EVACUATE

FP7-313161

A holistic, scenario-independent, situation-awareness and guidance system for sustaining the Active Evacuation Route for large crowds

ETHICAL AND LEGAL REQUIREMENTS ANALYSIS (SPECIFICATIONS, PROPORTIONALITY, IMPLEMENTATION AND EVALUATION)

Deliverable Identifier:	D.11.2
Delivery Date:	Mar 31, 2015
Classification:	Public
Editor(s):	Diana Dimitrova (ICRI/CIR, KUL); Bjorn Coene (ICRI/CIR, KUL)
Document version:	1.0 - 2015
Contract Start Date:	April 1st, 2013
Duration:	48 months
Project coordinator:	EXODUS S.A. (Greece)
Partners:	EXO (GR), IT INNOVATION (UK), ICCS (GR), HKV (NL), TEL (GR), TEK (ES), AIA (GR), VITRO (IT), CDI (UK), INDRA (ES), KUL (BE), DXT (FR), POLITO (IT), STX-FR (FR), TUD (DE), TUC (DE), ASRS (ES), METB (ES), TIM (IT)

Project co-funded by the European Commission under the 7th Framework Programme

SEVENTH FRAMEWORK PROGRAMME

Document Control Page

Title	**Ethical and legal requirements analysis (specifications, proportionality, implementation and evaluation)**	
Editors	Diana Dimitrova	ICRI/CIR, KUL
	Bjorn Coene (Ch. 8 and 9)	ICRI/CIR, KUL
Contributors	Diego Betancourt	TUD
	Dimitris Drakoulis	TELESTO
	Zoheir Sabeur	ITINNOV
	Francois Drezet	STX
	Pierre Berseneff	STX
Peer Reviewers	Eduardo Martinez Gil	INDRA
	Hanneke Vreugdenhil	HKV
Format	Text - Ms Word	
Language	en-UK	
Work-Package	WP 11	
Deliverable number	D.11.2	
Due Date of Delivery	31/03/2015	
Actual Date of Delivery	31/03/2015	
Dissemination Level	One of the following: Public Restricted to other programme participants (including the Commission Services) Restricted to a group specified by the consortium (including the Commission Services) Confidential, only for members of the consortium (including the Commission Services)	
Rights	eVACUATE Consortium	
Audience	☒ public ☐ restricted ☐ internal	
Date	31/03/2015	
Revision	HKV and INDRA	
Version	1.0	
Edited by	KUL	
Status	☒ draft ☒ Consortium reviewed ☒ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	06/03/2015	Comments on clarifications and improvement of the original text	Hanneke Vreugdenhil (HKV)
0.2	17/03/2015	Comments to the original text	Dimitris Petrantonakis (EXO)
0.3	12/03/2015	Corrections and clarifications of Chapters 4 and 5	Dimitris Drakoulis (TELESTO)
0.4	12/03/2015	Review of the original text	Eduardo Martinez Gil (INDRA)
1.0	27/03/2015	Final version	Diana Dimitrova and Bjorn Coene (KUL)

Table of Contents

Table of Figures

Executive summary

The present deliverable builds upon deliverable "D11.1 High level ethical and legal framework." Like D11.1, it will focus mainly on privacy and data protection. It was considered wise to add to the legal discussion also certain aspects related to Intellectual Property Rights (IPR) and Copyright. Ethical topics such as discrimination will be addressed in the legal discussion where relevant, e.g. in the section on video surveillance and its potential discriminatory effect.

D11.2 provides a more in-depth analysis of the privacy and data protection issues which eVACUATE raises. The purpose of D11.1 was to set out the general legal and ethical framework, applicable to eVACUATE. As a result, it derived the high-level legal and ethical requirements, stemming from the EU and Council of Europe privacy and data protection legal framework. In eVACUATE, these requirements have to be complied with by the partners (1) in the course of their research and development activities when working with personal data, such as video images, and (2) when designing the individual technologies and the overall eVACUATE solution so that privacy and data protection are embedded in these technologies from the outset.

As the project has been progressing since the delivery of the initial framework, further specifications as to the legal requirements and their application to the technological developments within eVACUATE are needed. Moreover, the results of additional tasks need to be reported as well, namely research on the topics related to the exchange of environmental and (geo) spatial data (e.g. the INSPIRE Directive).

D11.2 will thus focus on the following topics:

1. Discussion of the applicable law and legal basis for processing of personal data in emergency cases, as this is the focus of eVACUATE.

   That section examines whether Directive 95/46/EC on processing of personal data in the EU is applicable in emergency cases. Then it studies which of the existing legal bases in Directive 95/46/EC for processing personal data could be used in emergency cases. The discussion takes into account also the changes that the proposed General Data Protection Regulation and the proposed Directive on data processing in the law-enforcement sector could bring about. It also considers Directive 2002/58/EC on privacy in electronic communications, the Charter of Fundamental Rights of the EU (CFREU) and the European Convention of Human Rights (ECHR).
   The discussion reveals the complex picture of personal data processing in emergency cases in the European Union. Directive 95/46/EC excludes from its scope data processing, e.g. for law-enforcement and public safety and security purposes, which means that it would not apply in these cases. However, if the Proposal for a Directive on personal data processing in the law-enforcement sector is adopted, it would cover data processing by the law-enforcement. As regards emergency occasions caused by natural disasters, it seems that Directive 95/46/EC is applicable. The proposed Regulation, which could replace Directive 95/46/EC, refers to data processing in emergency cases. However, it does not provide much clarity on the topic and exhausts it only in one Recital, and does not regulate it in a separate article.

With regards to the legal basis in cases where Directive 95/46/EC applies, the deliverable proposes the legal bases most suitable to be relied on in emergency cases. The correct legal basis will depend on the particular emergency situation, as well as on the scope of rights and obligations of the authorities which are involved in the emergency response. Therefore, every end-user should always consult the national legal provisions to which they are subject. These could stem both from the data protection law, implementing Directive 95/46/EC, and from emergency management regulations to which the particular end-user is subject.
In all cases, the EU Member States are subject to Article 8 ECHR and 7 and 8 CFREU. Pursuant to it, interferences with the right to privacy could be justified only if they have a legal basis for the interference, it pursues a legitimate aim, and if the interference is necessary and proportionate to the achievement of the aim.

2. Analysis and specifications of privacy and data protection requirements, as well as their application to the technologies which eVACUATE is developing or working with:
    - the smartphone application (EVAMAPP),
    - data mining of social networks,
    - chipless RFID tags printed on tickets. As required by the European Commission, a first version of the Privacy Impact Assessment was carried out in order to identify the risks of the RFID technology and propose mitigation measures.
    - video surveillance features, such as software for motion and behaviour recognition.

These technologies are designed to process personal data. The analysis focuses on the data protection and privacy requirements, risks and recommendations which would apply especially when these technologies are deployed in real-life situations. As indicated above, processing of personal data during the research and validation stages of the project is the focus of D11.4. The separate chapters study the question of the legal basis for operating such technologies. Then, guidance is provided as to the data protection procedures that have to be followed when such technologies are operated. For example, when consent is proposed as a legal basis, as in EVAMAPP and the RFID cases, certain information about the data processing has to be provided to the data subjects in understandable manner. The consent must be voluntary, specific, freely-given and informed. As to the legal basis for the video surveillance features and social networks data mining, the situation is less straightforward. The analysis considers as a legal basis Article 7 (f) Directive 95/46/EC, which requires the legitimate interests of the data controller to be balanced against the rights of the data subjects. Again, it must be ensured that the intrusion into the rights of the concerned individuals is necessary and proportionate, as these concepts were explained in D 11.1.

Necessity and proportionality are general principles that have to be considered in all cases. The deliverable does not doubt that the proposed technologies pursue the legitimate aim of assisting the emergency management. However, the analysis from privacy and data protection point of view reveals that these technologies pose certain risks and recommends how they can be mitigated or avoided. These risks could be

common to all technologies. For example, constant surveillance and tracking, lack of information about their operation, usage of the technologies for other purposes, etc. Or the risks could differ per technology. For instance, inaccuracy of the data processed, e.g. in the chipless RFID system, which might not be able to read all tags and thus produces false estimates of the number of individuals at a certain place; or a high number of false alerts of the video technology or non-detection of situations that deserve attention. Another risk could be discrimination, especially in the video analytics case, whereby the algorithms could be based on discriminatory criteria, such as age or other particular features which are not necessarily "unusual," but are culturally and/or situationally acceptable. In general, it is questioned whether the machine can actually automate human judgment/expertise in events detection and whether and in what manner the system can be held accountable for the decision rules/classifications it makes, i.e. for designating the behaviour of a certain individual as suspicious. At the end of the discussion of each technology, recommendations about them are made in light of the rights to privacy and data protection. Such recommendations seek to apply the data protection principles to the particular technology, e.g. data security principle, purpose limitation, accuracy, limited storage, collection only of the minimum data necessary, etc.

When studying the above-mentioned technologies, the deliverable also takes into account that the data they process will be fused via the SOFIA platform and thus they will not function in isolation. Interlinking personal data presents higher risks as it allows interconnections to be discovered between the data and a fuller profile to be made on the concerned individuals. While this information could be helpful to evacuate individuals, it could also be abused. To prevent this from happening, it is recommended to keep the eVACUATE solution *as such* dormant and to activate only those sensors which are necessary in a particular situation. This would also comply with the proportionality principle.

3. Proportionality is further examined in a separate chapter. It studies the proportionality of measures that responders could take to react to an emergency. As these measures could be intrusive, they need to be properly balanced against fundamental rights. Since this balance is not universal, the analysis uses as an example the four scenarios for the final validation demonstrations.

   The analysis of the scenarios does not focus on the proportionality of the proposed response during the research phase, i.e. during the validation demonstrations. It assumes that they could actually happen in real life, i.e. the events and the technologies used could be a real-life scenario. The focus of the discussion is whether the selected technologies would be proportionate in responding to the particular scenarios. Therefore, the analysis does not criticize the technologies *per se*. However, it recommends that certain situations could be resolved through less intrusive technologies. For example, it questions whether it is effective and proportionate to use the chipless RFID system in order to count the passengers around a certain gate at the airport (see AIA scenario in D 2.3), i.e. if the technology is accurate and if this can be achieved otherwise, e.g. through the existing video surveillance technologies. In such a case there is also the question of accuracy – a lot of people have their boarding passes downloaded on their mobile devices. Thus, it

is not certain whether the technology will provide accurate results about the person count. At the same time, it poses higher risks to those who have the chipless RFID tag and whose movements could thus be tracked. When the data from the RFID technology is combined with other personal data from the other sensors, then there is also the risk of identifiability of the concerned individuals.

Thus, the chapter on proportionality recommends that the decision-makers should consider the usefulness of each technology before it is introduced on their premises. In addition, they should carefully assess in each situation whether all the sensors should be on.

4. Last but not least, the deliverable will discuss the existing EU legal regime on the exchange of environmental and (geo) spatial data (e.g. the INSPIRE Directive), focusing on the opportunities and limitations for exchange set out by the framework. Certain Intellectual Property Rights (IPR) such as Copyright issues will also be addressed.

   With regards to the exchange of environmental and geo – spatial data, the deliverable analyses the INSPIRE, the Aarhus and the Public Sector Information (PSI) Directives, which are applicable in the European Union. They do contain provisions on the exchange of data, e.g. between Member State authorities, which could be useful in emergency situations, such as information on addresses, transport networks, buildings, human health and safety; industrial production sites; or weather conditions. The analysis focuses on the conditions for exchange of such information, i.e. what the opportunities and the hindrance to the exchange of this information under the Directives are. While these Directives provide a framework for access to this information and/or its exchange, there are certain restrictions, such as intellectual property rights and licenses. While such restrictions could be overcome of certain procedures are followed, this is not always easy in emergency cases. In the case of INSPIRE, for example, there have been certain initiatives that tackled the question of exchange of data in emergency cases. However, the focus of the working group was the exchange of data from the Member States to the EU. Similar guidelines are needed for situations when Member States exchange data between each other in order to allow the efficient disclosure of the data within limited period of time.
   Last but not least, the proposed technologies for emergency management could have certain implications with regards to IPR and Copyright issues. These rights more specifically have an impact on the use and exchange of incorporations of data that embody an intellectual property protected result of efforts (e.g. the use and exchange of a digital copy of a map that embodies the copyright protected intellectual creation involved in developing the symbols used on the map). The chapter analyses the applicable framework/conditions for the exchange of intellectually protected data.

The depth of the legal analysis of the above-mentioned points reflects the state of technical progress of the eVACUATE project at the moment of the writing of the deliverable. As the technical elements are still under development and have not been finalized, the current deliverable analyses the present state of the art of the eVACUATE technologies. Further

specifications, recommendations and discussion from a legal point of view will be reported in deliverables D 11.3 and/or D 11.5 in M36.

This deliverable will not focus on the privacy and data protection requirements that apply to the partners when they work with personal data in the course of their research activities. This is the focus of Deliverable "D11.4 Ethical and legal evaluation report and recommendations," which is submitted at the same time as the present deliverable. The need for clearer instruction on how to work with personal data in the research domain during eVACUATE has been indicated by the partners and therefore Deliverable 11.4 will handle this topic. Thus, Deliverable 11.4 will provide an overview of the application of the legal framework to the research activities in eVACUATE and recommendations for the future work within eVACUATE will be made.

1. Introduction

From a privacy and data protection point of view, the following deliverable looks at the eVACUATE solution through the lens of the risk of surveillance of citizens. The deliverable does not seek to challenge the chosen technologies *per se*. Indeed, they could be helpful in emergency situations. However, they bring along certain risks that need to be properly addressed in order to avoid negative impacts on citizens.

Surveillance in society can take several different forms. For example, in the case of eVACUATE surveillance can be online, e.g. through social networks data mining; it can happen through tracking of people, e.g. through the location of smartphones and chipless RFID tags; it can be realized through video surveillance – CCTV cameras, thermal and hyper-spectral sensors. These are some of the technologies that form parts of the Smart Spaces in eVACUATE.

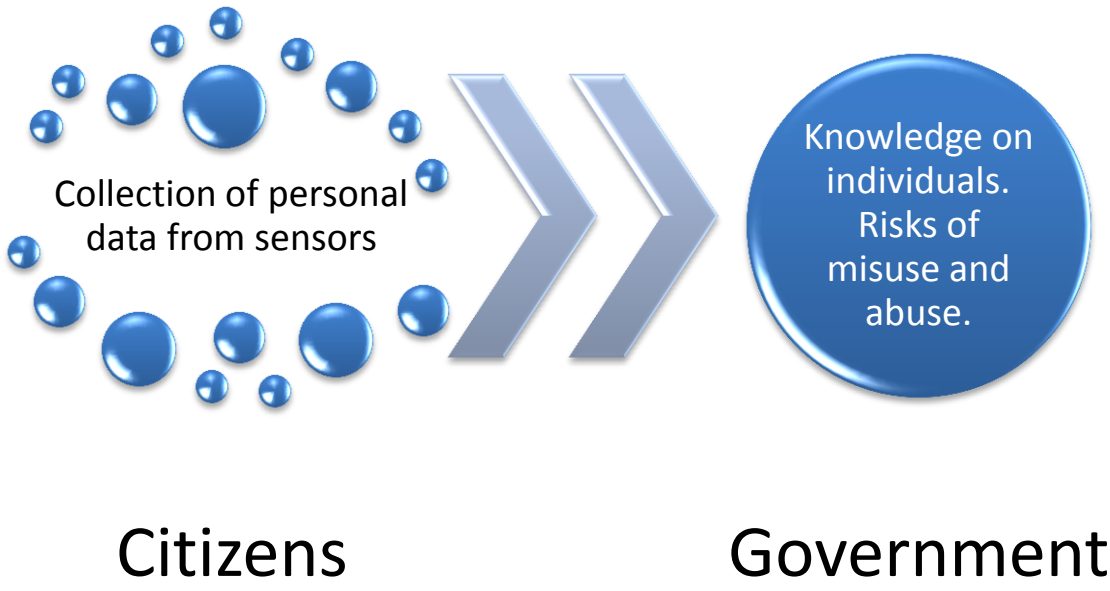

Figure 1: Risks of abuse of citizens' data by public authorities

While it is hard to dispute that the above-mentioned technologies can be useful in preventing and/or responding to emergency cases, they hide certain privacy and data protection risks for citizens. This is the case especially when all of them are used simultaneously to collect and further process citizens' personal data and the input from all of them is interlinked. Therefore, before these technologies are further developed and deployed in practice, they should fully take into consideration the EU privacy and data protection framework. In particular, the principles of necessity and proportionality should be respected in order to avoid a situation where the eVACUATE solution is used to subject ordinary people (moving in a crowd or individually) to constant, permanent and intense surveillance when the situation at hand would not necessitate it. This would be the case when no immediate and genuine threat has been identified but all sensors are on and yet all sensors are switched on and collect and further process personal data. For example, while it could be useful to have means to observe what is happening on end-user premises, which can be achieved through

video surveillance, it would not be necessary and proportionate to track all individuals who have downloaded the EVAMAPP at all times. The latter could be useful if someone is declared missing and needs to be rescued. It is reminded that the eVACUATE solution entails the fusion of all personal data into one platform, which is not currently the case and which raises additional risks, e.g. better tracking opportunities. Thus, the end-users of the eVACUATE solution are advised to assess which sensors they need to have running on a case-by-case basis, depending on whether they need certain personal data or not.

As a recap from D11.1, this deliverable reminds that citizens do not lose *per se* their right to privacy in public spaces. Therefore, their rights to privacy and data protection should not be unduly interfered with. Thus, safeguards for citizens should be put in place when citizens are being surveilled. The reason why surveillance could have negative consequences on individuals is that it enables the collection of information concerning them, which allows one to gain knowledge on individuals that can be held against them if misused and abused (see Figure 1).

This becomes the more possible when the input from all sensors is interconnected, which permits the fusion of data and its interconnection. Interconnection and data fusion in eVACUATE is made possible through the SOFIA platform. *Thus, one of the main recommendations concerning the eVACUATE solution, when it is used in real-life situations, is for the end-users to keep it as a dormant system when the personal data which the solution processes are not needed by the decision-maker. This is also in line with the data minimization principle. Pursuant to that principle, the eVACUATE technology should process only the minimum data which is necessary on a need-to-know basis. What is considered necessary depends on what data the individual technologies process, on the particular situations and scenarios, as well as on how the information the technologies process is merged in SOFIA. For example, for identification of possible emergency situations end-users could rely on their existing technologies and practices, unless they demonstrate that the existing technologies (e.g. the CCTV systems in place) are not sufficient in a particular situation. Thus, the eVACUATE solution should be designed in such a way that the sensors connected to it can be switched on or off by the decision-maker, depending on the necessities of the situation. In this way it can be ensured that eVACUATE does not allow the collection, storage and interconnection of all the collected data from one venue when that would not be necessary for the purposes of responding to an emergency.* Thus, for proportionality purposes, the interconnection should be avoided until the situation necessitates it.[1] To this end, purpose limitation, data minimization measures and proper data access control measures could be implemented. Further guidance on the right balance will be provided to the partners and end-users in the developments of the technology.

[1] DYVINE, Deliverable 5.2, "Final Version of Legal Issues," 7 March 2008, hereinafter "DYVINE D5.2."

2. Applicable Law

D11.1 briefly discussed the issue of applicable law and legal bases for personal data processing in emergency cases. The present chapter makes further comments relevant to the discussion.

Directive 95/46/EC on personal data processing excludes from its scope processing of data for such purposes as public and national security, law-enforcement, etc.[2] Still, in eVACUATE, the emergency evacuation could be caused not only out of public or national security breaches, but also out of natural disasters, in which case it can be assumed from Article 3 (2) that Directive 95/46/EC would apply. This means that in the context of eVACUATE, Directive 95/46/EC could sometimes be applicable (e.g. earthquake), while some other times it might not always apply (e.g. a very serious criminal threat). While the latter case might not fall under the scope of the Directive, often national laws, which contain similar provisions as the Directive, regulate the processing of data in such cases and therefore it is worth considering the principles and requirements of Directive 95/46/EC.

It is noteworthy that Directive 95/46/EC is currently under review. It is expected to be replaced by the Proposed General Data Protection Regulation once it is adopted and enters into force, which is expected to happen in 2015 or 2016. Recital 59 of the General Data Protection Regulation Draft (as originally proposed by the Commission) refers directly to data processing in the context of natural or man-made disasters. It provides that restrictions on certain data protection principles and rights could be justified for purposes amongst which the protection of human life, especially in response to *natural or manmade disasters,* or activities in the *criminal law* field. It looks like, however, that such restrictions should be enshrined in Union or Member State law first. In addition, they may be applied only as far as these laws respect the principles of *necessity and proportionality* and fulfil the requirements of the ECHR and CFREU. Thus, this provision could be interpreted to mean that a certain law should exist to regulate these restrictions and the situations in which they could apply. It could also be derived from the text that an emergency situation might need to be formally declared before the measures apply.

