eVACUATE

FP7-313161

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

HIGH LEVEL ETHICAL AND LEGAL FRAMEWORK, FORMULATING ETHICAL AND LEGAL REQUIREMENTS FOR EVACUATE

Deliverable Identifier:	D.11.1
Delivery Date:	October 14, 2013
Classification:	Public
Editor(s):	Diana Dimitrova (ICRI/KUL), Bjorn Coene (ICRI/KUL)
Document version:	0.2 - 2013
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	High level ethical and legal framework, formulating ethical and legal requirements for eVACUATE	
Editors	Name	Partner
	Diana Dimitrova, LL.M.	ICRI/KUL
	Bjorn Coene	ICRI/KUL
Contributors	Name	Partner
	Diana Dimitrova, LL.M.	ICRI/KUL
	Bjorn Coene	ICRI/KUL
Peer Reviewers	Name	Partner
	Francois Drezet	STX
	Elisabet Terrades Boix	INDRA
Format	Text - Ms Word	
Language	EN - UK	
Work-Package	WP 11	
Deliverable number	D11.1	
Due Date of Delivery	30/09/2013	
Actual Date of Delivery	14/10/2013	
Dissemination Level	PU	
Rights	eVACUATE Consortium	
Audience	☒ public ☐ restricted ☐ internal	
Date	14/10/2013	
Revision	10/10/2013	
Version	1.0	
Edited by	Diana Dimitrova; Bjorn Coene	
Status	☐ draft ☐ Consortium reviewed ☐ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	06/09/2013 25/09/2013	Revision comments provided on the two respective dates by the assigned reviewers STX-FR and INDRA.	KUL
0.2	10/10/2013	Revision comments provided by STX-FR and INDRA	KUL, STX, INDRA
0.9	11/10/2013	Quality Check	EXUS
1.0	14/10/2013	Final Version	KUL

Table of Contents

Table of Figures

Executive Summary

eVACUATE is an FP7 Project which focuses on the management of large crowd gatherings in emergency situations. In particular, it sets out to improve the decision-making process during evacuation by providing better situational awareness in order to reduce the loss of human life. This is to be achieved through the use of different sensors and technologies for the gathering, fusing and analyzing of different types of information. In addition, the project aims at improving the information and communication infrastructure to not only gather information but also to distribute it to the relevant actors. In the end, the system will be tested at 4 pilot demonstrations for validation – a cruise ship, an airport, a metro station and a stadium.

The current deliverable is the first deliverable on legal and ethical aspects. It sets out to outline and analyze the high-level ethical and legal framework and derive legal requirements which apply to the eVACUATE project. More specifically, it analyzes the legal and ethical issues that have to be considered during both the research and later during the operational phase of eVACUATE.

The analysis begins by exploring aspects of responsibility of the different public and private actors in the management of large crowds, including carrying out evacuations, giving as examples the situation at the 4 different scenarios. It then goes on to define the possible liabilities in cases of breach of these responsibilities. The deliverable pays particular attention to handling vulnerable groups, such as disabled persons and children, who are members of large crowds.

In the process of managing crowds, the responsible actors are supposed to take measures to ensure crowd safety to prevent crowd disasters and to respond to disasters once they have occurred. However, these safety measures have to respect other fundamental rights of the crowd members such as privacy and data protection. Thus, the correct balance between the different rights has to be struck. The deliverable will outline the requirements that stem from the rights to privacy and data protection in light of the measures of crowd control.

In addition, the deliverable provides a brief analysis of the privacy and data protection requirements that have to be complied with during the validation phase of the project when demonstrations will be held at the four venues – the STX cruise ship, the Athens International Airport (AIA), the Bilbao metro station (METB) and the Anoeta Stadium in San Sebastian (ASRS).

1. Glossary

Muster station – a place on a ship where people should gather in emergency cases.

RFID – "technology that uses electromagnetic waves to communicate with RFID tags, with the possibility of reading the unique identification numbers of the RFID tags or perhaps other information stored in them."[1]

RFID Tags – "composed of electronic memory that is readable and perhaps writable, and antennae."[2]

RFID Readers – "used to read the information on RFID Tags."[3]

RFID Applications – "process information developed through the interaction of RFID tags and RFID Readers […] supported by back-end systems and networked communication infrastructures."[4]

TETRA (Terrestrial Trunked Radio) – a professional mobile radio and two-way transceiver (walkie talkie) specification.

[1] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf, p. 3

[2] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf, p. 3

[3] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, p. 3

[4] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, p. 4

2. Introduction

2.1. Purpose and scope of the deliverable

The purpose of the present deliverable is to outline the legal and ethical framework which applies to the eVACUATE project. It examines the responsibilities of the different actors who are responsible for ensuring crowd safety. These responsibilities range from putting in place adequate measures to prevent crowd disasters from occurring to implementing measures and procedures to react to these disasters by, for example, carrying out a successful evacuation.

In addition, these measures have to take into account the needs of vulnerable groups such as children and disabled persons. The measures also have to be balanced against other fundamental rights, i.e. privacy and data protection. The purpose of the present deliverable is thus to provide a high-level legal and ethical analysis of all the above-mentioned aspects, which will be further specified in the following deliverables and applied to the system developed in eVACUATE.

Last but not least, the deliverable also provides an examination of the legal and ethical aspects of the research phase of the project, in particular the data protection requirements which have to be complied with when performing the four validation demonstrations.

2.2. Methodology

The current deliverable is prepared on the basis of research into the applicable legislation, case-law and soft-law, materials from the four end-users, as well as academic literature in order to provide a comprehensive and comprehensible analysis of the legal and ethical framework of managing large crowds.

2.3. Structure of the deliverable

The deliverable is structured as follows. It first provides an overview of some of the legal and ethical issues which have to be considered in the course of management of large crowds (prevention and crowd disaster management) by the different private and public authorities who are responsible for crowd management. It provides as examples the situation of the four use case scenarios. Then the deliverable examines the needs of vulnerable groups as members of large crowds.

The deliverable continues with an analysis of the privacy and data protection requirements and principles, since the crowd safety measures which have to be implemented

by the responsible authorities have to be balanced against the fundamental rights of privacy and data protection.

3. Legal and ethical aspects of crowd management

3.1. Introduction

The purpose of this section is to examine the legal and ethical issues associated with the process of management of large crowds. The responsibilities of the private and public actors involved in crowd management refer to putting in place measures to prevent the occurrence of large crowd disasters and to taking adequate measures to respond effectively and efficiently to crowd disasters. This section addresses the responsibilities and liabilities of those involved in emergency response (e.g. evacuation) in situations where there are large crowd gatherings at different types of venues, taking as examples the four scenarios: cruise ship, airport, stadium and metro.

3.2. Large crowd gatherings

Gatherings of large crowds - e.g. at football matches and concerts, busy metro stations and airports, large cruise ships – require adequate measures to ensure the effective management of those crowd assemblies. Crowd management, thus, aims at the effective organization of the movement of crowds[5] to ensure their safety. The actors, both private and public, who manage these crowds, should put in place relevant measures to ensure crowd safety, since crowd safety is "a major responsibility in heavily used public facilities."[6]

Ensuring the safety of the crowd is essential since ultimately safety means protecting human life. In general, the state authorities have both positive and negative obligations to protect *inter alia* the dignity and life of the individuals and guarantee their right to equal treatment. These obligations apply to all Member States of the Council of Europe through the European Convention on Human Rights (Article 2 ECHR) and to the Member States of the European Union through the Charter of Fundamental Rights of the European Union (Article 2 CFREU). In addition, similar provision can be found in national constitutional provisions, for example in the German Federal Constitution.[7]

Pursuant to these provisions, State authorities shall on one hand refrain from actions causing death of the individuals within their jurisdiction. On the other hand they should take

[55] J. L. Abbott and M.W. Geddie, "Event and venue management: minimizing liability through effective crowd management techniques," *Event Management,* Vol. 6, pp. 259-270, p. 260
[6] J. D. Sime, p. 313
[7] Articles 1, 2, and 14 Grundgesetz für die Bundesrepublik Deutschland of 23 May 1949 (BGBI. S.1), last modified by Law of 11 July 2012 (BGBI. S. 1478)

the relevant measures to safeguard the lives of individuals.[8] In the context of emergency relief, the scope of the positive obligation of state authorities depends on the particular circumstances of the situation, i.e. the nature of the threat and the extent to which it can be mitigated.[9]

Therefore, state authorities should ensure (e.g. through relevant laws and regulations) that adequate measures are put in place both by private and public actors during all the stages of managing crowds: the prevention of crowd disasters (pre-crisis stage), the reaction to a disaster once it has occurred (crisis stage), as well as the mitigation measures after the crisis is over (post-crisis).

The crisis stage occurs when the crowd gets trapped, falls in a hazardous location, becomes incapacitated because of unstable hazardous conditions or a combination of any of these situations,[10] i.e. the crowd has lost control. For example, the crowd crisis could be caused by a security threat such as a bomb threat at an airport, by disasters such as fire, or by the unruly behavior of the members of the crowd, such as hooliganism during football games. One of the possible reactions to a crowd disaster situation is ordering the evacuation of the members of the crowd, for example on a cruise ship to the muster stations or even to the life boats. Procedures on crowd control include "creating situations, models, and decision-making processes needed for the successful direction of equipment under a unified command."[11]

The different authorities (private and public) engaged in the management of crowd gatherings face different responsibilities, while they interact with each other to ensure crowd safety. These responsibilities depend on the rules by which the actors are bound and on the specific context of the crowd gathering, as situations and responsibilities are not identical.

3.3. Responsibilities for emergency prevention and response

In principle, the entities responsible for the management of large crowd gathering events seek to avoid the occurrence of crowd disasters from occurring. The adequate preventive measures vary according to the venue of the gathering. Once a disaster has occurred, the actors involved in the management of the crowd seek to react in such a way as to minimize the impact of the disaster.

[8] ECtHR, *Budayeva and others v Russia*, Applications nos. 15339/02, 21166/02, 20058/02, 11673/02 and 15343/02, 29.09.2008, par. 128
[9] *Budayeva*, par. 137
[10] J. D. Sime, "Crowd facilities, management and communications disasters," *Facilities, Vol. 17, Number 9/10, 1999, pp. 313 – 324,* p. 314
[11] Abbott and Geddie, p. 264

The following paragraphs provide various examples of crowd safety measures and the different roles and duties of the various private and public entities engaged in crowd safety. The examples are taken from the four use case scenarios: Anoeta stadium, STX cruise ship, Bilbao metro and Athens International Airport.[12]

3.3.1. Anoeta Stadium San Sebastian

In Europe, when football games are played under the auspices of UEFA, the UEFA Safety and Security Regulations apply.[13] Pursuant to these regulations, football organizers should take, *inter alia*, the following measures: appointment of a security coordinator,[14] cooperation with public authorities,[15] segregation of spectators and group dispersal strategy,[16] stadium inspection,[17] control of ticket sales,[18] screening and searching of spectators at entrances,[19] installed CCTV cameras which are monitored by the chief police officer or the stadium security officer,[20] keeping all exit doors and gates open/unlocked to be ready to be used as escape routes in emergency cases, and all passageways, corridors and stairs, etc., clear from obstructions,[21] ban on consumption of alcohol,[22] etc.

At the specific stadia across Europe, further rules, in compliance with local regulations, apply. For example, the following safety measures are taken at the Anoeta Stadium in San Sebastian. The stadium disposes of two camera systems, with 70 cameras installed inside the stadium. There are special cameras that are dedicated to the violent local supporters who are known in advance. A monitoring system for traffic control is installed outside the stadium.

The number of attendees during matches is controlled through the AVET system for access control at the gates and thus the number of persons in each section is known. A new system for access control for all events (matches and concerts) will be introduced in 2013 which will check all documents. Communication is realized through the emergency channel of the Bask TETRA network.

[12] The information has been provided by the end-users during meetings with the end-users or documents forwarded by the end-users to the project partners.
[13] Article 1(1) UEFA Safety and Security Regulations, Edition 2006, http://www.uefa.com/newsfiles/551778.pdf
[14] Article 4 UEFA Safety and Security Regulations, Edition 2006.
[15] Article 6 UEFA Safety and Security Regulations, Edition 2006.
[16] Article 10 UEFA Safety and Security Regulations, Edition 2006.
[17] Article 11 UEFA Safety and Security Regulations, Edition 2006.
[18] Articles 14-22 UEFA Safety and Security Regulations, Edition 2006.
[19] Article 33 UEFA Safety and Security Regulations, Edition 2006.
[20] Article 41 UEFA Safety and Security Regulations, Edition 2006.
[21] Article 38 -39 UEFA Safety and Security Regulations, Edition 2006.
[22] Article 36 UEFA Safety and Security Regulations, Edition 2006.

The stadium has a Control Room, through which operational coordination is provided and communication is organized (e.g. with private security, port guards and doctors in cases of injuries). There is a paper and electronic version of the map of the stadium, which is made available to the fire-fighters as well. The entities which meet in the Control Room are the Real Sociedad Manager; the Red Cross Operational Manager; a representative from the fire brigade and the police.

