrography or imaging (e.g., EEG, MEG, MRI);
☑ acceptance letter of clinical department (if appropriate);
☑ behavioral experiments/manipulations
☑ interview or observation
☑ collective study on students
☑ other:

Briefly describe the practical procedure. What will participants have to do specifically, when & in what order?

1. Project partners (i.e., the consortium) will contact participants - stakeholders of the EPISECC project (e.g., an employee at a fire fighter unit) by an email or letter which will contain an invitation to participate in the inventory. A template of the invitation letter has been approved by the consortium. All projects partners have agreed to use the same template while reaching out to stakeholders. The template letter (i.e., standard letter for data acquisition) is attached in the Annex.

2. In order to address stakeholders individually, the template letter will be adjusted and include details of the addressee (e.g., name and address of an entity). The letter will kindly ask to take part in the inventory or forward information to the person within the organisation who would be in official capacity to participate in the inventory. The letter will provide a link to the questionnaire.

3. Upon the access to the questionnaire a stakeholder will receive an information notice. The information notice will provide a brief description of the EPISECC project, the purpose of the inventory and the types of requested personal data. A participant will be allowed to fill out the questionnaire only after expressing informed consent, as foreseen in Directive 95/46/EC on the processing of personal data.

4. After expressing one’s consent a person will be allowed to access the questionnaire. The questionnaire will contain two stages.

5. The first stage will aim at authenticating a person (i.e., ensure that a person who enters data to the systems involved or works at that particular civil protection organisation). During this stage a person will be asked to fill in her/his name and information related to her/his official capacity (e.g., an organisation/entity, name, address, and a qualification/job title). Upon the completion of this phase a person will receive a key (number associate to his personal information) and an email with an URL link to the second stage of the questionnaire.

6. A participant will have to access the URL (i.e., web address) in order to proceed to the second stage of the questionnaire. Upon the access to the URL the person a person will be asked to use her/his key to create a profile and start the questionnaire. A participant will be asked to create a password for his profile. Provided the possibility to save the questionnaire before submitting it, the participant can fill in relevant information upon few instances.

7. In case a participant (i.e., stakeholder) has questions regarding the questionnaire (e.g., an...
intention of the question or an expected outcome), she/he can contact the EPISECC consortium and ask for clarification and additional guidance. As a result of the request, the managing partner will assign a partner that could assist the stakeholder.

Participants

**Age:** The selection of participants is not based on the age of stakeholders. Yet it is expected that participants will be above 18 years old.

Special characteristics (e.g., employees, experts, interns or students, paid volunteers, patients or clients, infants,...): Persons involved in national/regional crisis and disaster management.

Criteria for participant selection / recruitment:

Participants will be selected from pre-defined list of stakeholders.

The target group of the questionnaire is characterised by:

Field of activity: National/regional crisis and disaster management, especially in the response to disasters.

Special dimension of activity: The questionnaire will cover countries of the project partners, namely Austria, Croatia, Germany, Great Britain, Italy, Luxembourg, and Finland.

Work description: It is expected that in order to provide requested information to the questionnaire, a participant will have to be performing in a specific role in crisis and disaster management. For example, a person could be involved in a member of strategic executive or tactical executive personnel and be responsible for the area of information exchange.

Exclusion criteria: Actors primarily at political, operational actors, not/selected countries

☐ yes – specify:

Provided that a very specific knowledge is required to fill in the questionnaire, the invitation letters will be sent only to the entities providing PPDR (i.e., Public Protection and Disaster Relief).

☐ no

Protocol involves functionally or physically incapacitated participants:

☐ yes – specify:

☐ no

Compensation or remuneration

**Participant remuneration or compensation**

☐ yes – specify:

☐ no – why not?

The main objectives of the EPISECC project is to improve disaster management in the European Union. The invitation letter does not create an obligation to participate and fill in the questionnaire. It counts on voluntary participation of stakeholders. It is in the interest of stakeholders to improve data management in disaster relief.

Direct benefits of participation:

(Specify what a participant may learn from the study or what other benefits might result from participation.)

As a result of the EPISECC project, disaster management capacities of decision stakeholders should be strengthened. The inventory of past event will directly benefit the participating stakeholders as they will be able to analyse and compare different information sets (note: in the aggregated form, information about individual past events will not be available) that were used to provide disaster response.

Benefits to others, scientific community, patient groups, organization, society, etc.