With regards to situations where personal data are processed for law-enforcement purposes, e.g. a terrorist offense, the Commission proposed in 2012 a Directive on the processing of personal data for purposes of prevention, investigation of criminal cases. This Directive would contain, when it enters into force, expectedly in 2015 or 2016, similar principles and provisions as the current Directive 95/46/EC, thus effectively making applicable most of the provisions of Directive 95/46/EC to the criminal law field. In any case, already Council of Europe Convention 108 from 1981 on automated personal data processing applies to any processing of personal data, including the criminal law field. Also, Council of Europe Recommendation (15) from 1987 applies to processing of data in the police sector, and it warns that personal data should be processed only when there is an *imminent and real threat* to public security or once a *serious crime has occurred*. In principle, all the EU Member States are signatories to these Council of Europe legal acts.

Finally, it should be reminded that Article 8 ECHR on the right to privacy applies in all cases. It requires that any intervention with the right to privacy should (1) be based on a law, which

[2] Article 3(2) Directive 95/46/EC

is accessible and foreseeable, articulated with sufficient precision to allow individuals to regulate their conduct;[3] (2) pursue a legitimate aim; and (3) it should be necessary and proportionate to the achievement of the legitimate aim, i.e. it must respond to a pressing social need and be the least intrusive measure.

Therefore, in the context of eVACUATE there is a myriad of sources on privacy and data protection requirements, which need to be observed. The focus of the deliverable will be the European level legislation, i.e. EU and Council of Europe provisions. However, each prospective end-user should also consult their national data protection laws, implementing the EU legislation. In general, the principles of purpose specification, necessity and proportionality apply in all cases and need to be duly observed. In addition, national and regional provisions on emergency and disaster management also need to be consulted in advance, so that the powers of the end-users to process personal data are clarified. As these provisions are a matter of national law, they will not be examined here. They should be considered by each end-user of the eVACUATE solution.

Legal basis

As explained in Deliverable D11.1, in the EU the processing of personal data and other interferences with the right to privacy should have a legal basis, as required by Article 7 Directive 95/46/EC (for the cases when the Directive applies), Article 8 ECHR and Articles 7 and 8 j 52 CFREU. The list of possible legal grounds for processing of personal data as per Article 7 Directive 95/46/EC was discussed in D11.1. It is important to mention here that neither of these provisions *explicitly* refers to processing of personal data in emergency situations, which is the very focus of eVACUATE.

As to the ECHR and CHREU, amongst the legitimate aims in Article 8(2) ECHR that could justify interferences with the right to privacy, are the aims of ensuring public safety, national security and the prevention of disorder and crime. However, these aims have to be achieved through means that are necessary and proportionate to the particular aim and situation. In addition, such measures should be based in a certain law, e.g. an emergency response law. Articles 7 and 8 j 52 CFREU contain similar requirements.

The only explicit reference to emergency cases was found in the e-Privacy Directive. Article 10 (b) of the e-Privacy Directive provides an exception which could apply to organizations handling emergency calls and *recognized as such by the Member State*, e.g. law enforcement, ambulance, fire brigade. To respond to such calls, these organizations may process the location data of callers and override the elimination of the presentation of calling line identification on a per-line basis. The condition is that the Member State has provided transparent procedures for the provider of a public communication network or/and publicly available electronic communications service (e.g. telecom operators) to actually allow for these exceptions. Such procedures and the beneficiaries of the exemptions, however, are a matter of national regulations and thus may not be uniform across the EU. In addition, the purpose is limited – namely responding to such calls, which could mean that a citizen should initiate the contact with these authorities first. It seems to exclude such processing of personal data as data mining of social networks and general tracking of citizens' location.

[3] ECtHR, *MM v United Kingdom*, Appl. No. 24029/07, 13 November 2012

As mentioned above, Directive 95/46/EC provides a number of legal bases. Article 7 of that Directive requires that there must be at least one ground for the processing. Some of the legal bases in Article 7 will be discussed below from the view point of their applicability to emergency cases:

- Explicit, specific and informed consent of the data subject (Article 7 (a)). Consent might not be always possible in emergency cases as certain measures are taken immediately, without individuals being aware of them, e.g. in the case of social networks data mining. Consent could be a legitimate ground in the case of the smartphone app, where the individuals are informed of the usage of their data through the app (e.g. location data if the owner of the device is missing after an evacuation) in advance and give their consent for this future operation. It can also be applicable in the case of chipless RFID tags where the individuals can decide whether they wish to have the tag printed on their ticket or not. This would be the most likely legal ground during the validation demonstrations at the end of the project when volunteers are invited to participate and let the eVACUATE project process their data. Consent is also one of the possible legal bases for processing sensitive data, e.g. health related data (Article 8 (2) (a)).
- Processing is *necessary* to protect the vital interests of the data subject (Article 7 (d), Recital 31). This provision could be relied on as a legal basis if it is accepted that the protection of vital interests includes saving one's life, i.e. it is question of life and death or serious injuries.[4] While this provision reads like a good candidate for a legal basis, it is not immediately clear whether it can always be used in emergency cases. It would sound logical if it is used to find missing persons after disasters.[5] It appears, however, not to be sufficient before a disaster has actually happened or there is no immediate threat to the life or health of the data subject.[6]
- Processing is *necessary* for a legal obligation to which the controller is subject (Article 7 (c)). First of all, the controller must be clearly identified, i.e. the exact institution, department and officials that will actually use the eVACUATE system in real-life situations. This should be done by each end-user who decides to use the solution in real-life situations. The exact and specific obligations of the controller must be clearly and narrowly stated in a binding EU or Member State law. This law must comply with the data protection law, especially respecting the principles of necessity, proportionality and purpose limitation. Last but not least, the legal obligation must specify clearly the nature and object of the personal data processing and should not leave the controller undue discretion as to how to comply with this obligation.[7] It must be thus clear whether the obligation covers the particular data processing.
- Processing is *necessary* for the performance of a task in the public interest or exercise of official authority (Article 7 (e)). As in the other legal basis, necessity must be motivated. The task should fall within the institutional function of the

[4] Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC," adopted on 9 April 2014, p.20; hereinafter "Article 29 WP Opinion 06/2014."
[5] DYVINE, D5.2.
[6] Article 29 WP Opinion 06/2014, p.20.
[7] *Ibid*, p.19-20.

authority which carries it out and it must be related to the public interests. For this, the controller must be identified and their competencies established.[8]

- Processing is *necessary* for the purposes of the legitimate interests of the controller (Article 7 (f)). This provision requires a careful balancing between the interests of the controller and the fundamental rights of data subjects, such as privacy and data protection. To this end, the interest of the controller should be clearly articulated to allow balancing. In addition, this provision does not give a blanket permission to re-use and further process publicly available data, such as information that individuals post on their social networks profiles.[9] The balancing required under this provision aims at ensuring that the processing of data under this article pursues a legitimate aim and that for the achievement of this aim, the measures taken do not go beyond what is necessary to achieve the purpose and thus the disadvantage caused to individuals is only the minimum necessary.

Conclusion

The discussion of the legal basis reveals a very complex situation concerning the legal basis for personal data processing in emergency cases. In principle, it can be recommended that the EU framework should better address the issue of legality of processing in such cases. However, this is also a matter of national data protection laws, emergency laws and emergency powers. Thus, every potential user of the eVACUATE solution (e.g. every institution, department, official) should examine the legal framework (e.g. specific data protection requirements to which they are subject or other provisions stemming from the applicable emergency management legislation) in which they are allowed to operate and whether it covers the particular data processing and if yes, under what conditions. In any case, principles such as necessity and proportionality have to be always observed.

[8] DYVINE, D.5.2.
[9] Article 29 WP, Opinion 6/2014.

3. Chipless RFID System

System description

One of the technologies under development in eVACUATE is the chipless-RFID system. The chipless RFID system is composed of the chipless RFID reader and the chipless RFID tag printed on tickets, e.g. football tickets, metro tickets, boarding passes and cruise ship ID cards. The chipless tags could be used to identify a limited number of different categories of user groups, e.g. disabled, children, pregnant. This would happen by coding every category with a number, e.g. 1 – child, 2 - pregnant, etc. As the chipless tag itself cannot store any information, to recognize which category the ticket belongs to, the tag on the ticket will be tied to one of the numbers, associated with a category.

The tags will be read by special RFID tag readers, known as chipless RFID readers. These chipless RFID readers are placed on the end-user premises as a subsystem belonging to the eVACUATE framework. When the chipless RFID reader reads a particular tag, the information read, i.e. the category to which the user belongs (child, pregnant woman), as well as the time and place of reading, will be sent to the SOFIA platform, where it could be stored for a certain time.

Legal basis for the processing

As discussed in D 11.1, such information as “disabled” or “pregnant” is considered as sensitive data (Article 8 Directive 95/46/EC) and thus enjoys a higher level of protection under the EU data protection regime. Even though the tag itself will not contain further personal data, it is enough that it is carried by an individual. This individual could potentially be identified through other sensors that form part of the eVACUATE solution, such as the video cameras. To process such data, it is important to respect one of the legal bases in Article 8 of Directive 95/46/EC.

The most suitable legal basis for processing of such data in a *research context*, such as the validation demonstration in eVACUATE, could be consent (Article 8 (2) (a) Directive 95/46/EC). However, in certain EU Member States consent may not be used as a legal basis to process sensitive personal data and thus consent may not be suitable legal basis. In any case, the consent has to be given explicitly, i.e. it should not be presumed and the individual should take a positive action to give his consent.[10]

As concerns the legal basis for the processing of such data in *a real-life situation,* it is recommendable again that the individuals (e.g. metro, airport and cruise passengers, football spectators) are given the opportunity to choose whether they would like to have a chipless tag, which will place them in a specific category, or not to have such a tag. Providing the individuals with two alternatives – a ticket with or without chipless RFID tag, would respect the requirements to provide explicit consent. Thus, for example, at a metro station the metro users could be asked whether they would like to have the chipless RFID tag if yes, select which category of data they would like to have printed.

Information to the data subjects

[10] Article 29 Working Party, “Opinion 15/2011 on the definition of consent,” adopted on 13 July 2011, p.24.

Before the data subjects give their consent, however, they have to be given information at least about the data that is going to be processed, for what purposes the data will be processed, in which manner and by whom (i.e. who the controller of their data is) and about how individuals can exercise their rights (to access their data, have it rectified, blocked or erased). This information has to be provided in *understandable* manner. For instance, it can be provided on the screen of the ticket machine, after which there can be "accept" and "decline" buttons. The information could also be provided on leaflets at the disposal of the travellers. Suitable ways of providing the necessary information in the context of the cruise ship, the airport and the stadium have to be defined. For example, the information can be provided on a sheet of paper which can be signed by those individuals who consent to having such a chipless RFID tag on their football tickets, cruise ship cards or boarding passes.

Consent would also be the recommended legal basis when RFIDs are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure.[11] In that case the e-Privacy Directive would apply, according to which when location data other data than traffic data are processed, the processing must be based either on consent or the data should be anonymized.When data are made anonymous, this means that it must be impossible to identify the individuals, taking into account the personal data processed through the whole eVACUATE system.

Privacy Impact Assessment (PIA) of eVACUATE chipless RFID system

As discussed in chapter 5.4.3.1. of Deliverable 11.1, before RFID applications which process personal data are launched, a Privacy Impact Assessment (PIA) should be carried out. The purpose and methodology of the PIA was discussed at length in the same chapter. In this chapter an initial assessment of the eVACUATE chipless RFID application will be made. It will be further elaborated upon in Deliverable 11.3 [M 36] as the RFID application is still under development and thus a complete and finalized PIA cannot be carried out at this stage.

As explained in D 11.1, the purpose of the PIA is to *identify and mitigate the privacy and data protection risks* that the designed RFID application poses.

Before that it has to be identified what type of PIA has to be carried out – Level 1 Small Scale PIA, Level 2 Full Scale PIA or Level 3 Full Scale PIA. To determine the exact level, the decision tree below, endorsed by the Article 29 WP, was followed:

[11] Recital 56 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, L337/11-36, 18.12.2009.

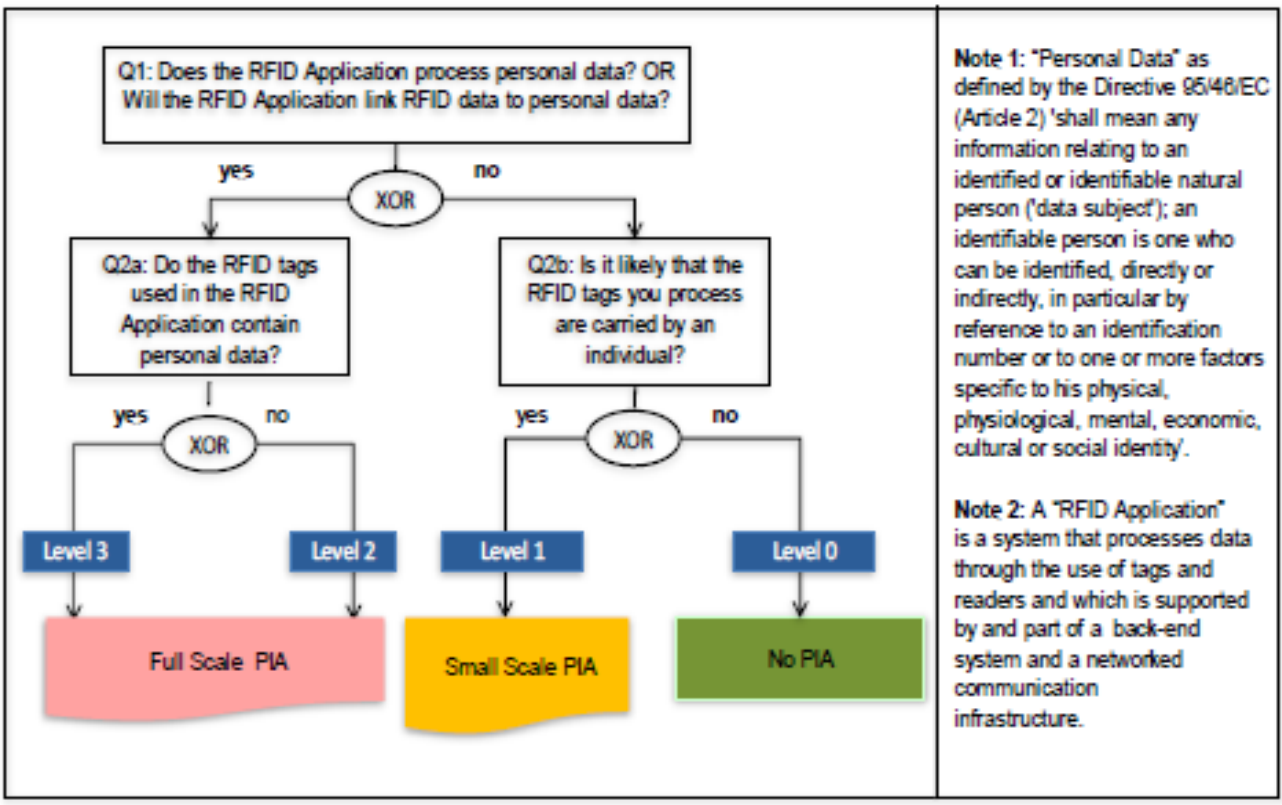

Figure 2: Decision-making tree (as proposed by industry and endorsed by Art. 29 WP

According to the current description of the chipless RFID application, provided by TU Dresden, the tags will refer to personal data (such as sensitive health data) and they will be carried by individuals. Thus, according to the tree above, a Full Scale PIA would be necessary. Even though the names of the individuals carrying such tags will not be stored on this chipless RFID application, the risk of identifiability of the individuals remains as the information from the chipless RFID application can be linked to other data on the individuals through the SOFIA platform.

Before the risks and their mitigation measures are identified, the application should be first well described. The description is provided at the beginning of the section. In addition to the information provided there, the declared purpose of the application is to obtain information about the number of for example (a type of) disabled people, pregnant, or children on certain premises and who would need special attention in cases of emergency evacuations. The chipless RFID system does this by providing to the eVACUATE framework the number and type of persons that have crossed through a particular position (the RFID reader) at the end-user venue. However, for this to be effective, the system should be able to read the direction of movement, so that an accurate number is provided. It would be also useful to know how the individuals who need special assistance can actually be located during a crisis. It is argued that the purpose of the application is not to track the specific location and movement

of individuals within the premises (although this could become practically possible if readers are placed at short distances and the there is only one person that belongs to a certain category, then his trajectory could be derived from the RFID application). It also does not seek to identify the persons carrying the chipless RFID tags. The information on which category the person belongs to will not be combined with other personal data printed on the tickets. One can take as an example the case of a chipless RFID tag included in a football ticket. In such scenario, the information available on this chipless RFID tag cannot be related to or combined with the names of ticket holders printed on the ticket itself. However, it can be combined with information such as CCTV images, or mobile phones applications.

For this reason, from a data protection perspective it is recommended that the information extracted from the chipless RFID application is automatically deleted from SOFIA as soon as it is not needed any more. This deletion period should be determined on a case-by-case basis for the different scenarios. For example, in the case of the metro, as soon as persons have exited the metro station, their RFID information should be deleted. It is assumed that there will be readers at both entry and exit and therefore when a certain chipless RFID tag is read at exit, it should be known that the person carrying it has exited the premises and therefore the record in SOFIA should be deleted. The technical partners need to determine how to ensure timely deletion of the data at every end-user location, depending on where readers will be placed and depending on whether an emergency has occurred or not. The general principle is that as soon as the data are not needed any longer, they should be deleted immediately.

The figure below contains the first draft of the PIA, i.e. the risks and necessary mitigation measures:

List of risks	Likelihood of occurrence	Recommended mitigation measures
The security of data, processed by the chipless RFID system could be compromised, e.g. skimming, eavesdropping and/or hacking.	High	Measures of secure the communication of the data through the chipless RFID system and to secure the storage of the data, e.g. on SOFIA. As the Commission has recommended, "… privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy-by-design')."[12]

[12] Recital 6, Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200) (2009/387/EC) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF

Accuracy of data: - **Tickets might be bent and tags are not correctly read** - **Reader cannot read all tags if a lot of people passing through at the same time**	High	Further research is being done in order to remedy this problem.
Tracking – processing of location information (many readers, which provide opportunity to track individuals' movements). Especially problematic if location data is saved all the time and if there is only one individual falling into a certain category.	High	Not placing readers at many locations but only at entry or exit, and not saving location data, but knowing only the last known location (if this is necessary for the purposes of the application).
Incomplete information or lack of transparency about the application (individuals not informed their tickets contain the sensitive info or on the purpose and use of their information, e.g. when the info will be read and used)	High	Placing easily-understood information before tickets are purchased about the RFID tags (on method and purpose of processing of data and controller) on information notices when tickets purchased at a ticket office on ticket machine screens.
Lack of consent (individuals forced to have the RFID tag)	High	Providing opportunity for consent – boxes on the screen that a person consents to having the tag and which category of tag they want? Same option when individuals purchase tickets at a desk.
The data processed via the application can be used for other purposes than identifying the type and counting the number of individuals and responding to an emergency: End-users might decide to use the data for other purposes and at times when no emergency has occurred and give access to the data not only to officers responsible for emergencies.	Medium	Strict data access control and purpose limitation in the internal policies of the end users
Tags can be read by other readers outside the premises of the end-users	Low	To be defined
Data not erased but stored permanently	High	Not storing data or storing only last known location (this is tied to the question whether it is necessary for the purposes of the application to store any data on when and where the tag was read). Systematic deletion of data.
Combining data from the chipless RFID system with data from other	High	Ensuring the data are not interconnected unless an

sensors (e.g. CCTV) all the time (i.e. outside emergency situations)		emergency has occurred and there is a valid legal basis for this interconnection.

Figure 3: List of risks and proposed mitigation measures for the eVACUATE chipless RFID system

Conclusion and recommendations

Thus, the analysis concludes that there are a number of risks related to the chipless-RFID application, as discussed in the table. Therefore, it is recommended that in the coming months further work needs to be undertaken on the mitigation measures as indicated in the table above.

Last but not least, when launching the RFID application, especially in real life situations, the Commission has recommended that a policy on the RFID application is drafted and published by the end-users in real-life situations:

"Without prejudice to the obligations of data controllers, in accordance with Directives 95/46/EC and 2002/58/EC, Member States should ensure that operators develop and publish a concise, accurate and easy to understand information policy for each of their applications. The policy should at least include: (a) the identity and address of the operators; (b) the purpose of the application; (c) what data are to be processed by the application, in particular if personal data will be processed, and whether the location of tags will be monitored; (d) a summary of the privacy and data protection impact assessment; (e) the likely privacy risks, if any, relating to the use of tags in the application and the measures that individuals can take to mitigate these risks."[13]

This could be done by each end-user before launching the RFID application in real life.

Recommendations to the chipless RFID system:

- The purposes of the chipless RFID system should be clearly specified and its functionalities should correspond to the declared purposes.
- The system should be based on the consent of the users also in real life situations (e.g. metro passengers).
- Before the consent is provided, the prospective users should be given information concerning the controller, the purposes of the system and the data it will process, as well as the rights of individuals.
- The processing of the data should be kept secure at all times.
- The data processed should be accurate, i.e. the count of individuals (if this remains its purpose).