A decision might be taken to close the stadium before an event in certain circumstances (e.g. overcrowding; incorrect power supply certificate).

The organization of football matches, the evacuation plan and the operational responsibility during an event is the responsibility of the Real Sociedad Manager. The local police is responsible in the case of football games, while the private security director is responsible for security at concerts but the security plan must be communicated to the police in advance. While in cases of evacuation it is the concert organizer who is responsible, in practice the civil protection authorities will take lead. However, efforts are taken to prevent an emergency from occurring by taking people with fireworks outside the stadium.

Other actors involved in the management of events, including managing crowd incidents, are the security personnel from football clubs. The private security company is responsible for security checks at gates during football games and control of spectators across the stadium after the start of the games.

The uniformed and not uniformed Basque police prepare an action plan for each event and ensure coordination during the event with the other actors. The coordinator manages incidents and works with the mobile police. He may stop the game and order evacuation. In addition, he monitors the cameras in the control room. The coordinator of the Bask Mobile Police coordinator sits in control room and takes tactical decisions together with Basque police and may deploy force in emergency cases.

The Red Cross may provide medical assistance to injured spectators. The fire fighters intervene in cases of fire and the civil protection authorities should be present at the stadium by protocol. The games and shows manager is responsible for the planning and realization of technical support, for safety of the infrastructure. During matches he sits in the control room and is responsible for checking if gates are open/closed. During concerts he is responsible for issuing permits for concerts and parking licenses, for checking the safety of ramps and removing the mobile structures once people are inside.

3.3.2. Cruise ships

The situation is quite different in the context of ensuring safety of passengers on ships, where the responsible actors and safety requirements are different. It is ultimately the master who has discretion for the ship's safety and security. Thus, the master of the ship may not be constrained by the Company, the charterer or any other person from making or executing any decision which is necessary to maintain the safety of the ship or to even implement temporary security measures.[23]

To avoid disasters, each passenger ship must comply with all the safety and security requirements set out in the SOLAS convention.[24] Such requirements refer to, *inter alia*, the construction of the ship: the prevention and suppression of fire and means of escape;[25] the monitoring and maintenance of effectiveness of the fire safety measures of the ship;[26] the functioning of the ship security alert system;[27] the availability of survival craft and rescue boats and lifebuoys;[28] adequate life-saving appliances and arrangements (e.g. a sufficient number of lifejackets, including in the vicinity of the muster stations);[29] muster stations, which are in the vicinity of the embarkation stations and have ample room for the marshaling and instruction of passengers, at least 0.35 m^2 per passenger;[30] a decision-support system for emergency management on the navigation bridge as well as at least a printed emergency plans which include all foreseeable emergency situations;[31] having at least two separate and independent means, each using a different radio communications service, of transmitting ship-to-shore distress alerts.[32]

[23] Regulation 8 Master's discretion for ship safety and security, Chapter XI – 2 Special measures to enhance maritime security, SOLAS Convention.
[24] http://www.imo.org/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx
[25] Parts A, B, C, Chapter II – 2 Construction - Fire protection, fire detection, and fire extinction
[26] Regulation 14 Operational Readiness and maintenance, Part E Operational Requirements
[27] Regulation 6 Ship Security Alert System, Chapter XI – 2 Special measures to enhance maritime security, SOLAS Convention
[28] Regulation 21 Survival craft and rescue boats and Regulation 22 Personal life-saving appliances, Chapter III Life-saving appliances and arrangements, Section II Passenger Ships, Part B Requirements for ships and life-saving appliances
[29] Regulation 26 (5) (1) Lifejackets, Chapter III Life-saving appliances and arrangements, Section II Passenger Ships, Part B Requirements for ships and life-saving appliances
[30] Regulation 25 Muster stations, Chapter III Life-saving appliances and arrangements, Section II Passenger Ships
[31] Regulation 29 (2) and (3), Chapter III Life-saving appliances and arrangements, Section II Passenger Ships, Part B Requirements for ships and life-saving appliances
[32] Regulation 4, Chapter 4 Radio Communications, Part A General, annex to the International Convention for the Safety of Life at Sea, 1974, and the 1988 Protocol relating thereto

In addition, every passenger ship should have at least one person who is qualified for distress and safety radio communications to the satisfaction of the administration.[33] There should also be readily available life-saving signals, which are to be used when communicating with life-saving stations, maritime rescue units, as well as search and rescue aircraft.[34] For purposes of emergency communication on passenger ships there must be a general emergency alarm system and a public address system.[35]

To ensure safe escape, the following requirements shall be met: safe escape routes shall be provided; they shall be maintained in a safe condition, clear of obstacles; additional aids for escape shall be provided to ensure accessibility, clear marking, and adequate design for emergency situations. From all spaces there should be at least two widely separated and ready means of escape, one of which consists of a readily accessible enclosed stairway, which should provide continuous fire shelter. Corridors and lobbies with one means of escape only shall be prohibited. Stairways and ladders should be arranged so as to lead directly from passenger and crew accommodation spaces to the lifeboat and lifeboat embarkation spaces. Doors in general shall open in the direction of escape. Cabin and stateroom doors shall not require keys to unlock them from inside, while escape doors from public spaces, which are normally latched, shall have a means of quick release. The escape routes shall be marked by lighting or photo-luminescent strip indicators placed not more than 300 mm above the deck at all points of the escape route, including angles and intersections.[36]

In general, in cases of total evacuation of a passenger ship, all survival craft shall be capable of being launched within 30 minutes after the signal for abandonment has been given.[37]

Since 2010 cruise ships which sail in US waters are required to maintain a video surveillance system to document crimes on the vessel and provide evidence for the prosecution of these crimes and provide upon request copies of the recordings to law-enforcement authorities in the course of investigation of the crime.[38]

[33] Regulation 16, Chapter 4 Radio Communications, Part A General, annex to the International Convention for the Safety of Life at Sea, 1974, and the 1988 Protocol relating thereto
[34] Regulation 29, Chapter V, Safety of navigation, annex to the International Convention for the Safety of Life at Sea, 1974, and the 1988 Protocol relating thereto
[35] Regulation 12 Notification of crew and passengers, Part D Escape
[36] Regulation 13 Means of escape, Part D Escape
[37] Regulation 21, 1.4, Section II – Passenger Ships (Additional Requirements)
[38] Section 3 Cruise Vessel Security and Safety Act of 2010, which adds par. 3507 to Chapter 35 of title 46, United States Code

3.3.3. Metro Bilbao

In the metro scenario measures to manage crowds at metro stations (e.g. Bilbao metro), include, *inter alia*, the monitoring of all the 800 security cameras by a private security company officer. In addition, if it is predicted that the platforms will be overcrowded, the metro personnel may decide to close down the entrances to the metro. Another measure is the decision – making power given to the coordinator in the control room who may decide whether a train will skip an overcrowded station.

The metro disposes of a Control Room with four employees, one of who is a command control chief. The access to the control room is restricted. The Control Room disposes of a CCTV system. In addition, a GSCView tool is used to select video recordings from each metro station. The metro disposes of an Incident Control Management System for registration and management of accidents.

One person is responsible for the communication between control centre and outside world. The metro staff uses the TETRA standard, on a separate network from the one used by the police.[39]

The main threat comes from overcrowding and the main decision that could be taken is whether to open or close a certain gate. A station employee might decide when to open the ticket gates to evacuate faster. Security officers may split the platform crowd to direct the people to use the two platform exits.

3.3.4. Athens International Airport

Different crowd management policies are implemented at an airport, e.g. the Athens International Airport (AIA). Due to the business consequences of a total evacuation, the focus of the security staff is on prevention of emergencies. Crowd movements are measured through CCTV. In the control room, the police has the priority to monitor cameras and disposes of a database of suspicious persons.

There is a clear distinction between fire emergency and a security threat (e.g. a bomb threat). In the latter case it is the Airport Hellenic police that is responsible for handling the emergency. Within its powers it may undertake searches and/or order an evacuation. Before evacuation is ordered, the threat is communicated by the Airport Duty Officer to the Airport Hellenic Police and the Hellenic Civil Aviation Authority (HCAA). The latter is the Chair of the

[39] TETRA (Terrestrial Trunked Radio) is a professional mobile radio[2] and two-way transceiver (colloquially known as a walkie talkie) specification. TETRA was specifically designed by ETSI for use by government agencies, emergency services, (police forces, fire departments, ambulance) for public safety networks, rail transportation staff for train radios, transport services and the military

Threat Evaluation Committee and it may order evacuation together with the police. Then the Airport Duty Officer instructs the ASOC to alert the airport personnel to prepare for evacuation. The Police Chief determines the evacuation routes, checks their status and manages the evacuation operations.

In the case of fire threats, to prevent fire from occurring, there is an adequate smoke detection system and a sprinkler system. In case of a structural fire outbreak the Airport Services Operations Centre (ASOC) Senior Supervisor and Coordinators notify a set of 16 agencies - amongst which the Airport Duty Officer (ADO), the Airport Hellenic Fire Corps (AHFC), the Hellenic Fire Corps and the General Secretariat for Civil Protection - and becomes an On Scene Commander. AIAs Fire Marshall is responsible for the initial evacuation, following the evacuation plan, until the arrival of the AHFC.

In case of an emergency, the security doors, which function as emergency exit doors to avoid congestion, can be released by the ASOC SS via a button from the Central Control System. The AHFC may carry out search and rescue operations after the initial evacuation. The ASOC Deputy Senior Supervisor records the details of the accident in the daily logbook of the ASOC SS. The Airport Hellenic Police may dispatch staff and provide assistance such as regulating traffic and control the public. The communication between staff takes place via TETRA.

3.3.5. Technologies for crowd management

In the course of crowd management, the responsible staff makes use of different equipment when managing crowds, e.g. CCTV, communication systems (e.g. TETRA), electronic cards. Such technological means should meet the adequate technological and performance standards so that the responsible staff can efficiently and effectively carry out its duties. Thus, also the producers of such technologies bear a certain responsibility in the crowd management process.

The consequences of the breach of the responsibilities of the different actors involved in managing crowds would entail their liability.

3.4. Liability

Liability refers to the legal responsibility for someone's actions or omissions to act. Wrongful actions and omissions to act could lead to civil lawsuits whereby the wrongdoer has to compensate for the damages caused or to criminal prosecutions.[40] Responsibilities, *inter alia* responsibilities to ensure the safety of individuals present at a certain event, could stem from contractual obligations between the parties involved in the organization of the event, and/or from statutory (written laws passed by the legislature) and regulatory obligations (e.g. rules and requirements which are drafted as policies by governmental authorities to regulate certain activities such as sports events).[41]

3.4.1. Criminal Liability

Under criminal law, liability is incurred when two elements are present – *actus reus* and *mens rea*. Pursuant to the former, i.e. *actus reus*, the physical element of a crime needs to be committed. This can be triggered either when an act committed was prohibited (e.g. to violently attack members of the audience at a concert) or when an individual did not act when action was required by way of duty of care, for example when an obligation exists to rescue someone in danger. The act or failure to act must meet all the physical and material elements which constitute a crime under the law.

Pursuant to the *mens rea* element, the perpetrator must have had the intention to commit a crime, regardless of his motives. Nevertheless, *mens rea* is sometimes not required. Therefore, an actor could still be held liable if he did not have the intention to commit a prohibited act or not to act when under an obligation to do so.[42]

An example of the criminal liability is the unfortunate accident of the cruise ship Costa Concordia in 2012, which resulted in the death of 32 passengers. Currently, the master of the ship, Mr. Schettino, faces trial. It has been alleged that he has breached his duty of care and that he has not followed the principles of prudent seamanship established by customary international law.[43]

The Love Parade in Duisburg 2010, a dance festival, turned into a crowd disaster, whereby 21 people died of suffocation and numerous more were injured. City officials could

[40] J. R. Silvers, "Risk Management for Meetings and Events," *Events Management Series*, Elsevier 2008, p. 56
[41] *Ibid*, p. 59 and 62-63.
[42] J. Dumortier et al, "D.7.1 Legal Requirements for Trust in the IoT," uTRUSTit – Usable Trust in the Internet of Things, p. 49-50
[43] http://www.independent.co.uk/news/world/europe/costa-concordia-captain-set-to-stand-trial-alone-for-disaster-in-which-32-people-were-killed-8616288.html; http://www.bbc.co.uk/news/magazine-16611371

be prosecuted because they issued the permit for the parade without ensuring that the organizer had put in place and complied with the necessary safety requirements (e.g. measures to avoid congestion).[44] In addition, the communication between the police officers was not efficient and the leading police officer did not recognize the danger on time and did not take timely measures to react to it.[45]

3.4.2. Liability under Civil Law

Liability can also be incurred under civil law. Liability could stem from contractual obligations between parties when a party to the contract breaches the contractual provisions to which it is bound, e.g. a concert organizer concludes a contract with the town hall to host a concert at the town square and commits to ensuring safety of the attendees.