The aim of the questionnaire developed by the EPISECC project is to create a publically available pan-European inventory on the following items:

- Fast critical events, disasters and their consequences including the time dimension and the response given in terms of means used, costs, etc.;
- Available information about the data sets, the daily information management tools and processes, the integration into crisis management procedures and the information systems used by first responders and police authorities in disaster and crisis management procedures;
- Gaps and shortcoming in the current systems, services and tools;
- Deployment of crisis and emergency management services in terms of organisational model: is-
house, outsourced, etc., and how each approach affects the service.

Participant information, confidentiality, & informed consent
- According to standard IC procedures & good scientific practices, participants should be informed as completely as possible about aims & practicacies of the study. Participants should definitely be fully informed about any possible discomfort or embarrassment they might experience during participation. All information should be individually provided, fully understandable, & in the native language of the participants. Also, debrifing after participation should be as complete as possible.
- Informed consent should be provided in written form by each and every well-informed participant. Information about compensation or remuneration can be provided on the IC form, but obviously, participants cannot be coerced in any way to complete a study or experiment.
- The IC model form on the SMEC webpages can be used, but may be extended or altered depending on particular characteristics of the study. The proposed IC form should include information about the study protocol as well as contact information of the responsible investigator & the SMEC board.
- Informed consent and study information should be part of a single form/document.
- Informed consent by proxy should be obtained from parents or legal guardians in case of participants below 16 years of age, or those functionally unable to provide consent. As a general principle, the Board discourages passive informed consent procedures – especially in the case of minors or otherwise vulnerable individuals.

Informed consent procedure and timing in relation to study protocol:
The informed consent form together with the information notice and request to fill in the questionnaire will be provided.

Justify deviations from standard IC procedure:

Include proposed IC form as Annex 1.

Information provided to participants before the start of the study/experiment:
Prior to starting with the questionnaire participants will be provided with the letter inviting to participate in the inventory. The letter will include a link to the questionnaire. Upon the access of that link participants will be provided with an information notice which will include information about the EPISECC project, the purposes of the questionnaire and how they can manage data that they provide. In order to proceed to the first stage of the questionnaire participants will have to express their consent to the processing of their personal details and information about their organisation.

How will this information be provided:
Project partners will contact a predefined list of stakeholders of the EPISECC project by email or offline means (e.g., letter could be send by mail). An information notice will provided in a digital form (upon the access to the questionnaire).
Project partners will approach stakeholders in their countries
Will participants be deceived?
☐ yes – explain why deception is necessary in this study:
☐ no
Explain how participants will be deceived:

Explain when and how participants will be debriefed about the deception:

Explain how confidentiality of personal information & anonymity will be ensured:
The following measures will be taken by the managing partner (i.e., AIT) of the EPISECC project with respect to the protection of confidentiality and anonymity of personal data:
The AIT will take organizational and technical measures to ensure protection of personal data. The AIT will ensure that only authorized personnel can access to data provided in the first and second stages of the questionnaire.
The AIT will ensure that data obtained in the first stage of the questionnaire is kept separately from the data obtained during the second stage. The data obtained in the first stage will be encrypted. Upon the completion of the first stage of the questionnaire the person will be given a key (number), which will be used during the second stage of the questionnaire. The second stage of the questionnaire will not require to enter personal data (e.g., name, surname, or email address).

Instruments & equipment

Which diagnostic instruments will be included? Which validated questionnaires? Published procedures or methods?

The questionnaire will contain a list of questions that will have been approved by the consortium members. The questionnaire will be accessible via an online link provided in the email or letter inviting to participate in the inventory.

Include details about unvalidated/unpublished devices as Annex 2.

Does the study involve research equipment or experimental devices?

☐ yes – specify:

☐ no

Specify certification, safety procedures, homologation of equipment:

Include certificates as Annex 3.
Discomfort
Participants might feel embarrassed or confused during the course of the study:
☐ yes – specify:

☒ no
Participants might experience other discomfort or inconvenience:
☐ yes – specify:

☒ no
Participants might experience (physical or mental) discomfort:
☐ yes – specify:

☒ no
Could there be any long-term consequences or sequelae?
☐ yes – specify:

☒ no
Is any support or counseling offered after participation?
☐ yes – specify:

Debriefing & feedback
Which information is given to participants during debriefing?
How will this be provided?
What information is provided to participants about outcome of the study?
After the completion of the questionnaire a person will have a possibility to access the inventory
where she/he on the basis of aggregated data can analyse various data sets related to disaster
relief (e.g., how much time did it take set up a field hospital in the event of an earthquake).
Additionally, the EPISECC project will publish reports and present the results to the stakeholders and
the general public.