[13] Par. 7, Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200) (2009/387/EC) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF

- The information collected by the system should be regularly deleted in order to avoid constant tracking of individuals. The storage period of the data should depend on the purposes of the system and on the individual end-user (to be further specified).

4. EVAMAPP

EVAMAPP

Another technology under development is the smartphone application, the so-called EVAMAPP. EVAMAPP could be offered to the visitors of the end-user sites, e.g. cruise ship, air and metro travellers, as well as stadium spectators. However, it is initially foreseen to be fully developed specifically for the cruise ship, as the specifications in terms of its use can be elaborated. **Therefore, the following legal analysis of the EVAMAPP will use as an example the cruise ship context.** Although the app could be adjusted to the other scenarios/end-user sites, this is under discussion at the time of writing the deliverable. In case such an additional app is indeed developed, it could be analyzed in the next version of this deliverable (D11.3). The app would be open for use by the general public, including the elderly, disabled and children. It is also contemplated to design and offer another smartphone app used primarily by first responders/staff members at these sites. The functionality of this staff app is expected to be centred around dispatching crew members, e.g. "please check on Mr. X. in room 123," and managing the crowd at the passengers' assembly stations, e.g. using the app to report how many passengers are present and which ones are missing.

In terms of privacy and data protection, both types of apps (i.e. for the public and for staff) raise similar concerns. If the necessary data protection measures are not taken, there is a risk of constant location tracking, collection and storage of large amount of data on the users of the app and those individuals whose images might be recorded through this app and the re-use of this data for incompatible purposes, such as marketing, etc.

High-level description of EVAMAPP

The purposes of the EVAMAPP and its functionalities, according to the developer of the app TELESTO, would be numerous. It could be used before the event/outside the venue, during the event/on the premises, and during crisis. The "Emergency Number option will be available at all times. The purpose of offering the app before the event is to provide information about the venue, e.g. a map of the premises and its facilities, safety and security procedures, as well as important phone numbers. Once on the premises, the user would be able to view, in addition to the information above, the nearest safety/security location and other security information relevant to his position. Furthermore, the user would be able to view the safety status of the venue to know whether there is an incident or not.

In emergency cases the app would offer all the above-mentioned functionalities. In addition, it might process the location of the users by sending it to the EOC for *emergency assistance purposes only* if the individual is *reported missing* and only if the user has provided his *prior consent* for this operation and they have not revoked it yet, and if their smartphone is still operational and the EVAMAPP application is activated. The location would be tracked via Bluetooth Low Energy (BLE) continuously emitting beacons (also called "iBeacons") that assist the application to determine if it is in the proximity of one or more beacons. The application continuously monitors for BLE iBeacons and (if needed for safety purposes) communicate to the EOC the location data of those individuals who have downloaded EVAMAPP.

The app would also provide the users with instructions on how to evacuate by informing them of the active evacuation route (alternative methods would include textual indications, 2D view) depending on their location. The app will also help the users find the nearest rescue resources that might be needed during the crisis. In these cases the location information will not be duplicated and disclosed to others.

The app could also allow users to send predefined or user defined text messages and audio-visual material to pre-defined recipients, e.g. first responders, and report their status, i.e. whether they are safe or in need of help. They would also be able to take pictures/videos of their surroundings and send it to the responders via the app. In case the app is not running, push notifications could be sent to the users if they have given their consent for this prior to downloading the app or at any point in time from the settings of the application.

TELESTO has explained that all interactions with the users will be recorded for testing the application and training the personnel in the emergency operation centre, thus ensuring that the info is not misused and that timely, valid information is sent to the users at all times. The data could be used for training purposes both during the validation demonstrations phase and in real life situations.

In case the users feel very sick at any time during the cruise, not only during emergency, they will have the opportunity to press the emergency button. Then, the app would acquire their location, sense their motion parameters (whether the user is stationary or is moving), the ambient temperature, humidity and pressure of their environment.

A survival kit would also be provided in this app. In addition, there will be separate sections with information for the disabled (e.g. ramps and elevators for accessing the assembly stations).

There is also a suggestion that in the case of the cruise ship the app could have the functionality to help people to find their rooms in normal, everyday situations, as well as to provide information about the entertainment events on the cruise ship. This opportunity is considered to offer numerous benefits, both to the commercial exploitation of the eVAMAPP, as well as to incentivize the passenger to download the application before the actual crisis.

It is planned that the EVAMAPP for crew passengers will be connected to the passenger cruise ship database (maintained by the cruise ship “Hospitality Information System”/ HIS). In the context of eVACUATE, this HIS would be the FIDELIO. It normally contains such information as the names, the cabin number, the travel document details, date of birth, family members on board, payment data, disability information, etc. Once on board the individual user will be issued a unique identification number (UID), to introduce to the mobile application the first time it is used. Thus UID will enable the connection between a certain smartphone and the personal information of a passenger contained in FIDELIO.

It is planned that the transaction between the system and the application will be logged.

When someone is directed to their rooms (in normal situations) or to the mustering station in emergency situations, their location data (and their movements) will be processed in the back office system. Thus, if a crew member wants to retrieve the location of someone and track their movements, they would be able to do so by accessing the back office part of the eVAMAPP application.

4.1. Legal analysis

4.1.1. EVAMAPP for passengers

Information and consent

As it has become evident from the description above, the proposed smartphone app would be designed to store and further process different types of information, amongst which *personal data of the users* (e.g. location data, a unique identification number, the MAC address of the terminal device) and *of the people around the users* (e.g. images of people who are recorded through the app). Therefore, the requirements of Directive 95/46/EC and of the e-Privacy Directive need to be considered.

Article 5 (3) of the e-Privacy Directive applies in cases when *any information*, i.e. *not only personal data*, is stored on or retrieved from the terminal device of the user. It requires that the *consent* of the user must be obtained first, which would give the legal basis for the storage and further processing of information on the device. Consent for the processing of personal data is required by Article 2(h) Directive 95/46/EC.[14]

Before the users are asked to give consent, they must be provided with clear and sufficient information about the placing and retrieving information through the app.[15] The requirement for consent, which is free, specific and informed, also applies in the case when apps process personal data.[16] Therefore, prior to downloading the app, the user should be provided with an information notice about the app. This information can be included in the description of the app, for instance, where the app developer is free to enter information. This could satisfy Article 5 (3) of the e-Privacy Directive. As recommended by Article 29 Working Party, before the app starts processing personal data of the user, the user should be given the opportunity to give his consent for each separate data processing operation of the app, including the personal data processed during installation. This can be done by offering individuals the opportunity to press an "I accept" button after they have read the information concerning the processing of their data. Thus, the consent would be granular, i.e. specific, and also informed.[17]

Before the app begins to process personal data, the following information has to be provided to the potential user:

- Who the controller of the app is, e.g. the safety and security officer of the ship/stadium/airport/metro, their identity and contact details. If there is more than one controller, then the other controller(s) should be mentioned, too. This could be the case with the cruise ship where entertainment information is advertised through the app by certain bars, casinos, etc, and the emergency-related functionalities are offered by the safety/security personnel.

[14] Article 29 Working Party, "Opinion 02/2013 on apps on smart devices," adopted on 27 February 2013, p.14.
[15] *Ibid*
[16] *Ibid*; Art. 2(h) Directive 95/46/EC
[17] *Ibid*

- What each separate *purpose* of the app is and related to that - which *categories of data* will be processed for each purpose. This includes what information might be stored on his smartphone or what information already stored will be accessed via the app. In addition, the information notice should inform the user of how his data will be processed through the app, e.g. that his location might be tracked during search and rescue operations if the individual is reported missing. Pursuant to Article 2 (h) Directive 95/46/EC, the consent should be specific, i.e. it should be given for the processing of data for a *concrete purpose*. Therefore, if the app is used for multiple purposes, such as location finding, entertainment, provision of safety/security or medial information, push notifications, these have to be clearly listed and consent should be given for each one of them.
- Last but not least, information such as to whom what data might be disclosed, how long the data might be stored, and how individuals may exercise their rights to information, erasure, blocking, rectification and objection should also be provided (see Article 10 Directive 95/46/EC).

It should also offer the opportunity to cancel or halt the installation of the app, i.e. the consent must be freely given.[18] Mechanisms for withdrawing consent for the download of the whole app or only from its individual elements, e.g. the location tracking function during evacuation or entertainment information provision, should be available to the user all the time. In addition, there should be mechanisms for *deactivating* the app once the users have exited the end-user venues or while he is on the venue if he wishes to deactivate the app. A reasonable retention period for data collected through the app should be defined, depending on whether there is an emergency or not. If it would be practical for the purposes of the application, a period of inactivity after which the account will be treated as expired could be predefined. If for the purposes of the application any data need to be stored, it is recommended to store the data on the terminal device of the user and not outside the device, e.g. on the COP. The recommendation follows the reasoning that storing data on the device enhances user control. The app should not retrieve/access data from the terminal device of the user of the app which is not necessary for the purposes of the application, e.g. contact list.

Location tracking and sending textual and audio-visual information

As explained above, the back-office part of the app will contain the location data of the individuals, e.g. of those who have requested assistance to find their rooms or need the active evacuation route or of those who are missing. However, collecting, storing and accessing information on the movement of individuals all the time would be disproportionate. Out of proportionality concerns, it is recommended that location data in the case of direction to cabins in normal situations is deleted immediately after the person is directed to their cabin and not accessed by anyone. In the case of emergencies, location tracking should be activated when an evacuation situation is declared with the prior consent obtained by the user of the terminal device. In addition, it is preferable to store only the last detected location by the iBeacons (or the last known 2-3 locations if the necessity is justified), as the app is supposed to be used to find a missing individual and it is reasonable to assume that only the last known location or last known 2-3 locations could reveal the potential location of the

[18] *Ibid*

individuals. There should be strict access control to the location data of individuals so that it is ensured that this data is accessed only when needed, i.e. to rescue someone with an app who is missing. The iBeacons in principle should not track the location of individuals without the smartphone app either, even if this is technically possible. If their location is detected, it should be immediately deleted.

A situation might arise where a person has not given his prior consent for tracking or has withdrawn it and he is declared missing. In this case accessing his location from the app cannot be based on consent. It could still be possible to access the data in order to rescue someone, potentially on the basis of Article 7 (d) Directive 95/46/EC (protecting the vital interests of the data subject). However, it is recommended that this happens if the responders could not locate the missing individuals through other means, e.g. CCTV, reports from people on the ground (staff members working on the venue), etc.

As to sending textual and audio-visual images to first responders via the app, this functionality should be activated again after the declaration of an emergency evacuation. The reason is that an app user might capture images of individuals around him, i.e. the personal data of other individuals. Since the purpose of the app is to facilitate the reaction *during emergencies*, processing of personal data outside the framework of emergencies risks breaching the purpose limitation principle and lead to disproportionate processing of data. Out of proportionality concerns, this function should not be active during normal situations to collect information on what is happening on board the ship, unless there is evidence that the available resources of a particular end-user are not sufficient to detect incidents and passengers have no other way of reporting incidents they come across. It is understood that nowadays all end-user dispose of cameras where they can observe their premises and see, e.g. fire, or people fighting. Moreover, the eVACUATE solution is supposed to be equipped with video analytics that help the officers behind the cameras find and analyse information. Last but not least, in the cruise ship case there are other ways to inform first responders of incidents. For instance, on the ship there are phones placed on board the ship in cabins and corridors through which individuals can call the safety/security staff. In addition, the app offers a “Call hotline” option where individual can simply call. If calling is not possible for persons with specific disabilities, then texting is an option.

Furthermore, personal information of individuals captured through this function should not be further used for incompatible purposes, e.g. for law-enforcement purposes.

Finally, it is recommended that there are certain blurring mechanisms so that faces of individuals captured can be anonymized, unless they would be deemed necessary to identify a certain individual for rescue purposes. Following that logic, information which contains personal data should be deleted as soon as it is no longer needed for rescue purposes.

Logging of transaction data and connection to the passengers (e.g.) FIDELIO database

While logging of transaction data could be helpful to evaluate the performance of the technology, both in the research context and real-life situations the data should be completely anonymized. SOLAS does not provide requirements concerning recording the communication between the cruise staff and the cruise passengers. Unless there is another legal basis for recording this communication, the data should be either deleted or completely anonymized.

With regards to the connection between the cruise app and the passenger database, TELESTO suggests that passengers register for the app with their unique number as registered by FIDELIO. This number is also personal data as it could lead to the identification of an individual. It should be considered which registration would be more data protection friendly – the registration with the UID or registration with the name. Such databases as FIDELIO contain a lot of personal data, including payment data. If registration via FIDELIO is retained as an option, the app should not have access to any of the information that is contained on a particular individual on FIDELIO. FIDELIO, on the other hand, should not have access to the movements of individuals or any other information processed by the app. Thus, there should be no communication between the app and FIDELIO. If there are missing persons, they can be identified when the ship cards are scanned at the mustering stations and a list of missing individuals is produced.

Environment sensing mechanism when individuals report themselves sick

When individuals report themselves sick, the app will acquire their location, which is also a form of personal data processing and requires a legal basis. It could be consent, given in advance when downloading the app, i.e. consent for processing location data in case the individual feels sick and reports himself as such. As to sensing the environmental conditions such as humidity and temperature, the usefulness of such information should be properly motivated. It is also contemplated to allow this functionality to operate 24/7 in order to detect incidents. However, it should be first assessed whether this function would indeed be necessary to identify incidents and whether it poses high privacy risks to the individuals with the apps. If it is indeed implemented, it should eliminate all risks of identifying from which terminal device the information comes and of tracking the movements of the individuals carrying these devices. It should not be possible to know where someone is and where they are moving, based on the environmental information derived from their devices.

Data security

Security of data processed via the app shall be ensured at all times. Data security means implementing the relevant and appropriate technical and organizational measures to ensure the security of the personal data processed via the app. The requirement stems from Article 17 of Directive 95/46/EC and has been discussed at large in Deliverable D11.1.

Liability for content of survival kit/first aid

The survival kit/first aid information will be provided by the end-users themselves. It is understood that TELESTO will only integrate the content within the app. The exact responsibility for the content should be regulated by a contract between TELESTO and each end – user who provides this information. It is recommended that since the end-user provides the content on the information, they should take responsibility for damages ensuing from any wrongful content, as long as TELESTO is not aware of the inaccuracy/wrongfulness of the information provided by the end-users and integrated it correctly, e.g. did not modify the content.

Recommendations for EVAMAPP before it is put in operation:

- Provide to the potential users during the download *information* about each functionality of the EVAMAPP (e.g. in the description of the app). *Consent* for each functionality (e.g. entertainment, room finding, location tracking, and push notifications) should be obtained before the app begins to process personal data. Mechanisms for *withdrawing the consent* and de-activating the app should be available at all times, including during installation.
- The location of the individuals who have given their consent for *location tracking* should not be tracked in normal situations but only in *emergency cases* when the individuals need to be *rescued*. Thus, EVAMAPP should not store and disclose to the first responders each recorded location but only the last known one of the individuals who are missing as this seems sufficient for the purposes of rescue operations. If more locations need to be stored and disclosed, the *necessity* of such a function needs to be properly *justified*. Location data used for directing passengers to their rooms should be deleted immediately. Access to location data should be strictly regulated.
- The app should not access other data stored on the terminal device of the end-user, e.g. contact list.
- If the app users registers with his cruise ship database ID number (e.g. FIDELIO ID number), there should be no communication (i.e. exchange of data) between the app and the database.
- The *necessity and usefulness* of offering the emergency button which will sense the ambient environment (humidity, temperature) needs to be demonstrated.
- For every use case there must be ways for timely *deactivation* of the app once it is no longer needed, e.g. the passengers have disembarked from the cruise ship or the stadium.
- The data should be *deleted* (e.g. from SOFIA) as soon as they are no longer needed, e.g. immediately after the end of emergency and rescue operations.
- The functionality to capture and send *video images and audio data* should be activated only after an emergency situation has been declared if it is deemed necessary to have such functionality in the first place. It should be considered whether this functionality should be active 24/7 and if yes, it should eliminate all risks of tracking individuals or identifying from which terminal device comes.
- With regards to disclosure of the personal data, it should be disclosed to those individuals only that need the data in the course of their rescue operations, i.e. on a need-to-know basis. Thus, a good access control policy should be implemented by the end-users of eVACUATE.
- When storing and further using the data processed through the app for *training, testing and evaluation purposes*, the data should be properly *anonymized* in such a way as to eliminate the risk of identifiability of the terminal device and its owner.
- *Data security* should be ensured at all times.
- Data subjects should be given the opportunity to exercise their rights (to information, access, rectification, erasure, blocking and objection).
- The liability for safety kit/first aid information should be defined in a contract between the partners that provide the information and TELESTO.

- The end-users of the app should delimit its usage and guarantee that the app will be used for emergency response purposes and not for further incompatible purposes, e.g. law-enforcement.
- Logs of communication between the EOC and the app users should be anonymized.

4.1.2. EVAMAPP for children

The potential group of users of the EVAMAPP could include also children. In that case additional legal aspects to the ones discussed above need to be taken into consideration.

The current legal framework, i.e. Directives 95/46/EC and 2002/58/EC, do not contain specific requirements for processing of personal data of children and do not require parental consent. A valid legal question is, if the app is based on consent, are children legally authorized to give consent? This is in principle a matter of national law.

A further consideration is that children's consent needs to be informed. This means that the information provided to children needs to be adapted to their understanding, which is arguably currently not the case with the existing apps. Thus, some scientists argue that the practice of relying on children's consent cannot be deemed as fair and lawful.[19]

Under the current legal framework, the Article 29 Working Party has recommended that for children to be allowed to download and use the EVAMAPP, the consent of the parents needs to be given, unless consent can be obtained by a minor under the national legislation. It is also the national legislation that defines the age limits for minors and children, which is currently divergent.[20] However, a question remains as to how parents can be involved in providing their consent for their children to use the EVAMAPP.

Under Article 8 of the Proposed General Data Protection Regulation (Proposed GDPR), when children below 13 are offered information society services, then verifiable parental consent would be needed, although the practicality of such an arrangement has been criticized. It is thus argued that Article 8 of the proposed GDPR, which is supposed to replace the current framework, would legitimize processing of data of children and it would be a tool to ensure children's protection in the online environment.[21]

Therefore, when EVAMAPP is offered to children, the age limit should be considered as under national law (after the adoption of the proposed GDPR it would be uniform across the EU Member States, i.e. 13 years). If children are not allowed to give consent under national law, ways to obtain the parental consent should be determined.

4.1.3. EVAMAPP for staff members

The app, as planned, would be necessary to help end-users organize their emergency response by ensuring that the designated officers are at their pre-defined locations. In addition, the app could serve as a means of communication between responders/officers.

[19] Jasmontaite, L. and De Hert, P., "The EU, children under 13 years, and parental consent: a human rights analysis of a new age-based bright-line for the protection of children on the Internet," *International Data Privacy Law 2014.*

[20] Article 29 Working Party, "Opinion 02/2013 on apps on smart devices," adopted on 27 February 2013, p. 26.

[21] Jasmontaite, L. and De Hert, P., "The EU, children under 13 years, and parental consent: a human rights analysis of a new age-based bright-line for the protection of children on the Internet," *International Data Privacy Law 2014.*

It would also be a good practice to inform staff members when they start being tracked at the beginning of an emergency. The usage of the app by the staff members should be clearly delimited to ensure against change of purpose and thus abuse. For example, the app should not be used to track the personnel all the time during their duty and certainly not off-duty or during breaks. It should also not be used to track whether the officers are late for work, etc. This would entail a change in the purpose.

As to the legal basis, in principle consent is not a suitable legal basis in the employment context. A possible legal basis would be the purposes of the legitimate interests of the controller (Article 7 (f) Directive 95/46/EC). This provision, as explained above, requires a careful balancing of those interests, e.g. guaranteeing the efficiency of the evacuation response, and the interests of the employees against excessive intrusion into their privacy. The question here is whether the app as it would be designed is the least harmful means for the employer to ensure that an emergency response is efficiently carried out and thus it is end-user dependent. If the answer is positive, then there must be sufficient safeguards against abuse of the app and against constant tracking and against uncontrolled access to the location data of the employees, e.g. crew staff members.

In cases where staff members are equipped with the EVAMAPP, they should be clearly informed by their employer of the functionality of the app and in what way it could process their personal data. This information could be included in the internal policies of the end-users.

During the 5th Plenary Meeting (2-5 March 2015) in Dresden, it was proposed to have a crew app for the cruise ship crew members. It is suggested that this app be connected to the FIDELIO database, which contains a list of all the passengers and a broad range of their personal data, as explained above. It is understood that currently only the hotel administration has access to the FIDELIO database. When crew members scan the ship ID cards of the passengers gathering at the mustering stations and everyone has gathered, the crew members bring their devices to the hotel, which reads them and generates a list of missing people (based on the FIDELIO database). If the crew app devices are to be connected to FIDELIO, the following safeguards should be implemented: (1) it should be one-way communication, i.e. from the app to FIDELIO and (2) the app should only communicate the names of the individuals whose cards were scanned; (3) crew members should not have access to FIDELIO, but they should receive at the end only a list of the missing individuals. This app should transmit data to FIDELIO only during emergencies. It should be first verified that the connection of the app to FIDELIO would not breach any local or international rules to which cruise ships are subject.