In the context of cruise ships, in the event of a shipping incident which causes "loss suffered as a result of the death of or personal injury to a passenger" the carrier shall be held liable for up to 250 000 units of account, unless the incident was caused by "act of war, hostilities, civil war, insurrection or a natural phenomenon of an exceptional, inevitable and irresistible character" or it "was wholly caused by an act or omission done with the intent to cause the incident by a third party."[46]

However, civil liability can also be triggered before a contract is actually concluded, i.e. in the negotiation stage. This is termed as *culpa in contrahendo*. It comes into play when one of the negotiating parties suffers damages in the negotiations phase due to a wrongful act of another negotiating party.[47]

Liability for unlawful damages can further be incurred outside the scope of a contract. Under civil law systems such as the French and the Belgian, this is called Aquilian liability. For Aquilian liability to be established, the following elements must be present: the actor(s) must have perpetrated a faulty act, damages must be sustained and the damages must be caused by the faulty act.

Under common law systems liability for unlawful damages outside the framework of a contract falls under the tort of negligence. For negligence to be established the following elements have to be satisfied: a duty of care must be established (e.g. a duty towards the

[44] Prof. Dr. T. Mayen and Dr. F. Hoelscher, "Zur Abgrenzung der Aufgaben von Veranstalter, Stadt Duisburg und Polizei bei der Loveparade 2010: Kurzgutachterliche Stellungnahme im Auftrag des Ministeriums fuer Inneres und Kommunales des Landes Nordrhein-Westfalen," Dolde Mayen & Partner, p. 31 -32; also http://www.welt.de/vermischtes/weltgeschehen/article13479369/Duisburger-Loveparade-Genehmigung-rechtswidrig.html

[45] http://www.wdr.de/tv/westpol/sendungsbeitraege/2013/0707/loveparade.jsp

[46] Article 3 (1) Athens Convnetion relating to the Carriage of Passengers and their Luggage by Sea, 1974 and the Protocol of 2002 to the Convention

[47] *Ibid,* p. 50

spectators at a stadium); the said duty of care must be breached which means the responsible person must have failed to fulfill standards which are expected to be met by a reasonable person (the standards are higher for professionals); damage must be established as a result of the breach of duty of care.[48] In the context of events management the duty of care refers to all the adequate measures taken to protect safety and health. The breach of the duty is normally examined in degrees of negligence. Thus, event organizers should be able to foresee the risks and their potential for harm, as well as take measures to mitigate them and warn the public of hazards.[49] In another example, carriers of passengers by sea (e.g. cruise ships) could be held liable in cases of negligent or faulty conduct of the carrier staff which causes death of or personal injury to a passenger the carrier and which was not caused by a shipping incident.[50]

However, also member of the crowds themselves could be held liable for negligent or provocative behavior. In principle citizens are under an obligation not to break public order. For instance, the UK Public Order Act of 1986 makes it a criminal offense of violent disorder if "*3 or more persons who are present together use or threaten unlawful violence and the conduct of them (taken together) is such as would cause a person of reasonable firmness present at the scene to fear for his personal safety.*"[51] The disorderly behavior of an individual in public is also criminalized.[52]

The breach of such provisions has sometimes led to fatal consequences like the tragedy at the stadium Heysel, Brussels in 1985 where 39 people died. The main responsibility for the tragedy was placed on the Liverpool fans and their hooliganism and ended in criminal convictions of involuntary manslaughter for 14 of the Liverpool fans.[53]

In addition, once an emergency situation has occurred, the members of the crowd could have certain rescue obligations towards other members of the crowd who have to be evacuated. Different obligations exist under the common law and the civil law systems.

Under the common law systems, such as in the UK, Australia and New Zealand, individuals do not have a legal duty to save/rescue other individuals in danger. This is also the case in the USA, with the exception of cases when there is a contractual relationship

[48] J. Dumortier et al*, "D.7.1 Legal Requirements for Trust in the IoT," uTRUSTit – Usable Trust in the Internet of Things*, p. 51
[49] J. R. Silvers, "Risk Management for Meetings and Events," Events Management Series, Elsevier 2008, p. 56-57
[50] Article 3 (2) of Athens Convention relating to the carriage of Passengers and their Luggage by Sea, 1974 and the Protocol of 2002 to the Convention
[51] Part I, Article 2 of the UK Public Order Act 1986
[52] Part I, Article 5 (1) of the UK Public Order Act 1986
[53] http://www.liverpoolecho.co.uk/news/liverpool-news/merseyside-police-officer-who-investigated-3424138

between the parties or a special relationship (e.g. parents – children).[54] However, if someone decides to rescue a person in danger on their own initiative, then they could be held liable if in their rescue efforts they cause greater harm.[55]

Under the civil law systems, such as the majority of European civil law systems, there exists the duty to rescue in the penal codes of states, such as Portugal, the Netherlands, Italy and France.[56] Further, under the Belgian and German Penal Codes individuals are under a duty to rescue persons exposed to serious danger as long as the rescue would not put the rescuing individual in serious danger. Non-compliance with this obligation could lead to both criminal and/or civil penalties. For example, pursuant to the jurisprudence of German courts tort liability does not ensue for failure to rescue but criminal liability could ensue. Thus, individuals might not claim damages from persons who did not help them when in great danger. By contrast, in France tort damages could be imposed for failure to rescue. Damages might also be claimed if the rescuer caused harm to the party he rescued unless the harmful measure he undertook was essential in saving someone's life. This is termed as the Status of Necessity.[57] In addition, again in France, the rescuer might claim damages from the party he rescued which he sustained in the course of the rescue.[58]

In the context of large crowd evacuations it is difficult to predict whether liability of ordinary individuals who did not rescue other evacuees will ensue as it seems likely that everyone will feel under threat for their own lives and try to escape. Thus, it might be difficult to establish whether indeed individuals could have saved other evacuees without a serious threats to their lives. In addition, those citizens who are accompanied by their children are likely to try to rescue them and ignore others around them.

[54] B. Crettez and R. Deloche, "On the optimality of a duty-to-rescue rule and the cost of wrongful intervention," *International Review of Law and Economics*, Vol. 31, Issue 4, December 2011, p. 263

[55] P. Cooke, DAN Legal Network National Coordinator for Britain in "The Good Samaritan Law across Europe," the DAN Legal Network, National Coordinators Committee.

[56] B. Crettez and R. Deloche, "On the optimality of a duty-to-rescue rule and the cost of wrongful intervention," International Review of Law and Economics, Vol. 31, Issue 4, December 2011, p. 263 - 264

[57] J. Hofstetter and W. v. Marschall, "Comments: Amendment of the Belgian Code Penal: The duty to rescue persons in serious danger," *11 American Journal of Comparative Law, 1962;* and Maitre F. Jaeck, Attorney at Law, DAN Legal Network Executive Director and National Coordinator for France

[58] Maitre F. Jaeck, Attorney at Law, DAN Legal Network Executive Director and National Coordinator for France

3.4.3. Product liability

Another type of liability is risk liability. Unlike the previous examples where an element of fault had to be established, in the case of risk liability, liability is established solely on the basis of risk. A notable example is product liability whereby a producer may be held liable for defective products even when his actions were not faulty.

The concept originated in the US, where a car manufacturer was held liable for the damages sustained by his products – negligent behavior of the manufacturer. Later, the concept evolved into the strict liability doctrine to mean that even if the producer was not negligent and thus did his behavior was not faulty, he could still be held responsible if someone sustains damages due to his products since he is responsible for bringing them onto the market.[59]

The doctrine of strict liability was introduced on a European level in 1977 through a 1977 Council of Europe Convention, which, however, was never ratified. Later on, in 1985, the European Union [then Community] adopted Council Directive 85/374/EEC on general rules on product liability without fault on the part of the producer who "should be liable for damage caused by a defect in his product."[60] The Council Directive was amended by Directive 1999/34/EEC.[61] Pursuant to the amending Directive a product is defined as "*all movables even if incorporated into another movable or into an immovable. "Product" includes 'electricity*.'"[62] Further, the definition of a producer encompasses not only producers of finished products, but also "the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer."[63] The Directive also sets up a regime of joint and severable liability.[64]

In order for product liability to be established, one needs to prove defect, damage and there must be a causal relationship between the product defect and the damage sustained as a result of its usage.[65] The definition of damage encompasses death or personal injuries; damage or destruction of property other than the defective product itself if it was intended for

[59] *Ibid*, p. 51-52
[60] Article 1 and Recital 2, Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, O. J. L 210, 07/08/1985 P. 0029 - 0033
[61] Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products
[62] Article 1 (1) Directive 1999/34/EC
[63] Article 3 (1) Directive 85/374/EEC
[64] Article 5 Directive 85/374/EEC
[65] Article 4 Directive 85/374/EEC

and used by the injured party for personal use and has lower value than 500 ECU.[66] A product is defective when it "does not provide the safety which a person is entitled to expect, taking all circumstances into account."[67] These circumstances include, *inter alia*, the presentation of the product,[68] the use to which the product would be reasonably expected to be put,[69] as well as the time of the launching of the product.[70] However, the Directive explicitly excludes the subsequent circulation of a better product as a criterion to determine defectiveness.[71] In addition, damage claims may be made only up to three years after the discovery of the defect and ten after the launch of the product.[72]

The Directive regulates the instances in which the producer will be exempted from liability.[73] One of the possible derogations refers to the level of scientific and technical development which did not allow a defect to be discovered.[74] However, the Directive allows the national legislation, when transposing the Directive, to derogate from that provision.[75] In cases of injuries and death Member States may limit the liability, but they may not limit it below 70 million ECU.[76] Still, in the context of personal injuries, the Directive explicitly states that liability may not be limited or excluded.[77]

If a product is developed within the framework of eVACUATE and subsequently marketed, the Directive on product liability would become applicable. However, since the Directive is transposed into national law by the national legislators, its provisions might differ. It has been studied that the Directive has been implemented and interpreted uniformly in the different Member States and therefore it can be considered as a general EU framework for product liability.[78] Still, certain provisions of the regime on product liability might differ depending on the different national implementations. Therefore, national laws must be considered by those involved in the production and marketing of the products.

[66] Article 9 Directive 85/374/EEC
[67] Article 6 (1) Directive 85/374/EEC
[68] Article 6 (1) (a) Directive 85/374/EEC
[69] Article 6 (1) (b) Directive 85/374/EEC
[70] Article 6 (1) (c) Directive 85/374/EEC
[71] Article 6 (2) Directive 85/374/EEC
[72] Article 10 and 11 Directive 85/374/EEC
[73] Article 7 Directive 85/374/EEC
[74] Article 7 (e) Directive 85/374/EEC
[75] Article 15 (1) (b) Directive 85/374/EEC
[76] Article 16 Directive 85/374/EEC
[77] Article 12 Directive 85/374/EEC
[78] J. Dumortier et al, "D.7.1 Legal Requirements for Trust in the IoT," uTRUSTit – Usable Trust in the Internet of Things, p. 54

3.4.4. Reducing liability and exemptions from liability

In principle to reduce liability, an entity needs insurance.[79] In the case of passenger ships insurance of at least 250 000 units of account per passenger on each distinct occasion is compulsory.[80] In addition, on EU level there exists a regulation pursuant to which there could exist national provisions which might limit the liability of the carrier or performing carrier.[81]

Thus, although under Article 7 (1) of the Athens Convention the liability of carriers in cases of death or personal injury of a passenger shall not exceed 400 000 units of account per passenger on each distinct occasion,[82] governments may limit this liability by specific national provisions on condition that the national limit on liability is not lower that 400 000 units of account per passenger on each distinct occasion.[83] Such limitations are regulated by the IMO Reservation and Guidelines for Implementation of the Athens Convention whereby a certain government should deposit a reservation or a declaration to the same effect.[84] Nevertheless, the carrier may not benefit from the limits to liability if the carrier intended to cause the damage or acted recklessly knowing that damage might ensue.[85]

Another means of limiting liability are disclaimers, which could be found, for example, on tickets. A disclaimer is a renunciation of a right and thus it might contain provisions limiting or excluding the liability of the organizer.[86] However, a disclaimer is not an absolute renunciation of responsibility. Sometimes it might not be enforceable if it was not legible on the back of the ticket or if the organizer was grossly negligent.[87]

---

79 http://www.crimeprevention.gov.au/Publications/PublicSafety/Pages/Planning_Safe_Public_Events_Practical_Guidelines.aspx

80 Article 4*bis* Compulsory Insurance, Athens Convention; the provision applies to passenger ships registered in a State Party which is licensed to carry more than 12 passengers and the Athens Convention applies.

81 Article 5 Regulation (EC) No 392/2009 of the European Parliament and of the Council of 23 April 2009 on the liability of carriers of passengers by sea in the event of accidents, O.J. L 131/24, 28.5.2009; it makes certain provisions of the Athens Convention relating to the Carriage of Passengers and their Luggage by Sea, 1974, as amended by the Protocol of 2002 (Athens Convention) and the IMO Reservation and Guidelines for Implementation of the Athens Convention adopted by the Legal Committee of the IMO on 19 October 2006 (IMO Guidelines) binding.