How is this information provided or how can participants request it?
The EPISECC consortium will be open to reply to any queries from the stakeholders that fill in the
questionnaire. Participants will be provided with an email address where they can send their requests
and queries.
Dear Ms Jasmontaite,

Your research protocol entitled: “Establish Pan-European information space to Enhance seCurity of Citizens (hereinafter “EPICECC”)” has been reviewed by the SMEC board, d.d. 9 February 2015.

The board concluded that your protocol meets the expected ethical standards regarding the voluntary involvement of human participants in scientific research. Its decision with regard to this protocol is therefore: Favorable

Your protocol received the following dossier no. G-2015 02 159

This is your final approval number. Please save this email properly and refer to the G-number in future communications.

If you have any further questions, please don’t hesitate to contact us.

Best regards,

Prof. R. D’Hooge
Chair SMEC KU Leuven

www.kuleuven.be/research/integrity/smac.html
Annex IV – Notification to the Austrian Data Protection Authority

This annex includes a letter confirming that the AIT notified the national data protection authority about the processing of the personal data in the context of the EPISECC inventory. During the notification procedure, the AIT team was assisted by its legal department. A screenshot of the national registrar follows the confirmation.
Vertreter des Auftraggebers in der EU bei der Datenanwendung:

Datenschutzbeauftragter:

Die Datenanwendung gehört zum
☐ privaten Bereich
☐ öffentlichen Bereich

Die Datenanwendung erfolgt
☐ automationsunterstützt
☐ manuell

Angaben zur Anwendbarkeit der Vorabkontrolle (§ 18 Abs. 2 DSG 2000):
☐ Verwendung von sensiblen Daten
☐ Verwendung von strafrechtlich relevanten Daten
☐ Vorliegen eines Kreditinformationssystems
☐ Vorliegen eines Informationsverbundsystems
☐ Videoüberwachung (gemäß § 50c DSG 2000)
☐ Vorliegen keiner der Voraussetzungen

Rechtsgrundlage(n) für die gemeldete Datenanwendung:
Forschungsaufrag der Europäischen Kommission - Projekt EPISSEC
(Establish Pan-European Information Spaces to Enhance seCurity of Citizens)
Datenanwendung gemäß §46 Abs. 2 Z. 2 -DSG 2000 - Projekt EPISSEC
Grant Agreement no 607078
Collaborative Project, Call: Seventh Framework, Theme (SEC-2013.5.1): Analysis and Identification of Security Systems and data Used by First Responders and Police Authorities-Capability Project
Zustimmungsverlängerung der Betroffenen gem. §8 (1) Z.2 DSG 2000

Bescheid der Datenschutzbehörde (Internationaler Datenverkehr gemäß § 13 DSG 2000):

Bescheid der Datenschutzbehörde (Auflagenbescheid gemäß § 21 Abs. 2 DSG 2000):

Besondere Angaben zum Inhalt der Datenanwendung:

<table>
<thead>
<tr>
<th>Betroffene Personengruppen</th>
<th>Datenarten</th>
<th>Nummern der Empfängerkreise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Befragte bei Umfragen (z.B. Behördenvertreter, NGOs, Forschung, Stakeholder und Organisationen im Kriseneinsatz)</td>
<td>Name</td>
<td>01, 02</td>
</tr>
</tbody>
</table>
### Datenanwendung (DAN) - Änderungsmeldung

#### Voraussetzungen

Die Formular wurde erfolgreich weitergeleitet:

- **Name der Datenanwendung**: Eintrag / Format
- **Datum und Uhrzeit**: 15.04.2023 13:22:01

**Anmerkungen**: Die Eingangsbestätigung dient als Nachweis des elektronischen Eingangs bei der zuständigen Dienststelle.

#### Verwendbarkeit

<table>
<thead>
<tr>
<th>Informationen / Links</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DDI-Dokumentation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meilensteine</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kontakt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Benutzer</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Christian Hönig</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Abteilung</th>
<th></th>
<th></th>
</tr>
</thead>
</table>