4.1.4. Conclusion

Before EVAMAPP is offered in real-life situations, the recommendations provided in the analysis above should be followed. In addition, before the prospective end-users offer the app to their customers, they should notify their respective national data protection authority.[22]

[22] The Data Protection Authority of the controller of the app.

5. Social networks data mining

Another element of the eVACUATE solution would be datamining of social networks, e.g. Twitter. The declared purpose would be to obtain timely on-site information if an emergency accident has occurred on the premises of the end-user, e.g. that a fire has broken out at AIA. These social networks would be searched using specific search words. When the search is run, the end-user will be able to see only the particular tweets that contain one of the search words. It is planned that the end-user will not be able to see details concerning the profile of the person who posted the particular tweet, such as contact details, previous posts, etc. The end-user who mines, e.g. twitter, will be able to see the alias/name and the profile picture of the one tweeting about the incident of interest to the end-user. If the tweet is a re-tweet, the end-user will be able to see the alias/name of the original tweet as well.

In order to verify whether the twitter account belongs to a reliable author is and it is a real one and not fake or spam, the system would automatically send an inquiry to an influence measurement mechanism called KLOUT. The KLOUT score of a user could be between 1 and 100. The higher the number, the higher the influence.[23]

It is planned that the one doing data mining will be able to see the accurate location of the tweets if individuals use Twitter from their smartphones and have allowed their Twitter client to enable location association with a given message. The purpose of extracting the position is to determine whether the one who tweets is indeed on or close to the premises of the end-user. It is argued that this would help determine the reliability/accuracy of the information posted. However, according to TELESTO, it is not the purpose of eVACUATE to track the particular person who is tweeting. Nevertheless, this could turn out to be technically possible if a user posts a lot of tweets about a certain accident and from this it can be determined how he is moving across and around the airport, for instance.

The only information that will be stored on SOFIA, only in case of an incident and only as long as the information is useful, is the actual tweet and aliases. By contrast, the names, profile pictures and location will be immediately deleted or anonymized if they are being stored for as long as necessary.

Tweets coming from the authorities, e.g. the police, might also be caught by the search engine. In some cases and Member States, the data protection recommendations could also apply to the mining of such feeds.

5.1. Legal analysis

Applicability of Directive 95/46/EC

The operation will process personal data, e.g. location data, aliases and profile pictures of users. These remain personal data even if they are posted in the public domain.[24] Therefore, their processing must respect the data protection framework. It is argued that aliases could be personal data as they refer to individuals who can be singled out even if they are not

[23] https://klout.com/corp/score

[24] boyd, D and Crawford, K., "Six Provocations for Big Data," Paper to be presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 21, 2011, p. 11.

identified. This is considered to be the case with aliases and pseudonyms when they are retraceable, even though the risks for the data subject are lower.[25]

Legal basis

When processing personal data, the controller should have a legal basis for it. For the validation demonstration, the consent of the volunteers could be considered a valid legal basis. However, it is difficult to conceive how in real–life situations consent can be relied upon as a legal basis. One of the possible legal bases is Article 7 (f) Directive 95/46/EC, i.e. the data mining is necessary for the purposes of the legitimate interests pursued by the controller. As Article 29 Working Party has stated, however, Article 7 (f) does not give a blanket permission to re-use and further process publicly available personal data, such as the data published through Twitter. First, the legitimate interests pursued by the controller should be clearly defined. This is necessary in order to answer the question whether indeed social networks data mining is the most suitable way to achieve it. It should be kept in mind that social networks were not created as intelligence gathering or early warning system for disasters. Re-using them for these purposes must be strongly justified. On the question of legitimate interest, it could be argued that ensuring the safety and security of the premises could be such an interest.

This legitimate interest and the chosen means to achieve it should be balanced against the fundamental rights of social network users, such as their privacy and data protection. In the first place, the *necessity and proportionality* of the chosen approach, i.e. data mining, should be strongly justified.[26] The *necessity* of using feeds from social networks has to be motivated by the end-users who should take into account all the available resources they have for detecting incidents. Currently safety and security officers dispose of resources to gather information about incidents, such as CCTV cameras, smoke detectors, officers on the ground, etc. Thus, it has to be proven that the available resources at the end-users' sites are not a sufficient means to collect safety and security-related information before and during an accident, so mining of social networks would have a significant added value to the current situation. When motivating necessity, end-users should distinguish between two stages where data mining of social networks could be used: (i) normal situations and (ii) once incidents have been identified and information could be needed for rescue purposes.

It must be noted that it cannot be guaranteed that the national courts and/or the Court of Justice of the European Union will accept relying on Article 7 (f) Directive 95/46/EC in real-life situations and their interpretation of the case could differ.

Even when the necessity and proportionality of data mining is motivated by the individual end-users, certain safeguards have to be implemented. When a certain tweet is caught by the search engine, then only the message containing information about a possible incident should be extracted. As twitter names could be considered to be personal data, as well as potentially profile photos, they should be anonymized before the messages are further processed. Anonymization of the selected social networks feeds, which will be stored by eVACUATE, should also be carried out on the original tweets when the first responders

[25] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data," adopted on 20th June 2007; Coudert, F. "+Spaces, Deliverable 2.3, Ethical Issues Report," 28 June 2010.
[26] Article 29 WP Opinion 06/2014.

come across a re-tweet. In general, the extracted messages should be used only for the declared purpose, i.e. obtaining information about possible incidents, not collecting evidence for future investigations. It is important also to ensure that in the course of the mining activity data which is not necessary for the purpose is not processed. Such data could be for example the contacts of the individual, their previous posts, pictures, etc.

Location data

The end-user wants to extract the location of the social network user to assess whether they are close enough to their premises in order to know how seriously to consider a certain message. However, location data is also personal data and the necessity of its processing has to be justified. It is worth repeating that security and safety staff have other means of verifying whether there is indeed an incident as might be claimed by a certain tweet – through CCTV, personnel on the ground, etc. In addition, it is recommended that the end-user performing the data mining should not be able to profile or track the individuals whose tweets are of interest. Tracking could be possible if a certain user posts numerous tweets from numerous locations and his location data are kept and associated with his particular profile.

Using the KLOUT

In eVACUATE it is planned that requests to KLOUT will be sent in order to verify whether the certain profile is fake or not in order to assess the verifiability of a certain tweet. This would involve sending information about the individual user (e.g. twitter name/alias) to the KLOUT API. As this operation constitutes a type of data processing, again the necessity and proportionality of such a processing should be motivated. Here it is important to take into account that when a case concerns an enclosed space as in the four eVACUATE scenarios, the reliability of information gathered from social networks could be verified through other means such as the staff on the ground or CCTV. If the necessity of using the KLOUT API is motivated, then a legal basis needs to be found. The most likely candidate would be Article 7 (f). However, it requires the motivation of necessity and a strict balancing against the rights to privacy and data protection (see example above on data mining of social networks in general). The question is whether this additional data processing would be really necessary to end-users and whether the purpose of verifying the influence of a social networks user can be achieved through other means.

In addition, the relevant eVACUATE partners are advised to consult the terms and conditions of using the KLOUT service and if necessary, comply with the relevant requirements.

Recommendations for social networks data mining:

- The purposes for using social networks data mining should be clearly articulated and narrowly specified.
- The necessity and proportionality of data mining social networks in order to achieve the declared purposes should be carefully studied and motivated. This necessity is likely to be different for the different end-user sites and situations. Thus, the end-users of the system should carefully assess the proportionality of resorting to data mining in their daily practices.

- If the necessity and proportionality are justified, then the mining should be based on a proper legal basis, e.g. Article 7 (f) Directive 95/46/EC. Article 7 (f) requires careful balancing between the interests of the controller and the rights of individuals.
- Personal data extracted from the social networks should be anonymized.
- The location of social networks feed of interest should not be stored and/or tracked. If it is necessary to verify the location of a feed in order to select a feed as relevant or not, the location information should nevertheless not be stored.
- It should be assessed whether it is necessary to use the KLOUT API and its legality should be examined.
- The terms and conditions of using KLOUT API should be respected.

6. Video Surveillance

The present section will examine the ethical and legal aspects related to the crowd and individual detection and monitoring through video surveillance as being developed in WP3 and WP4. The focus will be the features of the video analytics and the related data protection and privacy concerns that they raise, especially in a real-life context. Questions concerning how to work with video images during the *research phase* of the project are the focus of Deliverable 11.4.

According to eVACUATE Deliverables D 3.1, D 3.3 and D 3.6, eVACUATE aims to develop automated crowd behaviour detection. This involves the detection of crowd physical motions using behaviour algorithms that process visible, hyper-spectral and thermal images (i.e. multiple spectral bands). Crowd behaviour detection can be performed on the level of the whole crowd, sections of the crowd and single individuals within the crowd.

Currently, the efforts in WP3 are focused on extracting the following features: persons count, crowd density, crowd speed and direction of motion (D 3.1). Additionally, crowd energy, structure, translation (motion) are also analysed. It is argued that this information is needed to assist how to evacuate crowd in case of emergency, as well as get views on how much time evacuation to safety could take.

The detected crowd behaviours are interpreted using concepts on crowd psychology, humans' interactions within large groups and how they are likely to respond to critical situations. It is argued by WP3 that this knowledge is necessary to enhance situation awareness. In particular, WP3 aims to define whether certain behaviour is "usual" or "unusual". This behaviour classification is venue context-dependent in most cases, i.e. what would be usual in a metro-station context might be unusual in the airport context (D 3.1). The automated classification of usual or unusual behaviour would be done by machine learning algorithms that are trained on the basis of information provided by knowledge experts in safety and security management.

When classifying crowd behaviour (usual and unusual), the criteria for this classification are essential. According to WP3, unusual does not necessarily mean abnormal. It rather means not seen before during the classifiers training (D3.3). The declared purpose of understanding whether a crowd behaves usually or unusually, e.g. whether they are nervous, stressed , is (1) to find out what caused this behaviour, and (2) how it affects the situation, and potentially for example how it could influence evacuation. Crowd behaviour detection in eVACUATE will also investigate the effect of individual behaviour, i.e. "seeds," and its propagation within an overall crowd.

In addition, analysis would be performed on the characteristics of the crowd in terms of its age and gender distribution (D3.1). Moreover, according to Deliverable 3.3, with the help of high spectral information, it is possible to detect groups who share certain aspects, interact with each other and share a common identity. Spectral information can also have tracking algorithms and thus track particular objects. This would contribute to the goal of tracking individuals in an indoor environment.

According to WP 3, eVACUATE targets good rates of correct classification of the detected behaviours and motions, and it is acknowledged that the accuracy of these intelligent algorithms depends on the quality of observation data (D3.3).

6.1. Legal analysis

Currently there are already cameras for video surveillance installed at the end-user sites. However, eVACUATE aims to advance the functionalities of this surveillance by making it possible to examine the movements and behaviour of (1) large crowds of people, (2) groups within crowds and (3) individuals within the crowds. As already explained, privacy is not lost *per se* in public spaces.[27] Therefore, the privacy and data protection and ethical concerns have to be studied.

6.1.1. Legality for using algorithms to interpret (and track) behaviour and/or events

The above summary of motion and behaviour detection can be referred to as profiling. Profiling is described as a two-tier concept. On the one hand, it refers to the discovery of correlations between data (building of profiles, i.e. what is "usual" and what is "unusual" behaviour) that can be used to identify and represent a subject. On the other hand, it could mean the application of these pre-defined profiles to identify an individual as a member of a group or category (e.g. decide whether certain individuals' behaviour is usual or unusual according to the pre-defined profiles).[28] The construction of the profile(s) – usual or unusual behaviour in the case of eVACUATE – would take place during the research phase of the eVACUATE project on the basis of test data, while the application of this profile would take place during the validation demonstrations and potentially in real life situations. It is understood that the "usual" and "unusual" behaviour profiles would be applied to whole groups of individuals and also to separate individuals (e.g. the eVACUATE cruise ship scenario where the individual passenger who caused the fire is caught by the video analytics when he would not evacuate from the area under fire).

When these video streams, through which crowds will be "profiled," are not anonymized, especially in real-life situations, it would be technically possible to capture people's images. Therefore, the video streams in this case are to be treated as personal data in the sense of Article 2(h) Directive 95/46/EC as the images refer to identifiable individuals. This article certainly applies in cases when from the video streams it would be possible to single out/distinguish certain individuals,[29] which would be the case especially in real-life situations. Thus, the video streams, which will be analysed in an automated way, should be treated as personal data, even when it is not the intention to identify individuals when detecting and interpreting the motion and behaviour of crowds.

Pursuant to recital 16 of Directive 95/46/EC, sound and image data like video surveillance, is excluded from the scope of Directive 95/46/EC if it is carried out for purposes of public

[27] ECtHR, *Peck vs the United Kingdom*, No 44647/98, 28 January 2003; Coudert, F and Dumortier, J., "Intelligent video surveillance networks: data protection challenges," p.2.
[28] Schreurs et al 2008 cited in Coudert, F., "When video cameras watch and screen: Privacy implications of pattern recognition technologies," Computer Law and Security Review 26 (2010), p. 382.
[29] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data," adopted on 20th June 2007, p.13.

security, defence, national security or criminal law. However, the eVACUATE solution is not meant to be used exclusively for public security and law-enforcement purposes. The solution could potentially be deployed and used by civil protection authorities, for example, in cases of natural disasters, where the Directive would be applicable.

When it comes to law-enforcement matters, Principle 2 of Recommendation No. R (87) allows the collection of personal data for police purposes should be limited to what is *necessary* for the prevention of "a real danger" or "suppression of a specific criminal offence." Thus, data processing measures are not supposed to be used for general surveillance. Exceptions are supposed to be regulated by national law. In particular, the collection of data by means of technical surveillance is supposed to be regulated by specific legal provisions. *This could imply that the usage of such software as developed in eVACUATE to be used for public safety and national security purposes should be regulated in a certain national law to prevent from arbitrariness against individuals. There is a strong appeal to assess whether such algorithmic automated analysis would be necessary and whether it is used when genuine and real dangers are present as compared to generalized surveillance*. As explained earlier, also Council of Europe Convention 108 from 1981 also applies to data processing for law-enforcement purposes and it contains similar principles to Directive 95/46/EC and Recommendation No. R (87).

However, even if in certain cases Directive 95/46/EC does not apply and therefore none of the legal grounds in Article 7 of the said Directive could provide a legal basis, the proposed features of the CCTV are still subject to Article 8 ECHR and Articles 7 and 8 CFREU. These provisions require that the introduced measure pursues a clearly and narrowly articulated purpose, that it is based on a legal basis, e.g. a legal act that legitimizes the usage of such algorithms and that the necessity and proportionality of such CCTV in relation to the purpose it pursues are motivated. An example of how these provisions are to be interpreted is provided in light of the cruise ship case.

The cruise ship case

When discussing the legal basis for behaviour recognition for safety and security purposes through CCTV, the cruise ship scenario presents a separate case. The safety and security measures applicable to ships are set out in the International Ship and Port Facility Security Code (ISPS Code). It has been implemented through chapter XI-2 Special measures to enhance maritime security in the International Convention for the Safety of Life at Sea (SOLAS) 1974. It consists of two parts – a mandatory and recommendatory.

Chapter XI-2 of the SOLAS Convention *does not require* the installation of video surveillance, e.g. CCTV, on ships for safety and security purposes. It treats safety and security as a risk management activity. Thus, the security measures should be adapted to the level of security risk that each individual case poses.[30] This means that (1) the proposed CCTV surveillance features, including the suggested behavior monitoring, needs to be based in some law (it is interpreted that the SOLAS Convention does not provide an explicit legal basis for it) and (2) the necessity and proportionality of such "smart" surveillance need to be motivated first before it is legalized. These two points are intertwined. If the SOLAS Convention does not

[30]http://www.imo.org/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

oblige the ship owners to install CCTV, then Article 7 (f) Directive 95/46/EC could be considered as a legal basis if it is accepted that the Directive is applicable in this case. The applicability could be motivated if it is held true that the security personnel of cruise ships perform video surveillance for purposes of the safety and security on the ship and not out of public and national safety and security purposes, which qualify as an exemption from the Directive. Article 7 (f) of Directive 95/46/EC allows the processing of personal data when it is *necessary* for the purposes of the legitimate interests pursued by the controller unless these interests are overridden by the fundamental rights and freedoms of the others. It thus requires that the *necessity* of the measure is first established and a balancing assessment is performed between the intrusiveness of the measure (the video surveillance and its functions) and the rights of those under surveillance, i.e. the crew and passengers.

These considerations are also required to pass the test set out by Articles 7 and 8 j 52 of the Charter of Fundamental Rights of the European Union and Article 8 European Convention of Human Rights. In general, when assessing whether a certain intrusive measure should be deemed legal, the Strasbourg and the Luxembourg Courts examine whether there is (1) a legal basis for the intrusive measure into the rights to privacy and data protection, (2) whether the measure pursues a legitimate aim or meets objectives of general interest recognized by the Union, (3) the measure is indeed *necessary* and *proportionate* to achieve these aims and purposes and (4) the measure respects the *essence* of the rights and freedoms which are being restricted through the measures in point.

The conclusion is then that the *necessity* (i.e. the measure must be needed and not merely incidental for the achievement of the aim or be useful and desirable)[31], the *effectiveness* (the measure must lead to the fulfillment of the purpose, i.e. the video analytics should be accurate and well-functioning) and *proportionality* (that the chosen CCTV and its video analytics functionality are the least intrusive measures for the achievement of safety and security on ships) should be motivated and justified. *The question here is: can events and certain behaviors be detected without using such machine-learning algorithms and can the algorithms accurately detect the desired events?* In addition, it should be considered whether such CCTV surveillance and accompanying analytics are indeed needed during the whole cruise, on all ships and voyages.

This line of reasoning on necessity and proportionality of the proposed algorithms and balancing against fundamental rights applies not only to the cruise ship case, but also in the other cases.

Last but not least, if cameras which belong to different controllers, e.g. the cameras that watch the metro station in Bilbao and the cameras around the streets and to which the metro does not have access, are interconnected, this action would also need a legal basis and necessary data processing agreements need to be concluded to this end if the *necessity and proportionality* of the interconnection have been motivated first.

6.1.2. Privacy and Data Protection risks stemming from automated profiling

The simultaneous analysis of the input from multiple cameras at the end-user premises enables performances that were not possible on single cameras, e.g. location of events and

[31] ECtHR, *Handyside v United Kingdom*, Application Nr. 5493/72, 7 December 1976.

tracking individuals and crowds of individuals throughout the premises.[32] This could challenge the anonymity and freedom of movement of individuals.

As explained at the beginning of this section, the eVACUATE video surveillance features would use a certain pre-defined profile to automatically classify the behavior of a whole group or even of individuals into usual and unusual and signal this to the respective officers. Thus, this profiling is based on the basis of statistical probability of an object to fall within a certain category. In principle Article 15 of Directive 95/46/EC protects every individual from purely automated decisions based on the processing of his personal data intended to evaluate certain personal aspects[33] related to that person when these decisions produce legal effects concerning the individual or significantly affect him. Pursuant to Article 29 Working Party, individuals enjoy their right to freedom of movement without undergoing excessive psychological conditioning as regards their movement and conduct. It warns against disproportionate application of video surveillance in public places which would allow tracking of individuals' movements and/or trigger alarms based on software that automatically "interprets" an individual's supposedly suspicious conduct without human intervention.[34] Article 15 prohibition would not apply if there is a law which authorizes such automated decisions and which contains sufficient safeguards to prevent individuals from arbitrariness.

Similar provisions are contained in Article 9 of the Proposed Directive on Data Processing in the field of law enforcement. It would explicitly ban automated decisions/classifications if they are based solely on special categories of personal data, but the Directive seems to exclude in the current version of Article 8 images from the special categories of data.

What needs to be defined is what effect this software which would produce automated alarms will have on individuals in order to determine whether it falls under Art. 15 Directive 95/46/EC.[35] This might depend on the different end-users in the future, i.e. how they will decide to use this new technology.

In any case, if pattern recognition or profiling as in the eVACUATE video surveillance solution would lead to automated decisions, e.g. an alarm that triggers an action to be taken by the security officers automatically without the involvement of a human being in the decision-making process, then clearly such a measure must be based on a law. The purpose of such a law is to protect the individuals under surveillance from arbitrariness. Thus, such a law should contain enough safeguards to individuals and these safeguards should be commensurate with the impact of the profiling measure(s) on individuals. Whether such a measure would be deemed necessary and proportionate, is tackled in the discussion of Article 8 ECHR.