82 Article 7 (1) of Athens Convention

83 Article 7 (2) of Athens Convention

84 IMO Reservation and Guidelines for Implementation of the Athens Convention, adopted by the Legal Committee of the International Maritime Organization on 19 October 2006

85 Article 13 (1)

86 A. Cava and D. Wiesner, "Rationalizing a decade of Judicial responses to exculpatory clauses," 28 *Santa Clara Law Review 1988,* p. 646

87 J. E. Kastenburg, "A Three Dimensional Model of Stadium Owner Liability in Spectator Injury Cases," *Marquette Sports Law Review*, Volume 7, Issue 1 Fall, Article 5, 1996, p. 190; L. Ellis, "Notes:

Further limitations of liability could result also from the negligent or faulty behavior of members of the crowd. For example, carriers of passengers on a ship might be exonerated partially or wholly from liability for personal injury and death if the carrier establishes that the passenger caused or contributed to their own injury or death through their fault or neglect.[88]

3.4.5. Vulnerable Groups

In the course of managing large crowds special consideration should be given to vulnerable groups such as children and individuals with disabilities. Article 1 of Protocol No. 12 of the European Convention on Human Rights contains a general prohibition on discrimination in the enjoyment of the rights set forth by law.[89] Article 21 of the CFREU prohibits any discrimination on any grounds amongst which disability, age, sex, racial and ethnic origin.[90]

Another source of legislation on the rights of the disabled is the United Nations Convention on the Rights of Persons with Disabilities, which is the first legally-binding international human rights instrument to which the Union and its Member States are parties. Pursuant to the UN Convention, Parties are to protect and safeguard all human rights and fundamental freedoms of persons with disabilities. In principle, the rights of the disabled are also protected by way of respect for human dignity.[91]

One can identify different types of disabilities: mobility impairment; sensory impairment; cognitive or mental health impairment; hidden disabilities, whereby the disability is not physically visible but may be triggered by the emergency (e.g. asthma, heart problems); or a combination of any of the above-mentioned.[92] One of the problems with evacuating people with disabilities is the time they need to escape, which might slow down the response time. Another issue is the ability of people with impairment to receive information and potentially to interpret it and act upon it.[93] In some instances people might not be able to escape without the help of an assistant or caretaker. This might slow down the

Talking about my generation: Assumption of risk and the rights of injured concert fans in the twenty-first century," 80 *Texas Law Review* 607, 2001-2002, p. 617

[88] Article 6 of Athens Convention

[89] Article 1, Protocol No. 12 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 2000

[90] Article 21 Charter of Fundamental Rights of the European Union

[91] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "European Disability Strategy 2010 – 2020: A Renewed Commitment to a Barrier-Free Europe," COM (2010) 636 final, Brussels, 15.11.2010, p. 3 and Article 1 CFREU

[92] National Disability Authority (NDA), "Promoting Safe Egress and Evacuation for People with Disabilities," ISBN: 978-1-870499-18-7, p. 34

[93] *Ibid*, p. 35

escape time of the whole crowd if, for example, a person in a wheel chair is in front of the crowd. Additional problems arise if people with an impairment have to use lifts which in principle is not allowed in cases of emergency. Visual impairments might make it difficult or impossible for people to find their way to escape (e.g. not being able to follow the signs or the movements of the other people). People with hearing impairment might also have difficulty receiving information when it is transmitted orally. People with a cognitive impairment might receive all the information but be unable to process it or to process it on time.[94]

Therefore, when planning emergency response, one should consider the needs of the people with different disabilities and how their needs could be met in order to provide effective response.[95] Trained staff is essential for a successful evacuation of people with disabilities.[96]

More specific rules are contained in legislation such as EU Regulations on passengers when travelling by sea or air. With regards to maritime passengers, carriers are obliged to provide the disabled persons with, *inter alia*, assistance, where possible, adapted to the specific needs of the disabled person; the carriage of necessary equipment, including medical equipment; communication in an understandable form about the route; assistance with embarkation and disembarkation, etc.[97] Title III of the Americans with Disabilities Act (ADA), which prohibits discrimination on the basis of disability in areas of public accommodation and public transportation services, requires further measures to be taken even by foreign-flag carriers in American waters as long as the requirements do not interfere with the internal order of the cruise ship. Such measures could refer to, *inter alia*, placement of evacuation equipment in accessible areas or accessibility of cabins by persons who need to use mobility devices.[98]

Further safety measures with regards to persons with disabilities could be found in specific legislation such as the SOLAS convention which applies to passenger ships. Pursuant to its provisions, the master of the ship should have the "details of persons who have declared a need for special care or assistance in emergency situations" prior to the

[94] *Ibid*, p. 37-39
[95] *Ibid*, p. 40
[96] *Ibid*, p. 93
[97] Article 10 and Annex III, Regulation (EU) No 1177/2010 of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) NO 2006/2004, O.J. L 334/1; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:334:0001:0016:EN:PDF
[98] S. A. DiPolito, "Casenote: Title III of the Americans with Disabilities Act Applies to Foreign Cruise Ships; But qhat exactly is required?," *Mercer Law Review Spector, Vol. 57, 2006*, http://www2.law.mercer.edu/lawreview/getfile.cfm?file=57309.pdf

departure of the ship.[99] As concerns airports, passengers with reduced mobility (PRM) are to be provided with assistance by the air company.[100] Airports might have more specific provisions. For example, at AIA, the PRMCO personnel must be able at any time to provide reliable info to emergency services on the existence and location of PRM passengers and provide them with special assistance. In addition, medical staff should be notified if needed.[101]

Another vulnerable category is children. Article 24 of the CFREU in particular refers to the rights of the children, pursuant to which in all their actions public authorities and private institutions are under a positive obligation to take into primary consideration of children's best interests.[102] Therefore in crowd evacuation scenarios care and adequate assistance must be given to the needs of the children.

3.5. Conclusion

The preceding paragraphs elaborated on the legal and ethical issues which arise in the context of managing large crowd gatherings, in particular the duties, the interplay between all the parties (private and public) involved in crowd management in different scenarios, and the potential liabilities of these parties. The responsibilities for crowd management refer both to measures that have to be put in place with the purpose of preventing crowd disasters and measures which have to be implemented once a crowd disaster has occurred and evacuation is carried out.

Further, the section provided examples of the scope of duties and responsibilities of the different actors, which vary according to the specific situation or event, the rules by which the event could be regulated, as well as the nature of the crowd disaster when it occurs. The examples were taken from the crowd management procedures currently in place at the four use cases (cruise ship, AIA, ASRS, METB) to illustrate the different roles that authorities and entities could play (e.g. the police being in charge in cases of security threat at AIA or taking the lead in evacuations at ASRS, while on a cruise ship it is the captain of the ship that is in charge of all safety operations). In addition, the section paid attention to the needs of vulnerable groups who might require special protection in cases of emergency.

[99] Regulation 27 (2) Information on Passengers, Chapter II Life-saving appliances and arrangements, Section II Passenger Ships, Part B Requirements for ships and life-saving appliances

[100] Regulation (EC) No 1107/2006 of the European Parliament and of the Council of 5 July 2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air, O.J. L. 204, 26.7.2006, p. 1–9

[101] P. 6 and Annex A, Athens International Airport, Evacuation of MTB and/or STB due to security threat or event

[102] Article 24 Charter of Fundamental Rights of the European Union

The following section will examine the requirements and constraints that entities responsible for crowd safety have to take into consideration when implementing safety measures. Such requirements and constraints stem from the rights to privacy and data protection which have to be balanced against the requirements of safety.

4. Privacy and Data Protection

As discussed above, for the purposes of ensuring crowd safety the responsible authorities are obliged to take adequate measures. These measures could refer to the **prevention** of an incident from occurring (e.g. prevent overcrowding at metro stations or hooligan behavior at stadia via video monitoring) or to procedures to ensure that all present individuals are evacuated once **a crowd disaster has occurred (e.g. by tracking their location via their phones during rescue operations).**

For example, for search and rescue purposes all persons on board a cruise ship must be counted and the master of the ship must have the names and gender of all persons on board with a distinction between adults, children and infants.[103]

Such measures and procedures, while intended to save human life, could have privacy and data protection implications for the individuals in public places such as the use case scenarios (football spectators, metro and cruise ship passengers, as well as passengers and the general public at airports). While these measures could contribute to the safety of crowds, they involve tracking, monitoring and surveillance, as well as profiling the crowd or specific members of it. This is a realistic concern as crowd management involves a variety of sensors which collect and fuse personal data. This is in essence what the "Smart Spaces" to be developed in eVACUATE would do. This resembles Ambient Intelligence (AmI). AmI refers to:

> "*a complex technological environment, requiring little deliberate human intervention and encompassing a wide array of different emerging technologies, such as mobile sensors, radio frequency identification (RFID) tags, software agents, brain computer interfaces, ICT implants, affective computing and nanotechnology. […] The AmI will thus be characterized, on the one hand, by its invisibility, discretion and unobtrusiveness and, on the other, by its sensitivity, interactivity and responsiveness to the human person*."[104]

It might also lead in effect to increased tracking, monitoring and profiling.[105] One of the threats posed by the "Smart Spaces" is that they allow the integration and combination of information collected through all the different sources. The risk for the citizens is the

[103] Regulation 27 (1) and (3) Chapter II Life-saving appliances and arrangements, Section II Passenger Ships, Part B Requirements for ships and life-saving appliances

[104] N.N.G. de Andrade, «Right to Personal Identity: The challenges of Ambient Intelligence and the Need for a New legal conceptualization," p. 80 in S. Gutwirth, Y. Poullet, P. de Hert and R. Leenes (eds), "Computers, Privacy and Data Protection: An Element of Choice," Springer 2011.

[105] N.N.G. de Andrade, p. 82 - 83

discrepancy between the suggested pre-defined scenarios and the actual situation and facts.[106]

This necessitates the implementation of adequate privacy and data protection safeguards to strike the right balance between safety and privacy and data protection. Therefore, the implementation of such measures should respect the privacy and data protection requirements as laid down by legislation.

4.1. Introduction

The rights to privacy and data protection are two separate fundamental rights which are, however, complementary and interdependent. Their role is to guarantee the individual freedom to develop one's personality without undue interference and to control "some aspects of one's identity that one projects on the world."[107] In academic literature there has been an ongoing debate on which right is broader. Some consider privacy as a broader concept than data protection since it covers also non-personal elements which might have an impact on personal life.[108] Moreover, it extends further than private life, i.e. it covers different freedoms which protect one's privacy in public places.[109] Still, others suggest that data protection, having developed in response to the problems caused by technological progress, offers further protection to the individuals such as the right not be subject to automated decisions and thus extends beyond privacy.[110]

It is argued that the right to privacy refers to non-interference within the private life of individuals. Thus, it serves as an opacity tool which functions negatively and helps decision-makers determine which technologies should be prohibited. Data protection, on the other hand, serves as a transparency tool which regulates the lawful use of those technologies

[106] G. Buttarelli, "Legal Restrictions – Surveillance and Fundamental Rights," New technical Means of Surveillance and the Protection of Fundamental Rights – Challenges for the European Judiciaries, Vienna June 19th 2009, Justizpalast/Palace of Justice, p. 7

[107] A. Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence," Studies in Ethics, Law, and Technology, Berkeley Electronic Press, 2008. Available at SSRN: http://ssrn.com/abstract=1013984, Abstract

[108] D. Bigo, S. Carrera, B. Hayes, N. Hernandez and J. Jeandesboz, "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders. An evaluation of Current and Forthcoming Proposals," CEPS Papers in Liberty and Security, No 52/December 2012, p. 42

[109] M. Hildebrandt, "Profiling and the Identity of the European Citizen," in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives,* Springer 2008, p. 311

[110] P. de Hert et al, "Deliverable D 7.2: Biometrics in Europe: Inventory on Biometric Data and Privacy Legislation," *Biometric European Stakeholders Network,* November 2010; also F. Coudert, "Towards a new generation of CCTV networks: Erosion of data protection safeguards?, "*Computer Law and Security Review 25 (2009),* p. 148.

which have passed the privacy test.[111] Thus, when one examines the introduction of a privacy-intrusive technology, one should first study whether the technology should be introduced and under what conditions on the basis of the privacy test. Then, once its use has been "approved" the data protection provisions will serve as a tool to regulate the use of this technology with a view to minimising its impact on the fundamental rights of individuals.[112]

Therefore, those who process personal data have to comply both with the legal provisions enshrined in the data protection legislation and those that stem from privacy. These two rights will be examined in turn.