If, however, the process is only partially automated and there is a human in the loop, then the regulation of such a situation is less clear. In that case while the detection of "unusual behaviour" and the events or individuals to be further monitored would be automated, i.e. statistically selected, an officer still decides on the course of action. However, his focus is still largely influenced by the machine. Two situations could arise – the application of the pre-

[32] DYVINE, D 5.2
[33] Article 20 of the Proposed General Data Protection Regulation refers explicitly also to evaluation of behavior.
[34] Article 29 Working Party, "Opinion 04/2004 on the Processing of Personal Data by means of Video Surveillance," Adopted on 11th February 2004.
[35] DYVINE, Deliverable 5.1, "Preliminary Version of Legal Issues," 09 July 2007, hereinafter "DYVINE D 5.1."

defined profile to a group of individuals or to separate individuals. The latter situation could arise either if the profiling technique is advanced enough to focus on separate individuals or if the algorithm runs all the time on the premises of the end-users and there is no crowd but rather few dispersed individuals, then the profiling technique could focus on these individuals and assess their behaviour. Or as in the cruise ship scenario, the algorithm could catch the individual who is not evacuating and his behaviour is considered "unusual" by eVACUATE.

In either case, one sees the automated detection and interpretation of behaviours, which is far from being error-prone, ethically acceptable and objective or non-discriminative.

Such automated interpretation/classification of behaviour points to a clear issue of gap in accountability as to the results.[36] The question is who can be held accountable for classifying someone or a group of individuals as behaving "unusually" and by extension treated with more suspicion or tracked. It is also questionable whether the knowledge of the experts who will contribute to the creation of profiles can be automated, i.e. translated into machine learning algorithms (be made machine-readable). Thus, it should not be taken for granted that the machine can perform at the same level as a human being and be error-free.[37] In addition, it should not be assumed that the machine is objective *per se* as the design decisions which build the profiles into the machine stem from human interpretation/judgement.[38] Last but not least, the usage of the results produced by the algorithm should be clearly specified and restricted. This means that it should be narrowly defined what the consequences for individuals would be and how and for what purposes the end-users may use such algorithms in their practice in order to avoid abuse.

An additional risk is that the proposed CCTV may subject individuals to excessive surveillance and gain knowledge about the individuals when this is clearly not necessary. An example could be if according to the algorithm a certain group or individual behaves "normally" but the algorithm is able to tell or help the ones behind the cameras if the observed object is going to work or for dinner, etc (as described in D2.3 eVACUATE). It has to be motivated how the said information would be necessary of eVACUATE if it is to be implemented.

In addition, if the technology is able to recognize certain characteristics of the crowd – age and gender distribution, further knowledge can be gained about the individuals, which increases the chances of identifiability of individuals within the crowds. It must thus be motivated why such information is necessary for the purpose of eVACUATE as it poses higher risk of identifiability.

6.1.3. Accuracy

A crucial point related to the above-discussed behaviour and motion recognition based on pre-defined patterns and profiles is the construction of the actual profile. This will takes place during the research phase of the project. The profiling technique will be tested during the validation demonstrations at the end of the project at the venues of the 4 different sites. It is

[36] boyd, D and Crawford, K., "Six Provocations for Big Data," Paper to be presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 21, 2011, p. 11.
[37] Ibid, p. 6.
[38] Ibid, p. 5.

presumed that if the eVACUATE solution is purchased by the end-users, the same profiles will be applied in real-life situations to the individuals visiting their premises. It is assumed that before this profiling technique is offered to other end-users, the profiles will be adjusted accordingly.

One of the keys issue with regards to the profiles is their accuracy and reliability. The profiles (usual vs. unusual), which would be constructed and applied, would be based on interpreting the motions, e.g. gaits and gestures, and behaviours of individuals within the crowd. It should be borne in mind that sometimes the behaviour of the crowd or individuals in the crowd could be culturally dependent. Thus, the interpretation of the behaviour should also take into account these cultural differences. The above characteristics refer to soft biometrics and they are deemed to reveal information about the psychological condition of those observed and they are more difficult to interpret in an automated way. In addition, video surveillance cameras have a face-recognition capacity. Face recognition and behaviour analysis software are thus based on biometric data, which are defined as the "behavioural and psychological characteristics of an individual and may allow his unique identification."[39] Thus, it can be argued that profiling in eVACUATE is in effect an interpretation of the psychological state of the crowd. Indeed, according to Deliverable 3.1., to semantically annotate the input from the video streams, crowd psychology is employed in order to enhance the understanding of the set of behaviours unfolding at a venue. Thus, knowledge is derived about individuals using sensitive data, which pose higher risks and necessitate inclusion of adequate safeguards to prevent misuse and abuse. In addition, the necessity, proportionality and effectiveness of this measure need to be justified.

Profiling is in effect a statistical probability of falling into a category, which was constructed by the observer and built into a non-flexible technical framework. Furthermore, such technology could have machine-learning capacity, which means that it becomes autonomous in its actions and learning capabilities. Thus, its output is more difficult to logically link to human judgment.[40] The question of the quality of the decisions it makes is still valid. It is questionable whether such an automated pattern-recognition model can account for situations which are not unusual *per se*, such as someone or even 2-3 persons returning to the venue to help their friends/family, as pointed out during the stakeholder workshop in Athens, 14 November 2014. Another example to consider is that what is normal for one individual could be perceived as abnormal by the others. For instance, if there is a small group of individuals running towards the metro when there is no rush hour, the result of the profiling technique could be "unusual." However, the reason for this behaviour and the motion could be perfectly normal, such as the small group or individual being anxious to catch the first metro as they might be in a hurry to visit a friend who just had an emergency, etc. This risks producing many false alerts. In addition, in this case the profile is applied to a small group of individuals, who could be more easily identified. This would be the case also if the behaviour analysis specifically targets individuals and tracks them, thus increasing the risks for these individuals: risks of identifiability, profiling "innocent" individuals, making inaccurate conclusions about them, etc.

[39] Coudert, F and Dumortier, J., "Intelligent video surveillance networks: data protection challenges," p.5.
[40] Bygrave, L., "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling," Computer Law & Security Report, 2001, volume 17, pp. 17–24; also published in Privacy Law & Policy Reporter, 2000, volume 7, pp. 67–76, Footnote 27.

As the results from the testing sessions of the ADDPRIV project show, the real performance of such algorithms is far from perfect. For example, when automated deletion of unnecessary data (i.e. data that was not classified as an event worth observing) was tested, it simply did not work. Also, the amount of false positives was very high during one testing – in 12 hours 2852 evens were detected, while a lot of staged events were not detected (e.g. only 14 out of 96 were detected). While the detection rate improved with the further testing, it reached only 57%.[41] It is thus to be questioned whether such technology can actually improve the work of safety and security personnel in critical situations. It is acknowledged that context matters in interpreting events as it gives meaning and value to data.[42] However, while human can observe and interpret context, can automated detection also achieve this? It would also imply collecting and automatically analysing more data, which poses higher risks for privacy.

In addition, such algorithms bear the risk of discrimination against certain individuals or groups and challenge the anonymity of these individuals who are more intensely surveilled and even tracked. Therefore, the system could be discriminatory *per se,* thus subjecting individuals to statistical discrimination, which challenges the fairness of the algorithms. Moreover, it should be borne in mind that the machines would be trained on test data, which might affect their performance in real-life situations. This could further have negative impact on the individuals, e.g. classifying their behaviour wrongly or inaccurately (e.g. because of cultural differences), treating individuals as suspect, tracking them, etc.

The consequences of inaccuracies (of automated profiles) for separate individuals or for (large) crowds as a whole is that wrong assumptions can be made about them, which could prejudice the ones behind the camera and lead to automatic acceptance of the validity of the alerts and reduce their investigatory and decisional responsibilities,[43] even if they still take the final decisions about their actions, and possibly trigger a situation where the ones observed are treated as suspicious without a reason.

On the other hand, inaccuracies resulting from the automated profiling could distract the officials behind the cameras through triggering false alarms. At the same time there could be situations that deserve their attention but they are not "caught" by the "unusual motion/behaviour" profile, as exemplified by the ADDPRIV project. Last but not least, there is a risk that the discussed video analytics could be used to profile crowds and individuals beyond the scope of preventing or responding to an emergency. For example, according to D 2.3, in the metro scenario video analytics could be used to help the officers behind the cameras analyse whether a crowd, whose behaviour and motion are classified as "usual," is going to work, or for dinner or they are leaving after a party.[44] Until now the necessity of such a profiling has not been motivated. It is also questionable whether it is in proportion to emergency response purposes. Such profiling, no matter whether automated, semi-automated or not automated, can lead to gaining knowledge about individuals - their habits, their behaviour, etc. As such information has not been proven to be necessary for

[41] P. Murphy, D. Neyland, I. Kroener (2014). Deliverable 6.3 – Developing Ethical Principles and a Means of Assessment for ADDPRIV and 'Smart' CCTV. ADDPRIV consortium, www.addpriv.eu, p. 54-68.
[42] Boyd, D and Crawford, K., "Six Provocations for Big Data," Paper to be presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 21, 2011, p. 8.
[43] DYVINNE, D5.2.
[44] eVACUATE Deliverable 2.3, V1, p.21.

emergency response purposes, it leads to the conclusion that the intrusion it could result in would be excessive.

Recommendations

In order for the video analytics developed in eVACUATE to stay within the limits of the law, the following recommendations should be observed:

- The purposes of the video analytics under development should be narrowly and clearly articulated. Any usage of the proposed software/algorithms which goes beyond the declared purpose should be deemed illegal as it would amount to function creep.
- The necessity and proportionality of having the video analytics in real life situations by the different end-users should be motivated.
- In light of the proportionality principle, it is recommended that such analytics remains dormant until a situation is identified where it would be necessary for dealing with the situation. With regards to using the algorithms for preventive purposes, the question arises whether it is needed. It is assumed that in principle major deviations from normal situation, e.g. most or all persons running suddenly in different directions, people fighting, etc, are expected to be noticed without sophisticated profiling techniques.
- Before such algorithms are deployed in real life situations, the end-users should ensure that there is a legal basis for them to make use of such profiling technologies.
- Depending on the possible effects on citizens that such an algorithm might have, adequate safeguards for individuals should be ensured.
- The accuracy and thus the performance of the algorithms should be reliable. The criteria for usual and unusual should be carefully selected and motivated. Discrimination should be avoided.
- The new processing should ensure the security of the data, i.e. streams and recordings.

Introducing these algorithms can be seen as part of the tendency to add more intrusive surveillance measures to existing ones. The justification often used to legitimize such measures is that the existing ones do not "work." Thus, while cameras were introduced to allow officials to monitor citizens and event, now it is argued that this has not been effective enough and officials cannot notice major events. Thus, they argue in favour of video analytics, which as described above, could be more intrusive *per se*,[45] but not necessarily better in terms of performance.

[45] Bennett, C. and Haggerty, K. (eds), "Security Games: Surveillance and Control at Mega-Events, Routledge, 2011, p.12.

7. Proportionality

In emergency situations one of the key principles to observe is the proportionality of the measures taken to respond to a particular emergency. In the case of eVACUATE, the concept of proportionality means in essence striking the right balance between the emergency measures that safety and security officers have to take in order to respond to a certain emergency evacuation event and the fundamental rights of individuals, in this case mainly privacy and data protection since a lot of the technologies which are part of the eVACUATE solution are designed to process personal data. The purpose is to ensure that the chosen means and measures do not go beyond what is necessary in order to respond to the event and they are the least intrusive ones. It is often a challenge to strike this balance when the stakes are high, i.e. when the ultimate aim is to save human life. However, even such an aim requires careful consideration of the necessity of the chosen measures.

As each emergency situation is unique and thus the measures that need to be taken would differ on a case-by-case basis, there cannot be one general set of guidelines and rules on what is proportionate in all emergency cases. Therefore, in the following paragraphs the concept of proportionality will be discussed through the prism of the 4 scenarios developed in eVACUATE (as presented in D 2.3). The purpose is to exemplify how proportionality should be applied in emergency cases if the proposed scenarios would happen in real life.

The paragraphs do not seek to present an in-depth analysis of the scenarios as such. In addition, the scenarios have not been finalized at the time of the writing of this deliverable. The information flows in each scenario still need to be delivered. Afterwards, a more detailed analysis of the scenarios from a proportionality point of view can be made. Thus, as the scenarios are subject to further development, elaboration and refinement, the new versions of the scenarios can be discussed in the update of this deliverable in M36 (D11.3 and D 11.5).

Issues of proportionality from a privacy and data protection point of view have been touched upon when discussing the individual technologies in the previous chapters. In principle, when new, intrusive measures are introduced, they should pursue a legitimate aim. Saving human life, preventing crime from happening, preventing injuries and assisting injured individuals, etc could all be legitimate aims. However, to achieve these aims one should not put all individuals under general and permanent surveillance as this would be disproportionate. Thus, one of the recurring recommendations from the previous sections has been to keep the eVACUATE system as such dormant until an emergency is identified and the information collected from the different sensors would be necessary in order to take decisions about the evacuation strategy.

According to Article 29 Working Party, one factor in assessing whether a proposed (i.e. new) intrusive measure is strictly *necessary and proportionate* is by reviewing the effectiveness of the already existing measures "over and above the proposed measure."[46] When a new measure is proposed, such as adding new functions to the existing video surveillance or introducing new sensors for personal data collection, e.g. mobile apps or social networks data mining, evidence-led explanation of why the existing measures are not sufficient any

[46] Article 29 Working Party, "Opinion 1/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector," 27 February 2014, p. 9-10.

more is necessary. Once it is proven that the existing measures are not sufficient, it is necessary to prove again through evidence that the proposed measure will address effectively the pressing social need, e.g. through the validation demonstrations at the end of the project. It is important that when the technologies are introduced in real life, the scope of their usage must be carefully limited,[47] so that they are not used for incompatible purposes, thus exposing individuals to higher risks of abuse. Such could be the case if the EVAMAPP, for example, is used not only for evacuation purposes, but for tracking individuals for law-enforcement purposes.

The following sub-sections provide a preliminary discussion of whether the proposed scenarios strike a good balance between the needs of evacuation, taking into account the already existing procedures and technologies at the end-users' sites, and the privacy and data protection rights of individuals. The focus of the discussion will be in how far the added value of the eVACUATE solution is proportionate with regards to the rights to privacy and data protection. Thus, only the procedures and technologies designed to process personal data in the proposed scenarios will be discussed. Out of brevity considerations, the sections below only point out the points in the scenarios which need to consideration from a necessity and proportionality point of view. *This is not meant to criticise the technologies or the scenarios* per se *but the application of certain technological solutions to the particular scenario if these scenarios would be real-life scenarios.* The present scenarios have been developed in the framework of preparing the validation demonstrations. Due to the limitations of the validation demonstrations (e.g. space, volunteers), the scenarios cannot simulate a large-scale emergency which would involve larger spaces and higher number of individuals. While the proportionality analysis in the following chapter points out that the use of certain technologies might be disproportionate in the described smaller scale scenarios, it is without prejudice to the fact that some of these technologies could be useful in larger scale evacuations, provided they function effectively and process data accurately. However, it remains the responsibility of the end-users to decide when the usage of a certain technology which processes personal data would be really necessary and proportionate, depending on the situation at hand (whether a normal situation or an emergency and also what kind of emergency), i.e. on a need-to-know basis. The discussion below seeks to give them guidance by giving examples from the scenarios. The remarks below represent an initial analysis of the scenarios. Additional legal guidance will be provided to the partners in the further development of the scenarios.

The analysis is based on the scenarios as described in the current version of D 2.3 Evaluation Criteria and Scenario Definitions.The readers are invited to refer to this document for questions on the scenarios.

7.1. Airport Scenario – AIA

The analysis below is based on the scenario description in D 2.3 and the elaborated description of the data flows, which was provided in an email by INDRA on 3 February 2015.

The scenario develops over the course of 65 minutes at the Athens Airport, where there is a bomb threat. The expected added value of the eVACUATE solution in this scenario is that before evacuation is ordered, eVACUATE will provide the decision-maker with an overview

[47] Article 29 Working Party, "Opinion 1/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector," 27 February 2014, p. 9-10.

of the number of persons in the concerned area; it will predict crowd movements; it will facilitate communication with the service officers and predict evacuation time and routes. When the evacuation is ordered, then eVACUATE can again be used for communication with the service and security people; count individuals that have been evacuated (RFID and cameras); use social networks and app in order to inform the public. When the search of the missing person is going on, it is planned use RFID to find him/her; communication with the personnel via the app. Camera selection of type of behavior would also be employed.

In that case the following observations can be made about the new technologies introduced by eVACUATE.

7.1.1. Communication with passengers and with staff

The suspect bag, which triggers the evacuation, is located within fifteen minutes from the moment AIA was informed of its existence. This means that the area under threat, which is not big but only one gate, is identified quickly and communication with affected individuals can be established via Public Announcement (PA), as suggested by the scenario. PA does not require the processing of personal data (unlike sending messages through SMS (cell broadcast) or the EVAMAPP) and it is an effective means of spreading information within a certain area, which is identified in advance. In addition, the staff will be dispatched to the affected area to help individuals. Thus, it appears that PA solely would be a sufficient means of communicationand also the least intrusive one. This can be improved by preparing pre-defined messages in different languages. With regards to using EVAMAPP for passengers in this case, it can be helpful in providing evacuation guidance if passengers indeed download in advance the app. It could be helpful in cases when PA would not be enough, e.g. evacuation of the whole airport/all terminals is ordered, the traditional means of technology are not sufficient to guide individuals, etc.

As to introducing the EVAMAPP for security staff, it is already a practice at AIA for security personnel to use TETRA for communication purposes. TETRA appears to be less intrusive than the EVAMAPP since EVAMAPP could lead to tracking the location of each staff member. Thus, it has to be demonstrated that TETRA is not a sufficient and efficient technology for providing communication means for the airport staff and further technologies would be needed and the features of these new technologies actually meet the existing gaps of staff communication. In addition, it has to be demonstrated that the app has significant added value to the existing system of communication. If EVAMAPP for staff members is introduced, it should be compliant with AIA's staff policies/regulations.

As to disseminating information to citizens via the social networks it can be assumed that when the authorities spread messages over social networks, then this an effective way of disseminating information. However, this should only be an additional means, as it cannot be expected that all individuals will have access to internet and will actually read social networks at that moment when they are being evacuated and would be busy.

However, if social networks were to be data-mined in order to monitor the situation before and during the crisis, in that case the utility and this necessity and proportionality would be questionable. The reason is that the threat in the scenario under discussion cannot be identified through social network posts and it is announced via a phone. In addition, the passengers at and around the gate are not informed of the evacuation until the bag is found by the security agent and thus they are not aware of the threat in order to report on it. The

scenario does not demonstrate a lack of information and thus it is not justify how social networks data mining will remedy the situation if social networks were to be used. The affected area, moreover, is covered by cameras and security staff that can contribute to the information collection.

7.1.2. Video surveillance

It seems that video surveillance in this scenario will be multi-purpose – to provide density information and to identify "unusual" behavior.

With regards to individual counting/density information, it is understood that for this particular CCTV function no facial recognition would be necessary. Thus, if technically possible, the information displayed to the decision-maker for purposes of density counting should not contain personally identifiable information such as images.

While video surveillance can be helpful in monitoring the number and movement of individuals, in the present case it is doubted how it will be helpful in identifying unusual behavior with regards to the person who is declared missing.

It is understood that WP3 video analytics will be used, which is focused on identifying "unusual" behavior. The question is what will be used as a criterion for "unusual" behavior *in this scenario*. The scenario description indicates that the boy could be found hiding in the toilet with the help of the behavior detection analytics. It is reasonable to question how the software can classify the behavior of the child as "unusual," as entering the toilet and not exiting it within a short period of time cannot be classified as "unusual" *per se.* In general it would not be ethical to have an alarm which is based on people's entry into and exit from the toilets or alternatively an alarm which is focused on children *per se*.

In INDRA's explanation, once the area is evacuated, the video analytics will be looking for a young person who is wandering in the evacuated area/looking for someone to continue the search for the child. In general, a lot of people wander at airports and look for someone, especially in front of toilets (people wait for their friends, etc…), so this can hardly be expected to be unusual in an airport scenario. There is a risk that the system will produce a lot of false alerts, especially in view of the fact that security staff will be wandering there all the time, looking for the child. In addition, if there is an alert focused on "young persons" this might be interpreted as discrimination, since the algorithm will target one particular category of individuals.

It could be assumed that the child can be found by a person who actually is searching for him everywhere, including the toilets. It is also understood that after the area is evacuated, only a couple of security officers are around. If the boy comes out of the toilet, they can easily see this. Also, the person behind the cameras should be able to notice this without a special algorithm.

In light of the proportionality principle, first it needs to be motivated how behavior detection can actually increase the effectiveness of the current video surveillance and whether it is the least intrusive means of finding the missing child. If this is the case, it is good to restrict the behavior detection and crowd movement developed in WP3 and 4 only to the area concerned and not all over the airport. Also, in the present case it would be best to activate this function only after the call is made to AIA to warn of the bomb. In addition, it should be

borne in mind that not all cameras belong to AIA as some belong to the shops/restaurants at the airport. Thus, in principle the cameras which do not belong to AIA should not be interconnected to the eVACUATE solution, unless the necessity for doing so is proven and the necessary data processing agreements are concluded between AIA and the controllers of the other cameras.

7.1.3. RFID ticketing

In the AIA scenario it is questioned whether the chipless RFID application can ensure an accurate or at least reliable estimation of the individuals. The question is based on the fact that a lot of passengers print their boarding passes at home or download them on their smartphones. Others might have them printed at the airport but might not wish to have a chipless RFID tag. In this way, only a certain percentage of the boarding passes would in reality have RFID tags and thus may not present accurately the number and types of passengers. In addition, it should be considered whether it is necessary to know at each moment what category the passengers belong to or this information would be necessary only in emergency cases. If the latter is the case, then the partners are advised to design the system in such a way that it displays only the general number of passengers in normal situations and provides information on the break-up of passengers in emergency cases.

Another issue with accuracy is that oftentimes one family member carries all passes, e.g. the mother carries the boarding passes of her children and thus a couple of passes are piled together. It is thus questioned whether the readers will be able to read all the tags.

If it is proven that RFID tags could be useful in counting the number in individuals around a certain gate or the toilets, it is questioned whether it is practical to install RFID readers around the gates and toilets and how the application can be useful in detecting the location of the missing child in the toilet. It looks likely to happen if there are RFID readers in front of the toilet, which is highly unlikely. In addition, if the RFID tags are printed on the boarding pass, normally it is the parents and not the children who carry the boarding passes. Thus, the system might not be able to “detect” the location of children.

Last but not least, it must be clarified how the chipless RFID system will delete the information of passengers who have boarded the plane. Thus, either the system should automatically delete the information from the RFID system of the planes that have taken off or there must be readers at the boarding points where the tags that are read are automatically deleted from the system. When deciding where to place the readers, the decision-maker should make sure that they are not placed close to each other, thus allowing the tracking of individuals around the airport.

7.1.4. Other

If the eVACUATE solution is to be connected to external emergency systems, such as iSafety, the flow of personal data should be mapped. It should be ensured that such an interconnection does not disclose personal data to authorities/institutions or individual staff members that are not authorized to have access to certain data.

7.2. Cruise ship Scenario

eVACUATE aims to assist in the identification of the accident and the evacuation of passengers to the right muster stations.

7.2.1. Chipless RFID system[48]

The system is used for counting individuals at 5:00 am the majority of who, according to the scenario description, are sleeping in their cabins. This begs the question where the RFID readers will be placed in order to get accurate numbers (e.g. in front of the rooms?) and whether in this particular case it is not going to be more effective to use the information from the FIDELIO database to count the number of individuals who are checked in in those cabins which are close to the affected area.

Also, it should be clarified where the chipless RFID readers would be placed during the evacuation. If they are placed in front of the mustering stations, this might overlap with the current system of reading the ship ID cards. As understood, the staff members already scan the ship ID cards with RFID chips and gain information about the numbers and identities of the passengers and whether they are at the right mustering station.

7.2.2. CCTV behavior detection

In the scenario, CCTV behavior detection is used to detect the individual who does not evacuate the area and caused the fire and the lady who is unconscious. It is assumed that security personnel are responsible for watching the cameras. This should be especially the case when there is an identified incident, which should occupy the attention of the ones behind the cameras, whose duty it is to watch the cameras. Thus, it is expected that the official will be able to notice a human being in the area under consideration, which is considered empty according to the description ("hanging around in the evacuated zone," p. 61 in D 2.3) or that he is trying to start another fire. Thus, it is not clear how the unusual behavior detection will be of added value to the current situation. The same reasoning could be applied to the woman who is found unconscious. While it is clear that such cases should be promptly handled by the cruise personnel and that CCTV could be of help here, it must be demonstrate that the additional video analytics would significantly enhance the work of staff behind the cameras. these events cannot be noticed by the ones behind the cameras and thus they need assistance. And it is important that the algorithm is able to actually detect such events and not raise additional alerts, which could distract the security personnel at such a critical moment. Distraction might occur because the algorithms might detect security personnel walking around the area or fallen object (not an injured woman), which could produce false alarms. This could be the case if an alarm is programmed to detect as strange people who do not follow the AER.[49] These could actually be crew members coming to rescue someone.

If it is argued that the security personnel might not be close to the cameras to notice events, and thus they need automated detection, then it is questioned how they will be able to notice the alarm raised by the software if they are not watching the cameras. It must thus be demonstrated that in such a case as the described scenario, the software will have an added value and the identification of the said individuals would not be possible with the available resources.

[48] Here the Chipless RFID system refers to the system developed in eVACUATE
[49] See p. 19 of the Cruise ship scenario as communicated by Pedro Garibi (INDRA) on 24.02.2015.

7.2.3. EVAMAPP

The cruise ship scenario is a good example of how EVAMAPP can have an added value for passengers. However, its application should be elaborated better in the scenario so that it is seen how it is used in practice, in what manner it helps individuals and what data it processes.

7.3. Stadium Scenario – Anoeta Stadium

The focus would be the identification of unruly behavior as a result of which the stadium has to be evacuated while some people are trying to enter it.

7.3.1. Video Surveillance

Monitoring of behavior at stadia during football games in Spain could be allowed in certain situations. According to some Spanish legal provisions, it seems that video surveillance, which records the spectators and their behavior, could be allowed in order to fight hooliganism and violence during football games, especially during official sports events.[50] However, before such video surveillance measures are switched on, the end-user should verify the rules he is subject to with regards to the specific stadium or type of game and what surveillance measures he is allowed to take. When the end-users are not required to install and use such video surveillance, they should assess whether this would be proportionate for the particular type of game before each game.

The data protection authorities of the Czech Republic and Italy followed the same logic when examining the question of proportionality of safety measures at matches. In these cases individualized ticketing with names was not deemed proportionate for all the people and at all matches. It was accepted, however, that only for certain games and certain individuals, tickets with names would not be disproportionate.[51] Thus the questions is, if video surveillance that looks at the spectators' behavior is allowed in general, whether it is necessary to be used for all games. If it is used, it should be demonstrated that the additional video analytics as developed in eVACUATE are needed and have added value as compared to the existing CCTV at ASRS.

In the case at hand it appears that the suggested video surveillance could be useful in detecting hooligan behavior. Nevertheless, safeguards for individuals should be envisaged to ensure against abuse. For example, individuals should not be arrested only on the basis of the images and the usage of such "smart" surveillance should not be abused (i.e. used for other purposes). This means that if the allowed usage of the "smart" surveillance is to monitor for hooligan behavior, the algorithms, if deemed necessary and proportionate, should focus only on such type of behavior. Here it will be very important what events the system will be programmed to "detect" and who will decide on that.

7.3.2. Chipless RFID tag

RFID could be indeed very helpful in counting how many individuals have entered the stadium and how many have evacuated it afterwards. However, it is questioned whether in

[50] Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte; Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte

[51] Article 29 Working Party, "Opinion 1/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector," 27 February 2014, p. 17-18.

that case information on which category the individuals belong to would be necessary and helpful for the particular case at hand. In addition, in cases of such emergency when individuals need to exit the stadium as soon as possible, it is questioned how accurately the readers can read the numbers of passers-by. While it is useful to know how many individuals there are in a certain area or in the whole stadium, it should be considered whether the numbers cannot be calculated from the video surveillance in place or the number of seats available in the stadium and its sectors and how the RFID system could improve the situation. One of the current issues is that the RFID system cannot yet detect the direction of motion. However, if the system is designed in such a way that it can count how many people enter the stadium, e.g. turnstiles at entry which count the people passing by, and it can count the persons who exited, e.g. again by turnstiles which count people passing by exit turnstiles, and the information will be useful to the decision-makers (e.g. what would they do by knowing whether someone belongs to a category needing special assistance), then the usage of the system could be considered.

7.4. Metro Station Scenario – Bilbao

7.4.1. Chipless RFID System

The case raises similar concerns as the ones the RFID raises in the stadium case. In the metro case it appears necessary to have an accurate number of individuals at the station in order to assess the situation and plan the evacuation. However, it needs to be demonstrated how the additional information on which category the individuals in the crowd belong to, would be necessary in this particular scenario and how individuals needing assistance can be helped.

7.4.2. CCTV surveillance

It appears that the scenario includes surveillance through CCTV of the area outside the station. This entails interconnection of cameras with different controllers and thus proper agreements need to be concluded between the different controllers before the interconnection. Such interconnection, however, should take place only if this is deemed necessary and proportionate.

In addition, at 22:40 the “unusual” behavior detection is used to detect the arrival of the large group of individuals who are blocking each other (p. 63, D 2.3). While it is certainly necessary to have a means to detect such events in order to react to them, it can be assumed that after a football game the security personnel should be alert that a large number of individuals would crowd the metro stations and hooligan behavior could occur. Thus, it is expected that the security personnel will be monitoring the cameras and the described events can be noticed without the help of additional software. If it is motivated that the present resources cannot identify such situations, it should be demonstrated how the proposed “unusual” behavior detection can have significant added value to the current situation.

7.5. Conclusion

The proportionality discussion reveals that in general the eVACUATE solution has added value and can thus assist the decision-makers in emergency cases. Nevertheless, the necessity of employing certain elements of the solution in different types of real life situations, e.g. RFID ticketing or social networks data mining, needs to be motivated. It is

thus recommended to the end-users and the decision-makers in emergency situations to assess the usefulness of the different elements of the eVACUATE solution and use only the ones that would be relevant and not excessive for the situation unfolding in front of them. In this way it can be ensured that the right balance is struck between the privacy and data protection rights of individuals and the measures taken in response to an emergency.

8. Intellectual Property Rights

Intellectual property rights such as copyright also have an impact on the use and exchange of data in the eVACUATE-system. These rights more specifically have an impact on the use and exchange of incorporations of data that embody an intellectual property protected result of efforts (e.g. the use and exchange of a digital copy of a map that embodies the copyright protected intellectual creation involved in developing the symbols used on the map). Intellectual property rights determine the use and exchange of such incorporations of data that do not amount to intellectual property infringement.

In the context of the eVACUATE-system the cases in which intellectual property rights play a role are not to be underestimated. Incorporations of data that are valuable to evacuation scenarios will often prove to embody intellectual property protected result of efforts. This is for example frequently the case with text files, images and maps.

8.1. Basics of intellectual property rights

Intellectual property rights grant exclusive rights in relation to specific types of results of human efforts. The common characteristic of these results is that they can be embodied in more than one perceptible thing at the same time. For example, the copyright protected intellectual creation involved in developing symbols to indicate the available first aid supplies on a map can be embodied in several maps at the same time.

If an intellectual property right grants a person an exclusive right in relation to a particular result of efforts this has far reaching consequences. The person granted the exclusive right, that is the right holder, obtains the exclusive power to perform certain categories of acts concerning embodiments of the result of efforts (e.g. the exclusive power to 'reproduce' embodiments of the result of efforts). For persons other than the right holder the opportunity to perform these acts concerning these embodiments without committing intellectual property infringement is limited to two scenarios. The first scenario is that this person has obtained the permission of the right holder to perform these categories of acts as a result of their agreement on licensing[52] or transferring[53] the exclusive right granted by the intellectual property right. The second scenario is that this person can call upon an exception which the intellectual property right stipulates in relation to a category of acts subject to the authorisation of the right holder. Such exceptions describe specific circumstances in which performing such a category of acts without the permission of the right holder does not constitute intellectual property infringement.

[52] In a licence the right holder merely gives a person the permission to perform certain categories of acts subject to his authorisation. Obtaining a licence does not make a person the new right holder of the exclusive right granted by the intellectual property right.

[53] A transfer does make the person to whom the transfer is made the new right holder of the exclusive right granted by the intellectual property right.

8.2. Relevant intellectual property regimes

In the context of the eVACUATE-system, the intellectual property rights that deserve closer attention are copyright and the database *sui generis* right[54]. The incorporations of data that people will want to use and exchange within the system to organise an evacuation are most likely to be covered by these two intellectual property rights. Copyright can become relevant, for example, in light of the exchange of maps of the site being evacuated. The database *sui generis* right can become relevant, for example, if a first responder consults a database of the health risks caused by chemical substances and exchanges the search result with his colleagues (e.g. to discuss the possibility of still using an exit despite the presence of a cloud containing that substance).

8.2.1. Database sui generis right

The database *sui generis* right grants a right holder an exclusive right in relation to a 'database[55]' that demonstrates that there has been a qualitatively or quantitatively substantial investment in obtaining, verifying or presenting its content[56]. The exclusive right granted by the database *sui generis* right results in an exclusive power for this right holder to control the extraction and the re-utilisation of the whole or substantial parts of the content of that 'database'[57]. The database *sui generis* right can in fact be analysed as granting an exclusive right over the substantial investment in obtaining, verifying or presenting the content of a 'database' as embodied in the whole or substantial parts of this content[58]. Initially the database *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[59]. However, this exclusive right can be transferred to a new right holder or licensed to a licensee[60]. The duration of the exclusive right is, in principle, limited to 15 years counting from the date of completion of the 'database'[61]. Yet, any change to the contents of a 'database' that demonstrates a

[54] See: Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ* L 167, 22 June 2001, p. 10–19 (hereinafter: Information Society Directive); Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ* L 077, 27 March 1996, p. 20-28 (hereinafter: Database Directive); Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), *OJ* L 111, 05 May 2009, p. 16-22 (hereinafter: Computer Program Directive)

[55] In the database sui generis right a 'database' refers specifically 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. See: art. 1.2. Database Directive.

[56] Art. 7.1. Database Directive

[57] Art. 7.1. Database Directive

[58] M. LEISTNER, *Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht. Eine Untersuchung zur Richtlinie 69/9/EG und zu ihrer Umsetzung in das deutsche urheberrechtsgesetz*, München, Beck, 2000, p. 148-149

[59] Recital 41 Database Directive

[60] Art. 7.3. Database Directive

[61] Art. 10.1 Database Directive

qualitatively or quantitatively substantial investment has the 'database' resulting from that investment enjoy its own term of protection of 15 years[62].

A. Requirements for the grant of an exclusive right

In order to grant an exclusive right the database *sui generis* right requires that a 'database' substantiates that obtaining, verifying or presenting its content involved a qualitatively or quantitatively substantial investment[63]. In this regard, it is usually accepted that the requirement of the investment being 'substantial' is to be interpreted as a *de minimis* criterion that merely excludes insignificant investments[64]. Obtaining the protection offered by the database *sui generis* right does not require any formalities or registration. In practice, it is to be taken into account that many collections of data can turn out to be covered by exclusive rights granted by the database *sui generis* right (e.g. digital topographic maps[65] or websites[66])

B. Whole or substantial part of the content of a database

The exclusive right granted by the database *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'[67]. 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[68]. 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 *sui generis* right[69]. The database *sui generis* right does not give the right holder an exclusive power over individual elements of a 'database'.

C. 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'[70]. '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

[62] Art. 10.3 Database Directive
[63] Art. 7.1. Database Directive
[64] See for example: D. THUM, "UrhG § 87a Begriffsbestimmungen" in A. WANDTKE and W. BULLINGER, *Praxiskommentar zum Urheberrecht*, München, Beck, 2008, Nr. 55
[65] See: referral to the European Court of Justice, 16 January 2015, C-490/14 (*Verlag Esterbauer*) and M. LEISTNER, "Die Landkarte als Datenbank. Überlegungen zum Datenbankschutz für topografische Karten und geografische Daten." *GRUR* 2014, p. 528-536
[66] See e.g.: M. KÖHLER, "Der Schutz von Websites gemäß §§ 87 a ff. UrhG", *ZUM* 1999, p. 548
[67] Art. 7.1. Database Directive
[68] See European Court of Justice 9 November 2004, C-203/02 (*BHB v. William Hill*), para 69
[69] See: European Court of Justice 9 November 2004, C-203/02 (*BHB v. William Hill*), para 72 and recital 46 Database Directive
[70] Art. 7.1. Database Directive

means or in any form[71]. 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[72]. In this regard, however, the database *sui generis* right also explicitly states that the first sale of a copy of a database within an EU Member State by the right holder or with his consent exhausts the right to control resale of that copy within the EU Member States[73].Both 'extracting' and 're-utilising' only refer to type 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 a '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[74]. For example, using metasearch engines or data mining in relation to databases available on the internet and using the data achieved this way can under circumstances give rise to 'extracting' or 're-utilising' in the context of the database *sui generis* right[75].

D. Relevant exceptions to the categories of restricted acts

Finally, it is necessary to take into account that the database *sui generis* right also stipulates several exceptions in relation to the categories of acts that, in principle, are subject to the authorisation of the right holder. Some of these exceptions are relevant to persons responding to an emergency.

The first exception that is relevant in case of emergencies is the mandatory exception which 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 purposes whatsoever qualitatively or quantitatively insubstantial parts of its contents[76]. Note that this exception is somewhat stating the obvious given that, as a rule, the database *sui generis* right does not grant a right holder an exclusive right over acts that merely concern insubstantial parts of a 'database[77]'. In any case, it is to be accepted that, in principle, the database *sui generis* right does not prevent people from lawfully 'extracting' or 're-utilising' insubstantial parts of a database that has been made available to the public (e.g. 'extracting' or 're-utilising' the list of

[71] Art. 7.2, a.) Database Directive
[72] Art. 7.2, b.) Database Directive
[73] Art. 7.2, b.) Database Directive
[74] Art. 7.5. Database Directive and European Court of Justice 9 November 2004, C-203/02 (*BHB v. William Hill*), para 89
[75] See: European Court of Justice 19 December 2013, C-202/12 (*Innoweb vs Wegener ICT Media*) and M. BERBERICH, "EuGH: Eingriff spezialisierter Metasuchmaschinen in Datenbanken", *MMR* 2014, p. 185
[76] Art. 8.1. Database Directive
[77] E.g.: M. LEISTNER, *Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht. Eine Untersuchung zur Richtlinie 69/9/EG und zu ihrer Umsetzung in das deutsche urheberrechtsgesetz*, München, Beck, 2000, p. 189-190

characteristics which a database of the characteristics of chemical substances provides in response to a query about a single chemical substance).

The second exception that can be relevant in the context of emergency situations relates to public security. The Database Directive has allowed legislation of the Member States to provide that, for the purposes of public security, a lawful user of a database that is made available to the public may 'extract' or 're-utilise' a substantial part of its contents without the authorization of the relevant right holder. 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 people responding to an emergency (e.g. people helping to organise an emergency evacuation), provided that they qualify as 'lawful users'[78]. This condition of qualifying as 'lawful users' gives rise to uncertainty. The reason is the on-going debate whether the notion of '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[79].

8.2.2. Copyright

Copyright grants the right holder an exclusive right over a 'work'. Such a 'work' is 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[80]. 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'. 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[81]. The duration of this exclusive right is limited to the lifetime of the author of the 'work' plus an additional 70 years[82]. In copyright 'works' that relate to 'computer programs[83]' or to the selection or arrangement of the elements of a 'database[84]' are partially subject to significantly different rules than other

[78] Compare: D. THUM and K. HERMES, "UrhG § 87c Schranken des Rechts des Datenbankherstellers" in A. WANDTKE and W. BULLINGER, *Praxiskommentar zum Urheberrecht*, München, Beck, 2014, Nr. 37

[79] See, with regard to this debate, e.g.: V. VANOVERMEIRE, "The Concept of the Lawful User in the Database Directive", *I.I.C.* 2000, p. 63-81

[80] E.g.: European Court of Justice 1 December 2011, C-145/10 (*Painer*), paras 88-89 and U. LOEWENHEIM, "Abschnitt 2. Das Werk" in G. SCHRICKER, *Urheberrecht Kommentar*, München, C.H. Beck, 2006, p. 56 ff.

[81] See recital 30 Information Society Directive

[82] Art. 1.1. Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version), *OJ* L 372, 27.12.2006, p. 12–18

[83] See: recital 7 Computer Program Directive ("*For the purpose of this Directive, the term 'computer program' shall include programs in any form, including those which are incorporated into hardware. This term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage*.").

[84] In the context of database copyright a 'database' refers specifically 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. See: art. 1.2. Database Directive.

'works'. [85] From that perspective it is sometimes relevant to make a distinction between the rules set out by ordinary copyright, computer program copyright and database copyright[86].

A. 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) demonstrates 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'[87]. 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[88]. 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'.

B. 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 thing has to meet two requirements. The first requirement is that the perceptible thing 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 thing 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'[89].

C. 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[90]'.

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[91]. This broad notion of 'reproducing', in principle, also covers the often short-lived duplications which computers need to make in order to technically allow them to perform a task. Examples of such

[85] See: Computer Program Directive and Database Directive

[86] See: European Court of Justice, 22 December 2010, C-393/09 (*Bezpečnostní softwarová asociace*), para 44.

[87] E.g.: F. GOTZEN, "Art. 1" in F. BRISON and H. VANHEES (eds.), *Huldeboek Jan Corbet. De Belgische auteurswet. Artikelsgewijze commentaar*, Brussel, Larcier, 2009, p. 6-7

[88] E.g.: U. LOEWENHEIM, "Abschnitt 2. Das Werk" in G. SCHRICKER, *Urheberrecht Kommentar*, München, C.H. Beck, 2006, p. 56 ff.