4.2. Privacy

The right to privacy is enshrined in Article 8 of the European Convention of Human Rights (ECHR), as well as in Article 7 of the Charter of Fundamental Rights of the European Union (CFREU). Conceptualizing privacy as a fundamental right has been a challenging task. Following up on the discussion above on the scope of the right to privacy, it is agreed that privacy encompasses numerous dimensions, including, *inter alia*, privacy of the individual or bodily privacy; of personal behaviour (e.g. political, religious and sexual activities or freedom from systematic monitoring); as well as of personal data and personal communication. With the advent of the new technologies the latter two have been referred to as information privacy.[113]

The scope of the right to privacy has further expanded in tandem with technological advances to include privacy of thoughts and feelings; privacy of location and space (i.e. freedom of movement in public and semi-public spaces without being identified, monitored and tracked through space); and privacy of association, which encompasses group privacy (e.g. groupings or profiles over which we have no control).[114] In addition, in a judgment on 15 December 1983 the Bundesverfassungsgericht (the German Constitutional Court) established the right to informational self-determination. This right has been interpreted to mean that "an individual's control over the data and information produced about him is a (necessary but insufficient) precondition for him to live an existence that may be said 'self-

[111] P. de Hert and S. Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power" in *E. Claes et al (eds), "Privacy and the criminal law, Intersentia, 2006, p. 61-104.*

[112] F. Coudert, "When video cameras watch and screen: Privacy implications of pattern recognition technologies," *Computer Law and Security Review 26 (2010), p. 377 – 384, p. 381.*

[113] R. Finn et al, "Chapter 1: Seven Types of Privacy," in S. Gutwirth et al (eds), "*European Data Protection: Coming of Age,"* Springer 2013, p. 4 -7

[114] R. Finn et al, p. 7 - 10

determined'."[115] It thus grants the individuals the power to take decisions concerning the collection, disclosure and use of their personal data.[116] This personal autonomy which is protected by the right to privacy does not equal isolation from society. Instead, it is the right of individuals as members of society.[117]

The right to privacy, however, is not absolute. Pursuant to Article 8 (2) ECHR and Article 7 CFREU in conjunction with Article 52 (1) CFREU, the right to privacy could be interfered with under certain circumstances. As concerns the definition of interference, it includes, *inter alia*, the mere collection and storage of data,[118] surveillance, interception of communications,[119] etc. In order for such an interference to be legitimate, it must comply with certain principles. The European Court of Human Rights has established the following test: the interference it must pursue **a legitimate aim**; it must be **in accordance with the law**; it must be **necessary in a democratic society**; and it must observe the proportionality principle (**proportionality *strictu sensu*,** i.e. the interference should not go beyond what is necessary to achieve the legitimate aim; it should bring more benefits than damage to privacy).[120]

The principle of **legitimate aim** will be examined in more detail in the section on data protection when the principle of purpose limitation is examined. Under Article 8 (2) ECHR amongst the legitimate aims one could point out to, *inter alia*, national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. Saving human life could be one such legitimate aim.

Therefore, those who manage crowds should establish a legitimate purpose when introducing (additional) sensors (e.g. CCTV cameras; RFID tickets; abnormal behaviour detectors) or other data processing activities (e.g. the interlinkage of databases containing personal data, etc). Preventing crowd disasters or reacting to them could constitute such a legitimate aim.

As concerns the "**in accordance with the law**" requirement, the Court has stated that the interference must be *based in law*, which must meet the *quality of the law standard*, i.e.

[115] A. Rouvroy and Y. Poullet, "Chapter 2: The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy," in S. Gutwirth et al (eds), *Reinventing Data Protection?,* Springer 2009, p. 51
[116] A. Rouvroy and Y. Poullet (2009), p. 56
[117] *Ibid*, p. 57
[118] *S. and Marper v UK*, ECtHR
[119] *Kruslin v France*, ECtHR
[120] *Kruslin v France*, ECtHR, 11801/85, 24 April 1990, Series A no.176-A; *Rotaru v Romania*, EctHR, 4 May 2000, application no. 28341/95.

be *accessible and foreseeable* to the persons concerned and the manner and scope and purpose of the data processing activities must be sufficiently precise.[121]

This requirement implies that the measures that are put in place to prevent crowd disasters or react to them must be based in law. Example of such laws are the national laws on CCTV images which regulate the installation of cameras and retention of and access to the images (e.g. Belgium, France).

In addition, the intervention must be strictly **necessary in a democratic society**. Pursuant to the interpretation of the European Court of Human Rights, a measure is necessary for a legitimate aim if it responds to a pressing social need, if it is proportionate to the aim and "if the reasons adduced by the national authorities to justify it are 'relevant and sufficient.'"[122]

Last but not least, the measures taken, which constitute interference, must be **proportionate**, i.e. the least intrusive. This means that the measures must bring sufficient benefits for the public interest to level out the interference with other values such as privacy. In principle, the more intrusive the interference into privacy is, the more significant and necessary the legitimate objective of the measure should be.[123] Thus, a new technology should be efficient and effective in meeting the declared aim.[124]

Before privacy-invasive measures are introduced (e.g. tracking through smartphone applications; RFID tickets, databases to fuse the data from the sensors) it must be examined whether they will indeed contribute to the effective management of crowds and whether they are the least intrusive ones. It must be noted that in the preventive stage the margin of appreciation of the actors is narrower than the one during the emergency stage. However, in both cases measures should not go beyond what is necessary to react to the disaster.

4.3. Data Protection

The legal framework on data protection legislation can be traced back to the Council of Europe Convention of 1981, which was adopted in reaction to the emerging technologies to regulate the automated processing of personal data. Later on, on an EU level, the EU legislator passed the following legal instruments: Directive 95/46/EC on Personal Data Protection, whose purpose is also to regulate the automated and semi-automated processing of personal data; Directive 2002/58/EC (e-Privacy Directive), which is a *lex specialis* to

[121] *Kruslin v France*, ECtHR, 11801/85, 24 April 1990, Series A no.176-A, par. 27 and 30
[122] *S. and Marper v UK*, ECtHR, par. 101
[123] F. Coudert (2009), p. 150
[124] P. de Hert and D. Wright (eds), "Privacy Impact Assessment," Springer 2012, p. 63

Directive 95/46/EC and regulates the processing of personal data on public communications networks, as well as Directive 2000/31/EC (e-Commerce Directive).

The right to data protection has also gained the status of a separate right and is enshrined in Article 8 of the CFREU and Article 16 TFEU. The cornerstone of EU data protection legislation has been Directive 95/46/EC, which will be examined in detail in this section. The Directive, as any other Directive, required transposition into national law. Therefore, in the EU there exist 28 different national data protection legislations. The Directive is currently under revision since the Commission proposed a General Data Protection Regulation in January 2012. If the new Regulation comes into force, it will become immediately applicable in all the Member States of the EU and thus bring about harmonization of the data protection provisions.[125] Relevant aspects of the proposed regulation will be examined.

Definitions/Concepts

When discussing protection of personal data, it must be defined what is covered by the definition of personal data. Pursuant to Directive 95/46/EC, personal data comprises "any information relating to an identified or identifiable natural person."[126] The purpose of the Directive is to serve as a protection of natural persons and therefore, the scope of the definition is interpreted broadly.[127] Thus, the definition refers to any data that could lead to the identification of the natural person/data subject, whether directly or indirectly.[128]

In the framework of processing personal data for the prevention and mitigation of crowd disasters personal data could include, *inter alia*, the processing of unique identifiers (e.g. on an RFID chip on a ticket or a card used by passengers on ships); the processing of video images, the processing of location data of persons through their smart phones, etc. With regards to personal data which is made available through the social networks (e.g. Twitter), it should be noted that the data processing operations would in principle fall under the Data Protection Directive.[129]

[125] 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
[126] Article 2 (a) Directive 95/46/EC
[127] Article 1 (1) and 2 (a) Directive 95/46/EC ; Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data," 20th June 2007, p. 4
[128] Article 2 (a) Directive 95/46/EC
[129] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking," 12 June 2009, p. 5

As concerns data rendered anonymous, by definition they do not fall under the Directive as long as "the data subject is no longer identifiable."[130] Thus, even depersonalized or darkened video surveillance images might be covered by the definition of personal data if the persons on them could be identified, for example, by their haircut or if measures could be taken to re-personalize the images.[131] Therefore, Directive 95/46/EC would be applicable if a person could be re-identified, e.g. the blurred images from video surveillance cameras.

In order for the Directive to apply, it is not necessary that the individual is identified directly. Sometimes it is enough that a certain natural person is singled out from the others and classified under a certain category or profile on the basis of his behavior, for example, without his identity being disclosed.[132]

For Directive 95/46/EC to apply, there must be a data processing activity. A processing operation refers to "any operation or set of operations which is performed upon personal data." It includes, *inter alia*, the mere collection, storage, alteration, disclosure, use, etc made of personal data.[133] Thus, the mere storage of personal data (e.g. names, cabin numbers) of passengers on ships on a database, the interlinking of personal data of individuals from different databases, the recording of video images, etc would fall under the definition of processing.

Pursuant to the Directive, every personal data processing activity must have a clearly designated controller or controllers. The controller is the entity (i.e. a natural or a legal person) which defines the means and purposes of the data processing activity.[134] The controller, before commencing a personal data processing activity, is obliged to notify the data processing operation to the data protection authority[135] and ensure that all the data protection principles are complied with.[136] A complex environment such as the one which involves multiple actors engaged in crowd management poses challenges in terms of the application of the law. The difficulty arises with regards to the allocation of legal responsibility since these might result from the combined actions of the different agents involved in the Smart Spaces, such as the different authorities (e.g. police, private security, in-house security).[137]

[130] Recital 26 Directive 95/46/EC
[131] Article 29 WP, Opinion 4/2007, p. 16 and 21
[132] Article 29 WP, Opinion 4/2007, p. 14
[133] Article 2 (b) Directive 95/46/EC
[134] Article 2 (d) Directive 95/46/EC
[135] Article 18 (1) Directive 95/46/EC
[136] Article 6 (2) Directive 95/46/EC
[137] Rouvroy, p. 18.

For eVACUATE this implies that both in the research phase (e.g. recording and further processing of video images during the validation demonstrations) and the operational phase of the eVACUATE product, each personal data processing operation or set of operations must have a clearly designated controller who will be responsible for the compliance of the processing activities with the data protection legislation.

Sometimes the controller could delegate the whole or part of the processing activity to another entity, i.e. the processor, who processes the data only on behalf of the controller.[138]

In some cases there could be also a third party which is authorized to process the data and is different from the data subject, the controller or the processor.[139] In addition, there could be a category called recipients of the data, which could be third parties or not and to whom data are disclosed. This category does not include authorities which receive the data in the course of a particular inquiry.[140]

Scope

There are certain personal data processing operations to which Directive 95/46/EC does not apply. This is when the data processing activity falls outside the scope of Union law, as well as in the context of public security, defense, State security, as well as the activities of the State in the field of criminal law.[141] In particular, when sound and image data (e.g. video surveillance) is processed for the above mentioned purposes, the Directive is not applicable.[142] For example, if a crowd disaster at an airport is caused by a terrorist attack, where it is likely that the law-enforcement authorities will take the lead, the Directive might not apply. However, even when the Directive does not apply, the national data protection laws might still apply.[143] For example, the Greek data protection law does not apply when sound and image data are processed by a public authority within their powers to protect, *inter alia*, persons and property. However, the material has to be destroyed within 7 days unless it is requested by judicial – public prosecution authorities. Non – compliance with this provision could lead to at least one year of imprisonment.[144] In other Member States, e.g. Germany, if a public authority wants to install CCTV cameras, the regional police law would apply, which

[138] Article 2 (e) Directive 95/46/EC
[139] Article 2 (f) Directive 95/46/EC
[140] Article 2 (g) Directive 95/46/EC
[141] Article 3 (2) Directive 95/46/EC
[142] Recital 16 Directive 95/46/EC
[143] Article 29 Working Party, Opinion 4/2007, p. 24
[144] Article 3 (2) (c) Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data

means that there are 16 different legal regimes.[145] France provides another example. If CCTV cameras are installed in public spaces, then their installation has to be approved by the local "préfet" after the recommendation by a departmental commission, headed by a magistrate. If the CCTV cameras are to be installed in places not open to the public, then a notification to the CNIL (the French Data Protection Authority) is necessary.[146]

In principle applicable data protection provisions on the processing of personal data in the police sector can be found in the Council of Europe Recommendation R (87) 15,[147] in the Council of Europe Convention 108/81[148] and in the proposed Directive 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, which contains similar principles to the ones contained in the current Directive 95/46/EC.[149]

Some clarifications as to the scope could be found in the proposal for a General Data Protection Regulation. Pursuant to the proposal, public security includes "the protection of human life, especially in response to natural or manmade disasters."[150] However, the proposal itself would not explicitly exclude from its material scope public security, but only activities which are outside the scope of Union law, such as national security; processing by Union institutions, offices, bodies and agencies; processing by Member States in the area of the common foreign and security policy; by natural persons without a gainful interest for personal and household activities; and by competent authorities in the sphere of criminal law.[151]

In both the Directive and the proposal for a regulation the legislator allows restrictions and exemptions to be made with regards to the principles of data processing, certain rights of the data subjects, as long as these are necessary and proportionate to safeguard, *inter alia*, national security, defence, public security, the prevention, investigation, detection and

[145] M. L. Gras, "The Legal Regulation of CCTV in Europe," Surveillance and Society 2004, CCTV Special 2 (2/3), p. 219

[146] http://www.cnil.fr/les-themes/videosurveillance/fiche-pratique/article/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de/

[147] 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

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

[149] Proposal for a Directive of the European Parliament and 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

[150] Recital 59 COM (2012) 11 final

[151] Article 2 (2) COM (2012) 11 final

prosecution of criminal offences, or breaches of ethics for regulated professions, an important economic or financial interest of a Member State or of the European Union, the protection of the data subject or of the rights and freedoms of others. Such restrictions, however, should have a legal basis.[152]

For example, in the case of a crowd disaster caused by a security threat such as a terrorist threat at an airport (AIA), the police would take the lead in carrying out the evacuation and would be allowed to conduct searches and request access to any information they might need. However, the right to privacy still applies and thus any derogation or restriction of the data protection principles should be still proportionate and should not go beyond what is necessary to mitigate the disaster.