[89] E.g.: A. STROWEL, "La contrefaçon and droit d'auteur: conditions et preuve ou *pas de contrefaçon sans 'plagiat'*" , *Auteurs & Media* 2006, p. 268

[90] See: See: art. 2-4 Information Society Directive, art. 3 Rental and Lending Directive (2006) (Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version) *OJ* L 376, 27 December 2006, p. 28-35; Compare: Art. 5 Database Directive and art 4 Computer Program Directive.

[91] Art. 2 Information Society Directive; art. 5, a) Database Directive; art 4.1., a) Computer Program Directive

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 also '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[92]. 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[93]'. 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 his possibility to call upon copyright to control 'distributing' that particular embodiment in the EU Member States[94].

Copyright also makes 'renting' and 'lending' subject to the authorisation of the right holder[95]. 'Renting' covers making available for use, for a limited period of time and for direct or indirect economic or commercial advantage[96]. '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[97].

D. Relevant exceptions to the categories of restricted acts

Copyright also stipulates several exceptions to the categories of acts that, in principle, are subject to the authorisation of the right holder. Again, some of these exceptions are relevant to persons responding to an emergency.

The first exception that is relevant in the context of responding to an emergency is the mandatory exception for temporary technical reproductions which the Information Society Directive stipulates regarding ordinary copyright. This exception applies to all 'works' that do not relate to a 'computer program' nor to the selection or the arrangement of the elements of a 'database'. The 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 these circumstances arise if these temporary acts of reproduction are transient or incidental and have no independent economic

[92] Art. 3 Information Society Directive; art. 5, d) Database Directive; Compare: art 4 Computer Program Directive; Computer Program Copyright regularly does not recognise an explicit right of communication to the public.
[93] Art. 4.1. Information Society Directive; art. 5, c) Database Directive; art 4.1., c) Computer Program Directive
[94] Art. 4.2. Information Society Directive; art. 5, c) Database Directive; art 4.2. Computer Program Directive
[95] Art. 3 Rental and Lending Directive (2006); compare: art. 2 Database Directive art 4.1., a) Computer Program Directive
[96] Art. 2.1., a) Rental and Lending Directive (2006)
[97] Art. 2.1., b) Rental and Lending Directive (2006)

significance[98]. The exact scope of this exception has given rise to debate[99]. However, it is clear that this exception can be relevant for a person responding to an emergency who performs 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 find certain information[100]). To the extent that this exception for temporary technical reproductions applies performing those acts without the permission of the right holder does not infringe copyright.

The second relevant exception in the context of emergencies is the mandatory exception for normal use which the Database Directive stipulates regarding database copyright. In relation to the categories of acts that database copyright normally subjects to the authorisation of the right holder this exception states that the lawful user of a 'database' does not need any permission of the right holder to perform these categories of acts provided that performing them is necessary for the purposes of access to and normal use of the contents of the database[101]. With regard to the scope of this exception mainly the condition of qualifying as a 'lawful user' gives rise to uncertainty. The discussion on the interpretation of this notion is similar to the discussion on the meaning of a 'lawful user' in the context of the database *sui generis* right.

The third exception relevant to emergencies is the mandatory exception regarding use for the intended purpose which the Computer Program Directive stipulates in relation to computer program copyright. With regard to the categories of acts that computer program copyright normally subjects to the authorisation of the right holder this exception states that, in the absence of specific contractual provisions, the lawful acquirer of a 'computer program' does not need any permission of the right holder to perform these categories of acts provided that performing them is necessary for the use of the 'computer program' in accordance with its intended purpose, including for error correction[102]. The exact scope of this exception is highly disputed. The interpretation of the notion of a 'lawful acquirer', for example, gives rise to a similar debate as the one on the interpretation of the notion of a 'lawful user' in the context of database copyright and the database *sui generis* right.

A final set of exceptions that are relevant in the context of emergency situations are the exceptions for public security that are found in both ordinary copyright and database copyright. Computer program copyright, it is to be noted, does not have such exceptions concerning public security.

In relation to ordinary copyright the Information Society Directive has given EU Member States the option to introduce a particular exception for public security. The option offered is 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[103]. This exception stipulated by the directive applies to 'works' that do not relate to a 'computer program' nor to

[98] Art 5.1. Information Society Directive
[99] E.g.: 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, p. 727
[100] Compare: recital 33 Information Society Directive
[101] Art. 6.1. Database Directive
[102] Art 5.1. Computer Program Directive
[103] Art 5.3. e) Information Society Directive

the selection or the arrangement of the elements of a 'database'. Some Member States have made use of the option to introduce this exception[104]. In these states the notion of 'public security' is sometimes taken to also cover for example the health of citizens[105]. 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[106].

In relation to database copyright, the Database Directive has also allowed EU Member States to introduce an exception for public security. The option offered is to introduce an exception stating that the categories of acts which database copyright normally subjects to the authorisation of the right holder may be performed without his permission for the purpose of public security. In this case, most Member States have chosen to implement this exception quasi word for word. Given such an implementation, the reference to 'public security' can arguably be taken to cover activities of people responding to an emergency.

8.3. Impact in the context of the eVACUATE-system

What intellectual property rights do, as mentioned, has an impact on the eVACUATE-system. This impact does not depend on the actual venue in which the system is being deployed (e.g. an underground station, a football stadium, an airport or a cruise ship).

8.3.1. Using the system

In light of intellectual property rights people who use the eVACUATE-system to exchange and use data frequently have to take into account the issue of potential intellectual property infringement. This applies to both real-life situations and research phase, e.g. validation demonstrations. The incorporations of data that people will want to use and exchange within the system to organise an evacuation will often turn out to embody an intellectual property protected result of efforts (e.g. text files, images, pictures and maps). The acts involved in exchanging or using these incorporations of data within the system will often qualify as categories of acts which the relevant intellectual property right subjects to the authorisation of the right holder (e.g. 'communicating to the public').

Avoiding intellectual property infringement in using the eVACUATE-system often conflicts with an optimal exchange and use of data to organise emergency evacuations. To avoid intellectual property infringement people using the system sometimes have to discard the opportunity of exchanging or using data in the quickest, cheapest or most extensive way possible.

Merely assessing the intellectual property status of an incorporation of data in view of avoiding an intellectual property infringement can already prove to be burdensome. Incorporations of data embodying an intellectual property protected result of efforts do not

[104] E.g.: §45, 2) German Copyright Law and art. 22 Dutch Copyright Law. Contrary Belgian Copyright Law does not contain such an exception.
[105] S. LÜFT, "UrhG § 45 Rechtspflege und öffentliche Sicherheit" in A. WANDTKE and W. BULLINGER, *Praxiskommentar zum Urheberrecht*, München, Beck, 2014, Nr. 5
[106] E.g.: §45, 2 German Copyright Law

always come with information indicating this fact nor with information to identify and contact the right holder. In addition, there are no official registries of 'works' or 'databases' to verify whether an incorporation of data is indeed covered by copyright or the database *sui generis* right.

In case of an embodiment of an intellectual property protected result of efforts, the possibilities to use and exchange it within the eVACUATE-system without committing intellectual property infringement are often troublesome. They frequently do not allow a truly optimal exchange and use in view of organising emergency evacuations.

The possibility of sticking to acts that fall outside of the scope of the exclusive right granted by the intellectual property rights is a readily available option but mostly of limited practical significance. A person indeed does not require permission from the right holder to lawfully perform these acts. However, people relying on this possibility will often find themselves limited in the acts which they can actually perform concerning the embodiment. 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 exceptions to these categories of acts are often rather narrow. In addition, the scope of these categories of acts and the scope of the relevant exceptions can also turn out to be difficult. This mapping exercise is difficult because of on-going legal debates and – especially in case of the exceptions – differences between the relevant provisions in the national legislation of EU Member States.

The other possibility, namely obtaining the right holder's permission to perform the acts subject to his authorisation, is indeed a gateway to lawfully performing a great range of acts but also comes with disadvantages. A first disadvantage is that it takes time and efforts to conclude agreements with the right holders on a license or transfer of their exclusive rights. A second disadvantage of course is that right holders can make these agreements dependent upon payment.

Currently a person using the eVACUATE-system can be confronted with a situation in which respecting intellectual property rights is a serious obstacle to the exchange or use of an incorporation of data that can help organise an emergency evacuation. In such a situation this person, in essence, has to weigh his potential liability for intellectual property infringement against the usefulness of the actual use of the incorporation of data to safeguarding human health and lives. The problem in this regard is that the outcome of this person's balancing exercise might not always be the outcome that is best for all people involved.

8.3.2. Designing the system

Intellectual property rights also influence the optimal design of the eVACUATE-system. In light of these rights, the system should be designed in such a way that it aids its users in making an informed decision on dealing with the issue of intellectual property infringement. Efforts to that end should be aimed at enabling the system to quickly present users the available information about the intellectual property status of the incorporation of data that they intend to use or exchange. This means presenting users with the available information on whether the incorporation embodies an intellectual property protected result of efforts, on the identity of the right holder and on the terms and conditions that apply to using or

exchanging the incorporation (e.g. the information embedded in a digital file that indicates that a particular type of Creative Commons license applies[107]).

As things stand now, the design of the system should not aim at substituting the user in making decisions on the issue of intellectual property infringement in case of emergencies. (e.g. the eVACUATE-system automatically blocking a particular use of a copyright protected map in order to avoid intellectual property infringement). The machine-readable information on the intellectual property status of incorporations of data is often lacking or too imprecise to allow accurate computerised analyses on the acts that constitute intellectual property infringement. In addition, there is the question whether decisions on avoiding intellectual property infringement in case of emergencies can and should be entrusted to a computer.

8.4. Tackling intellectual property rights

Certain measures can mitigate the difficulties of dealing with intellectual property rights in case of emergency situations. There are means to ensure that avoiding intellectual property infringement poses less of a burden to an optimal use and exchange of data in response to emergencies.

A first measure is addressing foreseeable intellectual property issues in advance. For example, people entrusted with the task of organising the potential evacuation of a football stadium can foresee that their use of the eVACUATE-system will involve floor plans of the stadium. This means that prior to any emergency they can verify the intellectual property status of particular floor plans and if necessary contact the relevant right holders about obtaining permission for the intended use or exchange of the floor plans. These precautions help avoid that using or exchanging the floor plans in case of an actual emergency gives rise to issues of intellectual property infringement.

A second more fundamental measure would be the systematic introduction in intellectual property rights of a uniform exception in relation to emergency situations. A suggestion for such an exception would be, for example, to systematically state that in order to respond to an acute emergency situation all categories of act subject to the authorisation of the right holder may be performed without the permission of the right holder. In this exception the definition of an ‘acute emergency situation’ would serve as the parameter to regulate the scope of the exception. Such an exception could offer significant advantages to achieving an optimal use and exchange of data in order to respond to emergencies. If a situation qualifies as an emergency in the sense of this exception people would have an immediate and cost free opportunity to use and exchange embodiments of intellectual property protected results of efforts without committing intellectual property infringement. This also means that people would no longer have to worry about facing liability for intellectual property infringement when they use or exchange incorporation of data to respond to an emergency as described by the exception.

[107] See in this regard: http://creativecommons.org/licenses/

9. Legal regimes promoting the availability of public sector (geospatial and environmental) data

With regard to the exchange and use of data in the eVACUATE-system, it is also necessary to consider legal regimes that are aimed at promoting the availability of data held by the public sector. In emergency situations the availability of public sector data might be valuable to organising the best possible evacuation (e.g. data held by the local government on the immediate surroundings of the venue that needs to be evacuated).

9.1. Relevant Regimes

To have an overview of the relevant legal regimes on promoting the availability of public sector data it is appropriate to study the Aarhus Directive[108], the PSI Directive[109] and the Inspire Directive[110]. These directives set out the rules which the EU Member States need to implement on promoting the availability of public sector data. In several ways the rules set out by these directives facilitate the lawful exchange and use of public sector data within the eVACUATE-system.

9.1.1. 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[111]. It does so by introducing obligations for public authorities to make such information available to the public, both upon request of applicants and on their own initiative[112].

A. Scope of application

The obligations resulting from the Aarhus Directive relate only to environmental information that is held by or for public authorities of the Member States[113]. This makes 'environmental information' and 'public authority' the two most important parameters in delimiting the scope of application of this directive.

[108] Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, *OJ* L 41, 14.2.2003, p. 26-32 (hereinafter: Aarhus Directive)
[109] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ* L 345, 31.12.2003, p. 90-96 (hereinafter: PSI Directive)
[110] Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), *OJ* L 108, 25.4.2007, p. 1-14 (hereinafter: Inspire Directive)
[111] In doing so, 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.
[112] Art. 1 Aarhus Directive
[113] See: art. 3 and 7 Aarhus 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[114]. First of all, such environmental information can refer to information on the state of the elements of the environment such as air, water or landscape[115]. This includes information on factors (e.g.: noise, radiation and waste)[116] and measures (e.g.: legislation, plans and programs)[117] that are likely to affect the state of these elements. Secondly, environmental information can also mean reports on the implementation of environmental legislation[118], as well as, economic analyses and assumptions related to measures that are likely to affect the state of the elements of the environment[119]. 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[120].

The notion of a public authority is also explicitly explained by the Aarhus Directive. This directive uses the notion of 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 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[121]. 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.

B. Access to environmental information upon request

The Aarhus Directive formulates rules that specify an obligation for public authorities to make their environmental information available upon request[122]. These rules specify several aspects of this obligation.

First of all, the Aarhus Directive determines on what grounds a public authority is to grant or refuse a request to make environmental information available. In this regard, the directive starts by stipulating 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[123]. The directive then derogates from this principle by providing two lists of possible valid reasons for a public authority to refuse an applicant's request to access its

[114] Art. 2.1. Aarhus Directive
[115] Art. 2.1., a) Aarhus Directive
[116] Art. 2.1., b) Aarhus Directive
[117] Art. 2.1., c) Aarhus Directive
[118] Art. 2.1., d) Aarhus Directive
[119] Art. 2.1., e) Aarhus Directive
[120] Art. 2.1., f) Aarhus Directive
[121] Art. 2.2. Aarhus Directive
[122] Art. 3 Aarhus Directive
[123] Art. 3.1. Aarhus Directive

environmental information[124]. The first list enumerates reasons that can be said to relate to formal grounds. This list, more 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[125]. 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 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[126]. 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[127].

Secondly, 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[128]. 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[129].

Thirdly, the directive lays down rules on the opportunity for public authorities to make access to environmental information dependent on payment[130]. The directive more in particular stipulates that public authorities may not charge for examination *in situ* of the information requested[131]. It also forbids charging for access to specified public registers and lists that hold information on the public authorities holding environmental information[132]. Contrary to what is the case for examination *in situ*, the Directive does allow public authorities to charge

[124] Art. 4. Aarhus Directive. 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 national legislations. 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.
[125] Art. 4.1. Aarhus Directive
[126] For the exact description of these reasons, see: art. 4.2. Aarhus Directive which also 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.
[127] Art. 4.2. Aarhus Directive
[128] Art. 3.4. Aarhus Directive
[129] Art. 3.4. Aarhus Directive
[130] Art. 5. Aarhus Directive
[131] Art. 5.1. Aarhus Directive
[132] Art. 5.1. and 3.5. Aarhus Directive

for supplying environmental information, provided that the charge does exceed a reasonable amount[133]. The directive does, however, require public authorities to inform applicants on the charges made[134].

Fourthly, the directive sets public authorities a timeframe 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[135]. This timeframe can be extended to two months if the volume and the complexity of the information requested makes it impossible to handle the request within one month after having received it[136].

Sixthly, the directive requires that a public authority's decision on granting access to environmental information can be subjected to review. The directive more in particular requires an opportunity for the applicant of the request to subject this decision to both administrative and judicial review. The directive also allows Member States to give access to legal recourse to third parties incriminated by the disclosure of information[137].

Finally, it is to be noted that 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[138]. This last aspect includes, for example, making available registers or lists of the environmental information held by public authorities.

C. Active and systematic dissemination of environmental information

The Aarhus directive also lays down rules that result in an obligation for public authorities to disseminate their environmental information on their own initiative[139]. Again, these rules touch upon several aspects of this obligation.

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[140] and stipulates an obligation to make periodic reports[141]. 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[142].

[133] Art. 5.2. Aarhus Directive
[134] Art. 5.3 Aarhus Directive
[135] Art. 3.2., a) Aarhus Directive
[136] Art. 3.2., b) Aarhus Directive
[137] Art. 6 Aarhus Directive
[138] Art. 3.5. Aarhus Directive
[139] Art. 7.1. Aarhus Directive
[140] Art. 7.2. Aarhus Directive
[141] Art. 7.3. Aarhus Directive
[142] Art. 7.5. Aarhus Directive

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[143]. It also requires Member State to ensure that environmental information progressively becomes available in electronic databases which are easily accessible to the public through public telecommunication networks[144]. 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[145].

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 who could enable the potentially affected public to take measures against this threat[146]. 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[147]. 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 legislation[148].

9.1.2. Public Sector Information Directive

The PSI Directive (Public Sector Information Directive) stipulates rules to enhance the re-use of existing public sector information, by applicants making a request to do so[149]. According to this directive such '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[150]. 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[151].

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

[143] Art. 7.1. Aarhus Directive
[144] Art. 7.1. Aarhus Directive
[145] Art. 7.6. Aarhus Directive
[146] Art. 7.4. Aarhus Directive
[147] Compare: 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, p. 261
[148] Art. 7.4. Aarhus Directive
[149] Art. 1.1. PSI Directive
[150] Art. 2.4. PSI Directive
[151] Art. 2.4. *in fine* PSI Directive

created, for purposes different than the original one, but still for the performance of the public task[152].

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.

A. 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[153]. So, 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. Both this notion of documents and this notion of public sector bodies are interpreted broadly in this regard. A document refers to any content or part of it, whatever its medium. So this includes, for example, data written on paper, data stored in electronic form and data incorporated in sound, visual or audio-visual recordings[154]. A public sector body refers to the State, regional and local authorities and different sorts of bodies governed by public law[155].

However, the PSI Directive also explicitly excludes certain types of documents from its scope of application. In this 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 educational, research and cultural establishment[156]. 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[157].

B. Rules on re-use

The PSI Directive formulates rules which public sector bodies have to observe in deciding upon an applicant's request to re-use their documents. Again, these rules touch upon different aspects of responding to such a request.

First of all, the directive determines the elements on which a public sector body is to base its grant or refusal of the request to re-use documents. The general principle in this regard is that if a public sector body holds a document that is not explicitly excluded from the scope of

[152] 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.
[153] Art. 1.1. PSI Directive
[154] Art. 2.3. PSI Directive
[155] Art. 2.1. PSI Directive
[156] Art. 1.2. PSI Directive
[157] Art 1.3 PSI Directive and Recital 9 PSI Directive

application of the PSI Directive this public body is to allow the re-use of this document in accordance with the rules set out by this Directive[158]. So, 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[159].

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[160].

A second aspect, relates to the charges which sector bodies make for the re-use of documents. The directive requires public sector bodies to be transparent about these charges and, in principle, does not allow these charges to exceed the marginal costs incurred for their reproduction, provision and dissemination[161].

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[162]. In relation to licences, the directive encourages to make standard licences available that can be adapted to meet particular licence applications and that can be processed electronically[163].

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[164]. 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[165].

Thirdly, the directive compels Member State to make practical arrangements that facilitate the search for documents available for re-use. As examples of such practical arrangements

[158] Art. 3.1. PSI Directive
[159] Art. 3.2. PSI Directive
[160] Art. 5 PSI Directive
[161] Art. 6 PSI Directive
[162] Art. 8.1. PSI Directive
[163] Art. 8.2. PSI Directive
[164] Art. 10 PSI Directive
[165] Art. 11 PSI Directive

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[166].

Finally, the PSI Directive also gives public sector bodies instructions on how to handle an applicant's request to re-use a document[167]. 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[168]. 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[169]. 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[170]. 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[171]. 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[172].

9.1.3. Inspire Directive

The Inspire Directive lays down rules to establish the *Infrastructure for Spatial Information in the European Community* (INSPIRE)[173]. It does so, for the purposes of policies and activities relating to the environment. There are three objectives which the Inspire Directive wants to achieve in this domain by establishing this Inspire infrastructure for spatial information. A first and most important objective is to make it easier for public authorities to access, share and use, each others spatial data sets and services in performing their public tasks regarding the environment[174]. In this regard the Inspire Directive uses the same broad notion of a public authority as the Aarhus Directive does[175]. A second, minor objective is to create an opportunity for third parties to link their spatial data and services to the Inspire infrastructure[176]. Such a third party refers to any natural or legal person, other than a public authority[177]. 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

[166] Art. 9 PSI Directive
[167] Art. 4 PSI Directive
[168] Art. 4.1. PSI Directive and 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, p. 143
[169] Art. 4.2. PSI Directive
[170] Art. 4.3. PSI Directive
[171] Art. 4.3. *in fine* PSI Directive
[172] Art. 4.4. *in fine* PSI Directive
[173] Art. 1.1. Inspire Directive
[174] Art. 17 Inspire Directive
[175] Art. 3.9. Inspire Directive
[176] Art. 12 Inspire Directive
[177] Art. 3.10. Inspire Directive

infrastructure[178]. The Inspire Directive explicitly stipulates that its provisions are without prejudice to the Aarhus Directive and without prejudice to the PSI Directive[179].

A. Scope of application

The rules which 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[180]. 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[181]. 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[182]. 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[183]. The fifth condition is that the data set has to constitute the reference version[184]. 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[185]. 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. To be noted also is that the Inspire Directive does not require collection of new spatial data[186].

B. 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 Union (ex – Community). Its approach to creating this infrastructure is to determine specifications that are to be met by the infrastructures for spatial information operated by the Member States[187]. The directive determines these specifications through a combination of stipulating certain general rules in this regard and 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, in what is known as a 'Comitology Procedure'. The roadmap for the full implementation of the Inspire Infrastructure currently stretches to 2020[188].

[178] Art. 11 Inspire Directive
[179] Art. 2.1. Inspire Directive
[180] Art. 4.1., a) Inspire Directive
[181] Art. 4.1., d) Inspire Directive
[182] Art. 4.1., b) Inspire Directive
[183] Art. 4.1., c) Inspire Directive
[184] Art. 4.2. Inspire Directive
[185] Art. 4.5. Inspire Directive
[186] Art. 4.4. Inspire Directive
[187] Art. 1.2. Inspire Directive
[188] http://inspire.ec.europa.eu/index.cfm/pageid/44

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[189]. The second area relates to the technical arrangements for the interoperability of these spatial data sets and services[190]. 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[191]. 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[192]. A fifth area concerns coordination, monitoring and reporting obligations of the Member States in relation to the implementation of their infrastructures for spatial information[193].

Finally, the Infrastructure for Spatial Information in the European Community, established by the Inspire Directive, also has the Commission operate an Inspire geo-portal[194]. This Internet portal, which is operated at the Community level, provides access to the services which Member States operate for the spatial data sets under this directive[195].

C. 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 of the previous bodies or persons qualifying as a public authority,

[189] Art. 5 Inspire Directive
[190] Art. 7 Inspire Directive
[191] Art. 11 Inspire Directive
[192] Art. 17 Inspire Directive
[193] Art. 18-21 Inspire Directive
[194] Art. 15 Inspire Directive
[195] http://inspire-geoportal.ec.europa.eu/

has public responsibilities or functions relating to the environment or provides public services relating to the environment[196].

C.1. Making available

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[197].

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[198]. 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. So, 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[199]. 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[200]. Secondly, in case this public authority of 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[201].

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[202]. The directive also explicitly stipulates that Member States are to ensure that any information needed to comply with these specifications is made available to public authorities[203].

C.2. Sharing

Secondly, 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[204]. This directive does so by requiring measures that

[196] Art. 3.9 Inspire Directive
[197] Art. 7.3. Inspire Directive
[198] On the scope of application of the Inspire Directive see: art. 4 Inspire Directive
[199] Art. 4.1. and 4.3. Inspire Directive
[200] Art. 4.2. Inspire Directive
[201] Art. 4.6. Inspire Directive
[202] Art. 7.3. Inspire Directive
[203] Art. 10.1. Inspire Directive
[204] Art. 17 Inspire Directive

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[205].

It is but a specific group of public authorities that faces the requirements of the Inspire Directive on sharing spatial data sets and services in view of their public tasks relating to the environment. The directive only requires to enable such sharing between the public authorities of a Member state that qualify either, as the government or other public administration, or as a natural or legal person performing public administrative functions under national law[206].

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 indeed 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[207]. 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[208]. As a general rule, the directive merely requires that such charges and licenses are kept to the minimum required to ensure quality and supply, a reasonable return on investment, and possible self-financing requirements of public authorities[209]. In addition, the directive does not require any sharing of spatial data sets and services, if doing so would compromise the course of justice, public security, national defence or international relations[210].

In order to facilitate the sharing of spatial datasets and services between the different levels of authorities, a working group was set up to draft a proposal on how to regulate their exchange in different situations, including emergency situations. Although the focus of the working group was the exchange of information from the Member States to the Union institutions and bodies, it could be recommended that the general principles and good practices that the group develops should become the guiding principles in the exchange of data between the Member States in emergency situations.[211]

One of the situations which the drafting group considered was the case of data and services sharing in emergency situations. The group acknowledges that in cases of emergency the established normal procedures would slow down the emergency response, which might lead to more loss of human life and property. The group focuses on the actions which the producers of data can plan and provide in emergency situations in order to provide the necessary data without delay. It suggests that one might either conclude specific

[205] Art. 17.1. Inspire Directive
[206] Art. 17.1. Inspire Directive
[207] Art. 17.2. Inspire Directive; 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, p. 165-166
[208] See art 17.3. Inspire Directive that stipulates an exception relating to Community institutions and bodies
[209] Art 17.3. Inspire Directive; With regard to the possibilities to charge public authorities from other Member States, Community institutions and bodies of the Community and bodies established by international agreements, see: art. 17.4.-5 and 17.8 Inspire Directive
[210] Art. 17.7. Inspire Directive
[211] "Good Practice in Data and Service Sharing," Drafting Team – Data and Service Sharing, European Commission, 12.12.2011, pg. 5

agreements for emergency access or emergency access might be regulated by the regular license which provides for mechanism for a more extensive provision of data and services.[212]

In cases where the normal license accommodates also emergency situations, one might envisage, for example, that the potential user has access to the spatial datasets and services 24/7 or he can access them over an emergency line. The most important thing is that he is aware of the procedure he should follow. In cases where no license exists, there still must be procedures in place for emergency access, the information on which is widely available and easily accessible. In both cases the procedures must be established and communicated to the public in advance and it should be monitored whether they are effective enough. In those situations where access to datasets and services is regulated through a license but no such license has been concluded as of the time of the emergency, it should be possible in principle to grant access to the requested services first and afterwards conclude the necessary agreement without unnecessary formalities. Whatever the framework for sharing the datasets and services is chosen, it is important that the response takes as little time as possible.[213]

D. Third parties within INSPIRE

Secondly, 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[214].

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[215]. 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[216].

The consequence of a third party linking his spatial data sets and services to the Inspire network services, is that they become available both to the public at large and public authorities. The public access to his 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[217]. 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 that third party[218]. It is to

[212] Ibid, pg. 53
[213] Ibid, pg. 54
[214] Art. 2.10. Inspire Directive
[215] Art. 12 Inspire Directive
[216] Art. 10 Inspire Directive
[217] Art. 14 Inspire Directive
[218] Art. 4.5. Inspire Directive

be noted however that, 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[219].

E. Public access within INSPIRE

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 more in particular requires that the public has access to these spatial data sets and services through the network services within the Inspire Infrastructure[220].

The principle, laid down by the Inspire Directive is that 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[221]. 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[222].

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[223]. 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[224]. 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 is weighed against the interest served by limiting or conditioning the access[225]. 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[226].

---

[219] Art. 17 Inspire Directive
[220] Art. 11.1. Inspire Directive; 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, p. 100 ff.
[221] Art. 11.1. Inspire Directive
[222] 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, p. 102
[223] Art. 13.1. Inspire Directive
[224] For the exact description of these reasons, see: art. 13.1. Inspire Directive
[225] Art. 13.2. Inspire Directive
[226] Compare: art. 2.1. Inspire Directive

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[227]. With regard to view service, the directive, in principle, requires them to be offered for 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[228]. 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[229]. Finally, the directive explicitly states that view services may make data available in a form that prevents their re-use for commercial purposes[230].

9.2. Impact in the context of the eVACUATE-system

The legal regimes set out by the Aarhus, PSI and Inspire Directive also have an impact on the eVACUATE-system. Again, this impact does not depend on the actual physical venue in which the eVACUATE-system is being deployed (e.g. an underground station, a football stadium, an airport or a cruise ship).

9.2.1. Using the system

The legal regimes set out by the Aarhus, PSI and Inspire Directive make it easier to include three types of public sector data in the use of the eVACUATE-system: 'environmental information', 'spatial data' and 'documents' held by the public sector. In several ways these regimes facilitate the lawful exchange and use of these types of public sector data within the system. First of all, these regimes incite the public sector to enhance the availability of these types of public sector data. Secondly, these regimes clarify the conditions under which people and public sector bodies can lawfully access, exchange or use these types of public sector data. Finally, these regimes also stimulate public bodies to minimise practical impediments to a potential access, use or exchange of these types of public sector data (e.g. imposing mandatory technical specifications for data sets and services included within the Inspire Infrastructure).

Nevertheless the legal regimes resulting from the Aarhus, PSI and Inspire Directive do not eliminate all hurdles to a lawful, ready inclusion in the eVACUATE-system of 'environmental information', 'spatial data' and 'documents' held by the public sector. In practice achieving such an inclusion can still turn out to be strenuous or even impossible.

A first remaining hurdle is that a person using the system both in real-life situations and during the demos needs to perform a complex three-step analysis to establish whether his intended exchange or use of data within this system is indeed governed by the rules resulting

[227] Art. 14.1. Inspire Directive
[228] Art. 14.1-2 Inspire Directive
[229] Art. 14.4 Inspire Directive
[230] Art. 14.3 Inspire Directive

from the Aarhus, PSI or Inspire Directive. The first step in this analysis requires examining the nature of the data to which the intended use or exchange relates. This step requires assessing whether the 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 in the analysis requires an examination of the intended use or exchange of the data. This examination is to assess whether the intended use or exchange of the data involves 'accessing', 'sharing' or 're-use' as defined by the relevant directives. The third step in the analysis requires the person to assess whether he will use or exchange the data acting as a private person or, on the contrary, as a public authority or a public sector body as defined by the relevant directives.

A second hurdle are the time frames which the Aarhus, PSI and Inspire Directive set for public bodies to decide on requests in relation to the possible access, use or exchange of the data that they hold. These time frames well exceed the time frame in which people making such a request in the performance of an actual emergency evacuation need a decision.

A third hurdle relates to the possible decision of the public body on requests to access, use or exchange 'environmental information', 'spatial data' or 'documents' held by the public sector. The regimes set out by the Aarhus, PSI and Inspire Directive provide public bodies with several grounds to refuse such requests (e.g. respect for intellectual property rights and privacy law). These regimes also allow public bodies to make their grant of such requests dependent upon conditions such as payment or accepting a licence agreement. The Aarhus, PSI and Inspire Directive do not oblige public bodies to unconditionally grant requests that seek the access, use or exchange of their data in order to respond to an emergency situation.

9.2.2. Designing the system

The legal regimes set out by the Aarhus, PSI and Inspire Directive also have an influence on the optimal design of the eVACUATE-system. Given the efforts which these legal regimes make to enhance the availability of public sector data, the system should be designed in such a way that there are minimal technical difficulties to effectively process these data. This requires taking into account the formats which public bodies usually use to store 'environmental information', 'spatial data' and 'documents' (e.g. the formats that result from the mandatory technical specifications for spatial data sets and services within the Inspire Infrastructure).

9.3. Optimising the integration of public sector data

Certain measures can enhance the benefits in emergency situations of the legal regimes set out by the Aarhus, PSI and Inspire Directive. It is possible to create better opportunities for people providing emergency response to rely on 'environmental information', 'spatial data' and 'documents' held by the public sector.

A first measure, once again, is to deal with the availability of relevant public sector data in advance. For example, prior to any emergency the safety staff of an underground station should screen whether organising a potential evacuation of the station can benefit from the availability of any 'environmental information', 'spatial data' or 'documents' held by public bodies. The safety staff should then submit requests to access, use or exchange such data

which this assessment has identified as being useful. Taking these precautions helps ensure a maximum availability of relevant data in case of an actual emergency in the underground station.

Other possible measures relates to implementing the legal regimes set out by the Aarhus, PSI and Inspire Directive in a way that takes into account the need for quick and easy availability of data in case of emergency situations. A first such measure is to have public bodies offer a quick possibility to conclude pre-existing licences tailored to emergency situations. A second such measure would be to instate a rule requiring public bodies to decide immediately if a request to access, use or exchange their data is submitted in relation to actual emergency situations. Potentially this rule could also instruct the public body that in case of such an emergency it is to interpret the grounds for refusing the request in a restrictive way and to refrain from imposing conditions such as payment or the acceptance of a licence agreement. Alternatively, this rule could also instruct the public body that in case of an acute emergency licensing issues are to be settled only afterwards[231].

[231] For more examples of such measures, see: INSPIRE guidance document, "Good practice in data and service sharing", DT-DSS 18/09/2009, p. 59 and http://inspire-forum.jrc.ec.europa.eu/pg/pages/view/26329/

10. Conclusion

This deliverable examined the data protection and privacy implications of the technologies under design in eVACUATE. It also studied the opportunities to exchange environmental and geo-spatial data in cases of emergency, as well as certain Copyright and IPR issues.
The main recommendations with regards to privacy and data are protection are the following:

- Keep the eVACUATE system as a whole latent until an emergency is identified. This is without prejudice to the fact that the certain sensors, which collect personal data, such as CCTV, could be kept on as the end-users are authorized currently. In principle, sensors that process personal data should be switched on only when the data they process would be necessary in a particular situation, i.e. on a need-to-know basis. This will differ depending on whether the end-user faces a normal situation or an emergency. The end-user should decide which sensors should be switched on at a particular time. Thus, the risks accompanying the fusion of all data from all the sensors into one platform (i.e. SOFIA), will be mitigated;
- Respect principles of necessity and proportionality to decide which sensors and when they should be switched on and interconnected;
- When introducing the sensors, their purpose should be clearly articulated and narrowly defined so that it is used only for purposes of evacuation/emergency response and not for other, incompatible purposes;
- The usage of the eVACUATE solution should be fair and lawful, i.e. in compliance with European and local legislation;
- eVACUATE should collect only the minimum data necessary to react to a particular situation;
- The accuracy of the different sensors should be ensured. eVACUATE is a research project and further development of certain technologies will continue after eVACUATE, e.g. in other research projects. In the development of these technologies the issue of accuracy should be adequately addressed;
- The personal data should not be stored for longer than necessary, i.e. timely deletion of the data should be ensured;
- The security of data at all times should be guaranteed;
- The data protection rights of all concerned individuals should be respected;
- Respect the requirements of IPR and Copyright.

As to handling environmental and geo-spatial data, the deliverable has given guidance on the existing EU regimes, which should be followed. However, it is recommended to the legislator that clearer rules should be established for exchange of such data in emergency cases.

11. Sources

Academic:

Bennett, C. and Haggerty, K. (eds), "Security Games: Surveillance and Control at Mega-Events, Routledge, 2011

BERBERICH, M., "EuGH: Eingriff spezialisierter Metasuchmaschinen in Datenbanken", *MMR* 2014

boyd, D and Crawford, K., "Six Provocations for Big Data," Paper to be presented at Oxford Internet Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 21, 2011

Bygrave, L., "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling," *Computer Law & Security Report*, 2001, volume 17, pp. 17–24; also published in *Privacy Law & Policy Reporter*, 2000, volume 7, pp. 67–76

CLARK, S., "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

Coudert, F., "+Spaces, Deliverable 2.3, Ethical Issues Report," 28 June 2010

Coudert, F., "When video cameras watch and screen: Privacy implications of pattern recognition technologies," Computer Law and Security Review 26 (2010)

Coudert, F and Dumortier, J., "Intelligent video surveillance networks: data protection challenges"

DYVINE, Deliverable 5.1, "Preliminary Version of Legal Issues," 09 July 2007

DYVINE, Deliverable 5.2, "Final Version of Legal Issues," 7 March 2008

GOTZEN, F., "Art. 1" in F. BRISON and H. VANHEES (eds.), *Huldeboek Jan Corbet. De Belgische auteurswet. Artikelsgewijze commentaar*, Brussel, Larcier, 2009

JANSSEN, K., *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

Jasmontaite, L. and De Hert, P., "The EU, children under 13 years, and parental consent: a human rights analysis of a new age-based bright-line for the protection of children on the Internet," *International Data Privacy Law 2014*

KÖHLER, M., "Der Schutz von Websites gemäß §§ 87 a ff. UrhG", *ZUM* 1999

LEISTNER, M., *Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht. Eine Untersuchung zur Richtlinie 69/9/EG und zu ihrer Umsetzung in das deutsche urheberrechtsgesetz*, München, Beck, 2000

LEISTNER, M., "Die Landkarte als Datenbank. Überlegungen zum Datenbankschutz für topografische Karten und geografische Daten." *GRUR* 2014

LOEWENHEIM, U., "Abschnitt 2. Das Werk" in G. SCHRICKER, *Urheberrecht Kommentar*, München, C.H. Beck, 2006

Lüft, S., "UrhG § 45 Rechtspflege und öffentliche Sicherheit" in A. WANDTKE and W. BULLINGER, *Praxiskommentar zum Urheberrecht*, München, Beck, 2014, Nr. 5

STROWEL, A., "La contrefaçon and droit d'auteur: conditions et preuve ou *pas de contrefaçon sans 'plagiat'*" , *Auteurs & Media* 2006

THUM, D., "UrhG § 87a Begriffsbestimmungen" in A. WANDTKE and W. BULLINGER, *Praxiskommentar zum Urheberrecht*, München, Beck, 2008, Nr. 55

THUM, D. and K. HERMES, "UrhG § 87c Schranken des Rechts des Datenbankherstellers" in A. WANDTKE and W. BULLINGER, *Praxiskommentar zum Urheberrecht*, München, Beck, 2014, Nr. 37

VANOVERMEIRE, V., "The Concept of the Lawful User in the Database Directive", *I.I.C.* 2000

Article 29 Working Party, "Opinion 04/2004 on the Processing of Personal Data by means of Video Surveillance," adopted on 11th February 2004

Article 29 Working Party, "Opinion 4/2007 on the concept of personal data," adopted on 20th June 2007

Article 29 Working Party, "Opinion 15/2011 on the definition of consent," adopted on 13 July 2011

Article 29 Working Party, "Opinion 02/2013 on apps on smart devices," adopted on 27 February 2013

Article 29 Working Party, "Opinion 1/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector," 27 February 2014

Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC," adopted on 9 April 2014

Legislative:

Charter of Fundamental Rights of the European Union, OJ C 2008/C 364/01

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981

Council of Europe, Committee of Ministers, Recommendation No. R(87) 15 of the Committee of the Ministers to Member States regulating the use of personal data in the police sector, 17 September 1987

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, O.J. L 281, 23.11.1995

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and electronic communications)

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, L337/11-36, 18.12.2009

Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE)

Commission Regulation (EU) No 268/2010 of 29 March 2010 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards the access to spatial data sets and services of the Member States by Community institutions and bodies under harmonised conditions, O.J. L. 83/8

Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, *OJ* L 41, 14.2.2003

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ* L 345, 31.12.2003

Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (codified version) *OJ* L 376, 27 December 2006

Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version), *OJ* L 372, 27.12.2006

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, *OJ* L 167, 22 June 2001, p. 10–19 (hereinafter: Information Society Directive)

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ* L 077, 27 March 1996, p. 20-28 (hereinafter: Database Directive)

Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version), *OJ* L 111, 05 May 2009, p. 16-22 (hereinafter: Computer Program Directive)

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM (2012) 10 final, Brussels 25. 01. 2012

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) COM (2012) 11 final, Brussels, 25.1.2012

Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (notified under document number C(2009) 3200) (2009/387/EC) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF

SOLAS Convention

Spanish Law:

Real Decreto 203/2010, de 26 de febrero, por el que se aprueba el Reglamento de prevención de la violencia, el racismo, la xenofobia y la intolerancia en el deporte

Ley 19/2007, de 11 de julio, contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte

Case-law:

CJEU, C-203/02 *BHB v. William Hill*, 9 November 2004

CJEU, C-393/09 *Bezpečnostní softwarová asociace*, 22 December 2010

CJEU, C-145/10 *Painer,* 1 December 2011

CJEU, C-202/12 *Innoweb vs Wegener ICT Media*, 19 December 2013

CJEU, C-490/14 *Verlag Esterbauer*, 16 January 2015

ECtHR, *Handyside v United Kingdom*, Application Nr. 5493/72, 7 December 1976

ECtHR, *Peck vs the United Kingdom*, No 44647/98, 28 January 2003

ECtHR, *MM v United Kingdom*, Appl. No. 24029/07, 13 November 2012

Other:

"Good Practice in Data and Service Sharing," Drafting Team – Data and Service Sharing, European Commission, 12.12.2011

INSPIRE guidance document, "Good practice in data and service sharing", DT-DSS 18/09/2009

http://creativecommons.org/licenses/

Annex A – list of acronyms

Acronym	Meaning
AER	Active Evacuation Route
AIA	Athens International Airport
API	Application Programming Interface
ASRS	Anoeta Stadium San Sebastian
CFREU	Charter of Fundamental Rights of the European Union
CCTV	Closed-Circuit Television (Video Surveillance)
COP	Common Operational Picture
ECHR	European Convention of Human Rights
EOC	Emergency Operation Centre
GDPR	General Data Protection Regulation
IPR	Intellectual Property Rights
METB	Metro Bilbao
PA	Public Address
PIA	Privacy Impact Assessment
PSI	Public Sector Information
RFID	Radio Frequency Identification System
SOFIA	Smart Objects For Intelligent Applications