Grounds for legitimacy

Any data processing activity must fulfill at least one of the criteria for making the processing legitimate. These are to be found in the exhaustive list in Article 7 Directive 95/46/EC, *inter alia* the unambiguous consent of the data subject (e.g. by downloading a smartphone application on a metro or cruise ship which will allow the tracking of individuals in emergency cases; consent of volunteers who participate in the validation demonstrations); or the processing is necessary for the performance of a contract to which the data subject (e.g. tracking the location of crew members of a cruise ship to ensure that there is sufficient number of personnel to evacuate passengers at specific locations of the ship); the processing is necessary for compliance with an obligation to which the controller is subject (e.g. the master of the ship should have details of persons who require special care or assistance); or processing is necessary in order to protect the vital interests of the data subject (e.g. tracking the smartphone of a passenger on a metro to rescue them after a terrorist attack); or the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed, etc.[153]

[152] Article 13 (1) (c) Directive 95/46/EC; Article 21 (1) (a) and Recital 59 COM (2012) 11 final

[153] Article 7: Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden

In the framework of eVACUATE under the different scenarios various data processing operations would take place and thus each one of them would fall under a different legal basis. For example, on a cruise ship the master is under an obligation by the SOLAS Convention to collect different categories of personal data of the passengers and crew members and have them available for the duration of the cruise tour, whereas processing of location data through smartphone applications which were downloaded voluntarily are likely to fall under consent of the data subject. If consent is the chosen legal ground, then it must be "freely given," "specific," i.e. given only for a concrete data processing activity, and "informed," i.e. the data subject should be informed of the categories of data to be processed, the purposes of the processing, his rights, etc.[154] In any case, any personal data processing operation in eVACUATE must fulfill at least one of the grounds for legitimacy.

If special categories of personal data (i.e. sensitive) are processed, then the legitimate ground is to be found in Article 8 Directive 95/46/EC. Currently, Article 8 covers the following categories of sensitive data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, as well as data concerning health and sex life.[155] As a general principle it is forbidden to process sensitive personal data unless one of the grounds in Article 8 (2) Directive 95/46/EC is met. These grounds are stricter than the ones under Article 7 Directive 95/46/EC.[156] For instance, if it is necessary for the different authorities to exchange information about a disabled person or a

by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

[154] Article 2 (h) Directive 95/46/EC

[155] Article 8 (1) Directive 95/46/EC

[156] 2. Paragraph 1 shall not apply where:
(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.
3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

pregnant woman in order to save his/her life (e.g. metro operators to police and fire brigade), then it could be possible that the processing of this information could fall under Article 8 (1) (c) Directive 95/46/EC to protect the vital interests (e.g. life) of the data subject where the data subject is physically or legally unable to give consent.

However, if personal data processing is carried out by the law-enforcement authorities in the area of criminal law, e.g. in the framework of a terrorist threat at a metro station, then national legislations on exchange of information in the police sector would apply. If the Proposed Directive for processing of personal data in the criminal law sector passes, then its provisions would apply. The principles of data processing in the Proposed Directive are similar to the ones in Directive 95/46/EC.[157]

Principles of Data Processing

When the legitimate ground(s) for the processing has been defined for every data processing activity, the processing operation(s) should comply with all the principles in Article 6 of Directive 95/46/EC. These principles will be now outlined.

Pursuant to the principle of *purpose limitation*, data may be collected only for "specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[158] Thus, the principle is composed of two elements - purpose specification and compatible use.[159] As concerns the first limb of purpose limitation, i.e. purpose specification, it is related to the principle of foreseeability under Article 8 (2) ECHR. Thus, the data processing operation must be "formulated with specific precision to enable the citizen to adjust his conduct accordingly."[160] Purpose specification is a pre-requisite for assessing the application of the other data quality requirements, such as the proportionality principle, accuracy, data minimization, retention periods, etc.[161]

The second limb, compatible use, defines the boundaries within which personal data collected for the specified purpose may be legally processed and when it may be further processed.[162] As a whole the principle of purpose limitation ensures the separation of data processing which pursues a specified pre-defined purpose from other data processing

[157] 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
[158] Article 6 (1) (b) Directive 95/46/EC
[159] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation," 2 April 2013, p. 3
[160] F. Coudert (2009), p. 149; Court of Justice of the European Union, C – 275/06, *Promusicae*, Opinion of the General Advocate J. Kokott, 18 July 2007, par. 53
[161] WP 29, Opinion 3/2013, p. 4
[162] *Ibid*

operations and prevents abusive interlinkages of data and databases, which could occur as a result of sharing of information between different authorities, for example.[163] This is related to the principle of separation of information (informationelles Trennungsprinzip), which applies in the case of exchange of data between authorities and pursuant to which data should not be transferred for new, incompatible purposes to other authorities.[164]

Therefore, every personal data processing operation must have a clearly defined purpose and all the usages of the personal data must be compatible with the original purpose. For example, in cases of rescue operations the location data of passengers could be exchanged between authorities in order for the authorities to provide the adequate assistance. By contrast, video surveillance footage which is recorded from metro stations, may not be further disclosed to the media.

Furthermore, the data processing activities must process only the minimum data necessary for achieving the legitimate purpose(s), i.e. fulfill the principle of *data minimization*. Pursuant to that principle, the controller may only process personal data that are "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*."[165] This implies that the controller may collect and process only these categories of data that are necessary and relevant to achieve the legitimate purpose(s). Therefore, the controller(s) in each scenario must assess and justify the necessity and relevance of all categories of personal data in advance of the processing.

Moreover, the principle of *data accuracy* must be complied with. Pursuant to it, personal data must be accurate and where necessary kept up to date.[166] An example of that is the accuracy of data stored on all the passengers on a cruise ship.

Next, is the issue of *data storage*. Personal data must be de-personalized, i.e. not to allow the identification of the data subject, as soon as they are no longer necessary for the specified purposes. Personal data could be stored longer for historical, statistical and scientific use when adequate safeguards are put in place.[167] Thus, different storage periods would apply to the different scenarios in the different countries. For example, retention periods of CCTV images are often regulated by national law and thus these rules have to be complied with by the controller.

[163] F. Coudert (2009), p. 149
[164] Bundesverfassungsgericht judgment, 1 BvG 1215/07, 24.04.2013
[165] Article 6 (1) (c) Directive 95/46/EC
[166] Article 6 (1) (d) Directive 95/46/EC
[167] Article 6 (1) (e) Directive 95/46/EC

Last but not least, any data processing activity must be *fair and lawful*,[168] i.e. fair and lawful in relation to the legitimate purpose, fulfilling all the above-mentioned principles. It has been subject to criticism that this provision in the Directive does not provide guidance as to the substantive/normative questions regarding when a processing fair and lawful.[169] Thus, one could argue that the Article 8 ECHR and the jurisprudence of the ECtHR and the CJEU are better equipped to give substance to the notions of fair and lawful.

Rights of the data subject

When personal data are processed, the controller must respect the following rights of the data subjects: the right of information,[170] whereby the controller or his representative shall inform the data subject at least of the identity of the controller and if necessary of the processor, the purpose of the processing, as well as the rights of the data subjects; the right of the data subject to access data concerning him/her; the right of access covers also the right to rectification, erasure or blocking of data whose processing does not comply with the Directive;[171] the right to object to the processing of data relating to him/her;[172] and the right to judicial remedy in cases of breach.[173] Therefore, each controller involved in the processing of personal data in eVACUATE (e.g. partners who process personal data in the framework of the validation demonstrations; controllers of video surveillance images; the master of the cruise ship) must guarantee the rights of the data subjects.

Automated Decisions and Profiling

Pursuant to Article 15 (1) of Directive 95/46/EC individuals have the right "*not be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as […], conduct, etc.*."[174] Member States shall allow a person to be subjected to such a decision if the decision is authorized by law and provides adequate safeguards.[175]

According to the Proposal for a General Data Protection Regulation this provision would extend to the analysis or prediction of a person's behavior. The name of the Article is

[168] Article 6 (1) (a) Directive 95/46/EC
[169] P. de Hert et al, "Deliverable D 7.2: Biometrics in Europe: Inventory on Biometric Data and Privacy Legislation," Biometric European Stakeholders Network, November 2010
[170] Article 10 and 11 Directive 95/46/EC
[171] Article 12 Directive 95/46/EC
[172] Article 14 Directive 95/46/EC
[173] Article 22 Directive 95/46/EC
[174] Article 15 (1) Directive 95/46/EC
[175] Article 15 (2) (b) Directive 95/46/EC

changed to profiling.[176] Again, there are exceptions to the general prohibition. Thus a person may be subjected to profiling measures if profiling is "expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests"[177] or if it is based on the consent of the data subject, the conditions for which are defined in Article 7 of the proposal, as well as on the implementation of adequate safeguards.[178] However, the processing under Article 20 may not be based solely on special categories of data.[179] In any case, if profiling takes place, the data subject should be informed of its existence and its envisaged effects.[180]

Currently at all the four scenarios there are video surveillance technologies, monitored by designated officers. However, it is argued that for purposes of preventing crowd disasters applications could be developed and installed which can detect abnormal behavior. If the detection of abnormal behavior of a crowd as a whole or within a crowd is the result of an automated process, it would imply that the detection is based on *"complex probabilistic calculations*"[181] and not on human judgment. The result is that individuals might be singled out from a crowd and subjected to more intense profiling. This could pose threats to an individual's autonomy since he would be judged on the basis of group characteristics which produces information obtained through statistical analysis.[182]

Profiling would thus be based on the traits of the behavior of the members of the crowd. Such type of personal identification is defined as "new biometric traits," such as behavioral or soft biometrics (e.g. gait analysis). Behavioral biometrics represents technologies which "'measure' human characteristics related to a person's conscious or unconscious behavior, actions or skills – and not his/her physical features."[183] Amongst the numerous problems that they raise some have identified the covertness of this profiling activity, as well as the nature and amount of information which they could reveal about the profiled individuals:

> "*the most critical implications of next-generation biometrics are that future biometric recognition could take place remotely, covertly and/or from a distance*

[176] Article 20 (1) Measures based on profiling, COM (2012) 11 final
[177] Article 20 (2) (b) COM (2012) 11 final
[178] Article 20 (2) (c) COM (2012) 11 final
[179] Article 20 (3) COM (2012) 11 final
[180] Article 20 (4) COM (2012) 11 final
[181] F. Coudert, "When video cameras watch and screen: Privacy implications of pattern recognition technologies," *Computer Law and Security Review 26 (2010),* p. 377
[182] *Ibid*, p. 379
[183] A. Yannopoulos et al "Behavioral Biometric Profiling and Ambient Intelligence," in M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspective,* Springer 2008, p. 90

and may produce material with a high degree of sensitive (and surplus) information."[184]

This richness of the extracted information or features allows one to engage in pattern recognition activities.[185] There is a danger not necessarily that the individual is identified, but that they are categorized and decisions are made about them based on the profile they present.[186]

Sometimes the criteria for defining abnormal behavior might be *per se* discriminatory.[187] This becomes even more evident if one considers that pattern recognition technologies are normally data driven. They are based on a pre-collected dataset that is pre-designed to recognize certain patterns and to identify the new data that fit the pattern. Such technologies are thus designed to generalize.[188]

Such an abnormal behavior detection capacity modifies the role of video surveillance which changes from a reactive to a proactive technology and serves new purposes, i.e. to detect risk factors before an event has actually occurred.[189] The WP 29 Working Party refers to it as a "*dynamic-preventive surveillance*."[190] However, the installment of such advanced computer vision technologies might not be sufficient to ensure the safety purposes for which the technology was installed since eventually the determining factor is the ability of those behind the cameras to analyze the events and their capacity not to put too much weight and trust in the technology when taking a decision, thus assuming it is infallible and effectively running away from their own responsibilities as decision-makers.[191]

In addition, the tracking and monitoring individuals who display abnormal behavior also raises concerns with regards to the freedom of movement of individuals in the sense that individuals enjoy the freedom "without having inevitably to leave continued and/or frequent traces of one's movement for the benefit of permanent 'optic informers.'"[192] This problem becomes even more pertinent if alerts are stored and interlinked with each other, in

[184] R. Finn, D. Wright and M. Friedewald, "Seven Types of Privacy," p. 22 in S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet (eds), "European Data Protection: Coming of Age," Springer 2013 (refer to S. Venier and E. Mordini, "Second - generation biometrics," in Privacy, data protection and ethical issues in new and emerging technologies: Five case studies, eds. Rachel Finn and David Wright (PRESCIENT consortium, 25 November 2011).
[185] A. Yannopoulos, p. 89
[186] Finn, "Seven Types of Privacy," p. 24
[187] G. Buttarelli, p. 9
[188] A. Yannopoulos, p. 102
[189] Coudert 2010, p. 377
[190] WP 29 (2004), p. 4
[191] F. Coudert 2010, p. 377 and 379
[192] G. Buttarelli, p. 9; also WP 29 (2004), p. 6 and Article 2 Additional Protocol No 4 European Convention on Human Rights

particular if they concern the same individual who is present on the premises under surveillance regularly.

Confidentiality and Security of processing

Pursuant to the principle of data confidentiality, any person acting under the authority of the controller or the processor with access to personal data may process the data only on instructions from the controller, unless required to do otherwise by law.[193] Another essential aspect of any data processing activity is its compliance with the principle of data security. Thus, the system(s) which process personal data must implement adequate technical and organizational measures to ensure against any accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. These measures are applicable both to the controller and the processor if there is one.[194] Thus, all elements (e.g. emergency response centre) must ensure the technological robustness of the system and protect all its components against attacks. This is termed as integrity of the system by the German Constitutional Court in a landmark ruling.[195]

Examples of measures of confidentiality and security are the restricted access to the control rooms at the different end-user scenarios (e.g. metro Bilbao, AIA) and the security of the networks and equipment over which personal data are processed. If eVACUATE introduces additional equipment and/or software applications, they too have to enjoy an adequate level of security.

Liability

It has already been discussed that for each personal data processing activity there must be a designated controller and sometimes processor(s) with clearly pre-defined responsibilities under the Directive.

In general, it is the controller who has to ensure that the data processing activity complies with the principles regarding the processing of personal data.[196] Further, the controller has to ensure that the data subjects can exercise their rights,[197] that the principles of confidentiality and security of processing are complied with,[198] as well as that the supervisory authority is notified of the data processing activity.[199] The designation of responsibilities is essential since pursuant to Directive 95/46/EC in the case of breach of the

[193] Article 16 Directive 95/46/EC and Article 27 COM (2012) 11 final
[194] Article 17 Directive 95/46/EC
[195] Judgment of the German Constitutional Court, BvG 370/07
[196] Article 6 (2) Directive 95/46/EC
[197] Article 10, 11, 12 and 14 Directive 95/46/EC
[198] Article 16 and 17 Directive 95/46/EC
[199] Article 18 Directive 95/46/EC

responsibilities of the controller(s) and where applicable the processor(s) these can be held liable severally or jointly.[200]

Pursuant to the Directive if an individual "has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to that Directive" may claim damages from the controller.[201] In case where the controller is not responsible for the event which caused the damage, the controller or processor may be exempted from liability in whole or in part.[202]

Further, the Directive makes provisions for the administrative remedies, *inter alia* before national data protection supervisory authorities. In addition, every person in entitled to a judicial remedy for "any breach of the rights guaranteed him by the national law applicable to the processing in question."[203] In cases of infringement, the Member States may impose sanction in order to ensure the full implementation of the Directive.[204] Pursuant to the Proposal for a General Data Protection Regulation, the supervisory authority would be entitled to impose fines for personal data processing breaches.[205]

4.4. Review of the EU Data Protection Framework

As already mentioned above, in January 2012 the European Commission proposed a new legislative package to reform the existing data protection framework in the EU. The new legislation will be a Regulation and not a Directive as currently in force. The difference between the two instruments is that a Directive needs further implementation into national law, whereas a Regulation does not. Therefore, currently in the EU there are 27 different legislations on data protection and some differences exist. A regulation would bring about harmonization of all those national laws and there would be one data protection law in all the Member States of the EU.[206] The novelties which the regulation seeks to introduce are numerous and therefore the section will not provide an exhaustive overview of its provisions. Therefore, only some of them will be discussed below.

The Proposal for a General Data Protection Regulation would introduce and formalize, *inter alia*, two new principles, namely Privacy by Design and Accountability, which

[200] Article 23 Directive 95/46/EC ; Article 77 (1) and (2) COM (2012) 11 final
[201] Article 23 (1) Directive 95/46/EC ; Article 77 of COM (2012) 11 final refers not only to the controller as a liable party but explicitly mentions also the processor. It also introduces the possibility for controllers and processors to be held jointly and severally liable when there are more than one controllers or processors.
[202] Article 23 (2) Directive 95/46/EC; Article 77 (3) COM (2012) 11 final
[203] Article 22 Directive 95/46/EC
[204] Article 24 Directive 95/46/EC
[205] Article 79 COM (2012) 11 final
[206] The European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the data protection reform package," 7 March 2012, p. 14, pt.86

will be discussed in the following two sections. It would also introduce the obligation to conduct Privacy Impact Assessments.

4.4.1. Accountability

Accountability has developed as one of the general principles in a number of data protection frameworks,[207] in particular in the legal framework of the European Union (EU). Following the most recent legislative developments in the EU, accountability of the controller(s) has been introduced as a separate principle in Article 22 of the Proposed Regulation.[208]

The added value of accountability as a separate principle is that it ensures that the data protection substantive norms and obligations are translated into measures and practices, thus moving data protection "from theory to practice."[209] Thus, ideally, the controller would minimize the risks associated with personal data processing and have a better reputation.[210]

Accountability is constructed as a two-tiered principle. On one hand, it serves as a tool which ensures that the controller respects the substantive provisions of data protection in the course of each and every data processing operation and that data subjects can exercise effectively their rights. To that end, it requires data controllers to put in place mechanisms, procedures as well as binding and enforceable policies, which will guarantee the compliance with the norms and provisions prescribed in the data protection framework. On the other hand, pursuant to the principle of accountability, the controllers are under an obligation to demonstrate the above-mentioned compliance upon request by the relevant data protection authorities.[211]

In practical terms, controllers should put in place internal mechanisms and implement practical tools for more effective data protection *from the outset*. The mechanisms should be in place throughout the whole processing activity, thus implying that accountability should be "an ongoing activity."[212] Article 22 (2) of the Proposed Regulation proposes a non-exhaustive list of the possible measures to ensure compliance with the data protection laws. These

[207] J. Alhadeff et al, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," SSNR, September 26, 2011, http://ssrn.com/abstract=1933731, p. 1;
[208] Article 22, COM (2012) 11 final
[209] Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010, executive summary;
[210] *Ibid*, p. 5
[211] J. Alhadeff et al, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," SSNR, September 26, 2011, http://ssrn.com/abstract=1933731; Article 29 Working Party, Opinion 3/2010, executive summary; P. Hustinx, "Accountability in the Proposed Regulation," Brussels, 3 December 2012
[212] P. Hustinx, "Accountability in the Proposed Regulation," Brussels, 3 December 2012

include keeping documentation of the processing operations, implementing the data security requirements, carrying out a Privacy Impact Assessment, where necessary complying with the requirements for prior authorization or consultation, as well as appointing a data protection officer. Some further elements of accountability have been put forward – executive oversight, education and awareness amongst the staff who process data, ongoing risk assessment and mitigation, event management and complaint handling, internal enforcement, sanctions and redress.[213]

According to the second tier of the principle, accountability would require data controllers to have the necessary internal mechanisms in place *to proactively demonstrate* compliance to external stakeholders upon request.[214] The capacity to demonstrate compliance would enhance the transparency of the practices of the data processing entities. This would increase trust in the entity processing personal data and facilitate the oversight of the supervisory authorities and facilitate their enforcement actions and help them prioritize their focus.[215]

Pursuant to the Article 29 Working Party opinion, the formal legal requirements of accountability represent only a minimum requirement and the controller may decide to implement stricter measures which will serve the purpose of adequate data protection-conform processing activities.[216] In addition, if a controller has ensured compliance with the accountability principle, this fact does not constitute a legal presumption of compliance with the substantive norms in the data protection legal framework.[217] Last but not least, the principle of accountability should be applicable to both public and private controllers and should be scalable.[218]

[213] J. Alhadeff et al, p. 4 and 15; Article 22 (2) COM (2012) 11 final
[214] Article 29 Data Protection Working Party, Working Party on Police and Justice, "The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data," Adopted on 1 December 2009, p. 20
[215] Article 29 Working Party, Opinion 3/2010, p. 7 and 16, J. Alhadeff, p. 22
[216] Article 29 Working Party, Opinion 3/2010, p. 6
[217] Article 29 Working Party, Opinion 3/2010, p. 11
[218] Article 29 Working Party, Opinion 3/2010, P. 19

4.4.2. Privacy By Design

The proposed Regulation has formally incorporated in the European Union data protection framework the principle of privacy by design.[219] Pursuant to that principle, technological data protection and privacy safeguards should be embedded into the design and operation of information and communication technologies (ICT).[220] In addition, privacy by design requires that data processing systems are designed to process a minimum amount of data; that the data are not retained for longer than necessary and that they are made accessible only to a defined number of individuals.[221] According to the wording of Article 23 of the Proposed Regulation, the implementation of privacy by design in technologies will become mandatory.[222]

The concept of privacy by design was developed in answer to the faster development of the ICTs in comparison to regulatory developments. Thus compliance with data protection legal frameworks proved not to be enough. Pursuant to privacy by design, privacy settings need to be implemented into the system on a technical level and become the organizations' default setting, i.e. privacy by default.[223] The latter refers to privacy features which are activated automatically.[224] The responsibility for protection personal data, in addition to the role of the controller, thus applies also to producers of technology[225] and to the processors of personal data.[226]

The scope of the principle of Privacy by Design should ideally extend to the following fields: information technology, business practices and physical spaces. Thus, it is essential that information technology is used to protect personal data, for example through Privacy Enhancing Technologies (PETs), and not to pose risks to this data. In addition, it entails the accountability of entities processing personal data which grants them competitiveness. As

[219] Article 23, COM (2012) 11 final
[220] Article 29 Data Protection Working Party, Working Party on Police and Justice, "The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data," Adopted on 1 December 2009, P. 13;
[221] EDPS Comments on DG CONNECT'S Public Consultation on Improving Network and Information Security (NIS) in the EU, 10 October 2012,p. 5; Article 23 COM (2012) 11 final
[222] Article 23 COM (2012) 11 final
[223] Cavoukian A., Chibba M., Stoianov A, "Advances in Biometric Encryption: Taking Privacy By Design from Academic Research to Deployment," Review of Policy Research, Vol. 29, Number 1, (2012); p. 41
[224] Kuner, C, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," Privacy & Security Law Report, 11 PVLR 06, 02/06/2012, Bloomberg, BNA, p. 7
[225] Kuner, C, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," Privacy & Security Law Report, 11 PVLR 06, 02/06/2012, Bloomberg, BNA, p. 7; Article 29 Working Party, p. 3
[226] EDPS Opinion, 7 March 2012, p. 29, where the EDPS calls on the Commission to explicitly add the role of processors.

concerns physical design, the physical infrastructure where data are stored and processed must be secure. [227]

In substance, privacy by design comprises seven elements, which have been proposed by Dr. Cavoukian and endorsed in the 2010 Privacy by Design Resolution. Privacy by Design ensures a proactive approach to data protection to prevent abuse of personal data; it is automatic and should not depend on an action by data subjects; it is integrated into the systems; it ensures both security of the systems and their data protection compliance; it guarantees data protection throughout the whole lifecycle of the operation of the data processing system; it ensures transparency and empowers the users.[228] The Article 29 WP refers also the principles of data confidentiality, data quality and use limitation.[229]

For the systems or ICTs to successfully implement privacy by design, they should put in place Privacy Enhancing Technologies (PETs) and Best Available Techniques (BATs).[230] PETs refer to technologies which minimize personal data use, maximize data security and empower individual users.[231] The importance of security has been confirmed by the German Constitutional Court, which established the principle of confidentiality and integrity of information technology systems, since abuse of the rights of data subjects may occur as a result of the exploitation of the weaknesses of a system. Thus, the technical robustness of the system is essential as the complexity of ICTs have made it impossible for individual data subjects alone to ensure the protection of their personal data.[232] With regards to BATs, the EDPS recommends that entities use the most updated technology which implements the highest degree of data protection settings.[233]

Thus, the eVACUATE partners should embed into the product(s)/system functionalities that respect and facilitate the implementation of the privacy requirements. For example, they could develop functionalities for automated deletion of video surveillance images; ensure RFID tags/cards/tickets are not active outside the concerned premises; smartphone apps do not collect more that location data, etc.

[227] http://privacybydesign.ca/about/trilogy/
[228] http://www.ipc.on.ca/site_documents/pbd-resolution.pdf; http://privacybydesign.ca/about/principles/
[229] Article 29 Working Party, p. 14/15
[230] EDPS Comments, 10 October 2012
[231] Cavoukian A., "Privacy By Design," http://www.ipc.on.ca/images/Resources/privacybydesign.pdf, p. 3; Also, in its Judgement 1BvG 370/07, the German Constitutional Court established the principle of confidentiality and integrity of IT systems, p. 3
[232] 1BvG 370/07, also par. 180.
[233] EDPS Comments, 10 October 2012

4.4.3. Data Protection Impact Assessment

Pursuant to Article 33 of the proposed regulation the controller or the processor shall carry out a data protection impact assessment when the processing operations "present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes."[234] The legislator has provided some examples of such operations, *inter alia* video surveillance and automated processing which could predict individuals' behavior and could affect or produce legal effects against individuals.[235] In principle the impact assessment should contain a description of the processing operation (s), evaluation of the risks as well as the measures and safeguards to mitigate them. The process should involve the data subjects or their representatives.[236]

4.4.3.1. RFID Privacy and Data Protection Impact Assessment

Even though the Proposed Regulation has not passed, pursuant to a Commission recommendation the industry developed a framework for privacy and data protection impact assessment for RFID tags, which was endorsed by the Article 29 Working Party.[237]

The purpose of conducting a privacy and data protection impact assessment for RFID tags is to carry out an assessment of the implications of the RFID applications with regards to privacy and data protection, implement adequate safeguards, to have this assessment reviewed and to make the assessment available to the respective authority at least 6 weeks before the deployment if the RFID application.[238]

In general the overall goal of conducting a PDPIA is to "establish and maintain compliance with privacy and data protection laws and regulations" and manage the risks associated with the deployment of RFID applications to both the operator and the users.[239] The PDPIA seeks to promote the principle of privacy by design in RFID applications, to make RFID applications transparent, provide better information to individuals and to serve as a

[234] Article 33 (1) COM (2012) 11 final
[235] Article 33 (2) (a) to (e) COM (2012) 11 final
[236] Article 33 (3) and (4) COM (2012) 11 final
[237] Point 4, 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
[238] Point 5, Commission Recommendation C (2009) 320 (2009/387/EC)
[239] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, p. 3

basis for dialogue with the competent authorities.[240] One of the essential components of the PDPIA is to identify and assess the risks that a certain RFID application could cause.[241] **Thus, the PDPIA is based on a "privacy and data protection *risk management* approach**."[242]

In addition, the use of RFID applications should be transparent and thus RFID operators need to provide data subjects with easy to understand information on the use of the applications. This information policy should include at least information on the identity and address of the employer, the purpose of the application, the categories of personal data to be processed and whether the location of tags is to be monitored, a summary of the privacy and data protection impact assessment, as well as the likely privacy risks and the measures that individuals can take to mitigate them.[243]

The PDPIA is characterized as a *process*, which should ideally begin at the earliest possible stage so that the outcome of the application could be influenced.[244] Pursuant to the framework developed for PDPIA by the industry and endorsed by Article 29 Working Party, the process should have two phases. During the initial phase, the operator/controller conducting the PDPIA should determine whether a PDPIA is required for his RFID application or not and in case a PDPIA is required, whether it should be a Full or Small scale PDPIA. During the second phase, the criteria and elements of Full-scale and Small-scale PDPIA are outlined.[245]

A PDPIA for a certain RFID application can be conducted after the operator/controller has defined the RFID application and specified the categories and sensitivity of the data as well as the personal data processing activity.[246] At this stage the RFID application for eVACUATE has not been fully developed. According to the initial description provided so far, it is envisaged that the RFID tags will be passive and they will be printed on tickets and their target range will be approximately 1m. There would be potentially 7 categories of information in the RFID – whether the ticket is for individuals with a disability, pregnant women, etc. The

[240] Article 29 Data Protection Working Party, "Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications," 11 February 2011, p. 7
[241] Article 29 Data Protection Working Party, "Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications," 11 February 2011, p. 5
[242] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, p. 3, emphasis added.
[243] Point 7 and Recital 23, Commission Recommendation C (2009) 320 (2009/387/EC)
[244] PDPIA Framework, p. 6; P. de Hert and D. Wright (eds), "Privacy Impact Assessment," Springer 2012, p. 5
[245] Article 29 WP, p. 7; the Framework, p. 6
[246] PDPIA Framework, p. 6

frequency of the tag is yet to be defined. In addition, it is not clear yet who the controller of those RFID tags would be and who would have access to the information, whether there will be a database, whether any other personal information (e.g. unique number) would be processed, whether the RFID tags would be active outside the premises of the envisaged application, etc. Therefore, a PDPIA for the RFID application in eVACUATE cannot be completed yet. Instead, the elements of a PDPIA process will be outlined and later applied to the eVACUATE RFID application.

Elements of a PDPIA for RFID

As mentioned above, the PDPIA consists of two phases – an **initial phase** and a **risk assessment phase**.

During the **initial analysis phase** one should answer the questions in the decision tree below in order to determine whether a PDPIA is necessary and whether it should be a full-scale or a small-scale one.[247]

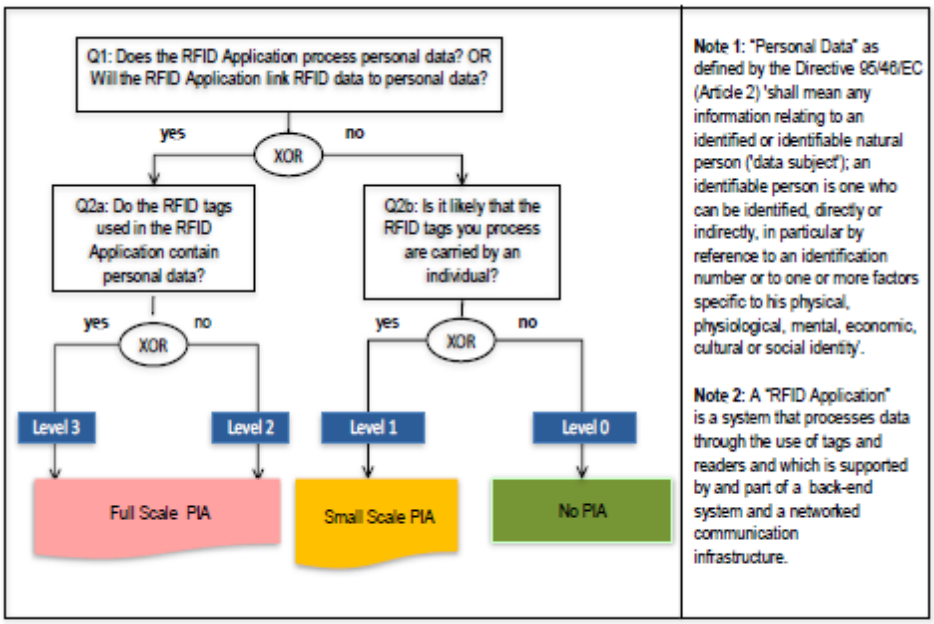

Figure 4.4.3.1: A Decision Tree format in view of determining whether a full-scale or a small-scale PDPIA is necessary

According to the initial information on the RFID application in eVACUATE, there will be different categories of RFID tags, which will contain personal data, e.g. tags for pregnant women and for people with disabilities. These categories of data could be classified as special categories of data or sensitive data under Article 8 (1) of Directive 95/46/EC, as this

[247] The Decision Tree is taken from Figure 1 of the PDPIA Framework, p. 7

discloses information on the health life of the bearers of the tags. Their processing is in principle prohibited. However, there is an exclusive list of provisions which allow the processing of sensitive data.[248] The potential legal basis for processing of this information could be consent and/or legitimate interests of the data subject.[249] If other personal data is processed, e.g. a unique number, this would also qualify as personal data[250] and thus a relevant ground for processing it must exist (i.e. in Article 7 Directive 95/46/EC).

The PDPIA should contain a highly detailed risk assessment and the mitigation measures (for both back-end and tag data) are well developed. In addition, if the personal data processed by the RFID application could be used for other purposes, a new PIA might need to be carried out to ensure that the new (additional) risks are mitigated.[251]

During the **risk assessment phase** the operator should identify at an early stage of the application development the possible privacy risks that might ensue from the RFID application and to document what measures are to be or have been taken to mitigate these risks. [252] It is advisable that the thorough risk assessment is carried out before the architecture of the RFID application is finalized so that the necessary privacy enhancing technological solutions are incorporated in the design of the application from the very beginning.[253]

When carrying out a risk assessment the questions that need to be considered are the likelihood of occurrence of the identified risks and the scale of the consequences so that the risks can be classified as low, medium or high.[254] The PDPIA Framework authors have described the process visually in the following way:[255]

[248] Article 8 (2) Directive 95/46/EC
[249] Article 8 (2) (a) and 8 (2) (c) Directive 95/46/EC
[250] WP 29 Opinion 9/2011, p. 5
[251] PDPIA Framework, p. 7
[252] PDPIA Framework, p. 7
[253] PDPIA Framework, p. 8
[254] PDPIA Framework, p. 8 -9
[255] PDPIA Framework, p. 8

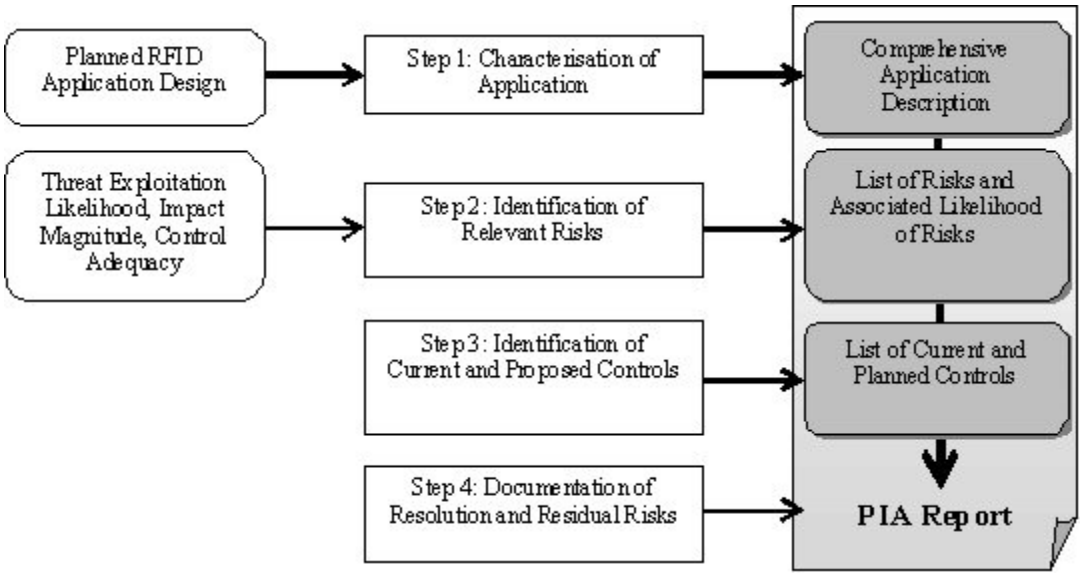

Figure 4.4.3.2: Steps that should be followed by the operator of an RFID application

As is shown above, the steps that the operator of an RFID application should take are the following: detailed description of the application,[256] the identification of the associated privacy risks, the identification of controls to mitigate the risks, as well as the drafting of a PDPIA report, which concludes whether RFID application is approved after the risk assessment and risk mitigation strategies have been implemented or whether the current application needs further risk mitigation measures in order to be approved and thus a new PDPIA needs to be carried out at a later stage. With regards to the mitigation controls that are to be considered, they could be of either a technical or non-technical nature. The former ones refer to the settings and mechanisms which are embedded into the application (e.g. encryption). The latter relate to management and operational controls and procedures. These aim at preventing or detecting and warning of potential or actual violations.[257]

Once the PDPIA is completed by the operator, it should be submitted to the internal data protection officer if one is appointed as well as notified to the respective national data protection supervisory authority.[258] In addition, the RFID Application operator is required to draft and publish an information policy for each application. This policy should be accessible and easy to understand by the affected individuals and should contain a summary of the

[256] Annex I describes in detail the information to be provided: RFID Application Operator; RFID Application Overview (RFID Application name, purpose(s) of the application, basic use case scenarios, components and technology used, geographical scope of the RFID application, categories of individuals impacted by the application, individual access and control), PDPIA Report number and version, RFID Data processing (categories of data processed; if sensitive data will be processed); Data Storage (data stored and retention period); Internal and External Data Transfer (recipients, purposes, transfers outside the EEA). P. 12
[257] PDPIA Framework, p. 10
[258] PDPIA Framework, p. 11; Article 18 Directive 95/46/EC

PDPIA.[259] It is recommendable that in the process of conducting a PIA the stakeholders are consulted.[260]

Although the eVACUATE RFID tag application is still under development some initial remarks with regards to the risks posed by RFID cards and tickets could be made.

In the context of eVACUATE, which seeks to facilitate the evacuation of large crowds, it must be demonstrated that the functionalities of the RFID tags will actually contribute to the more effective evacuation and saving of human life. Currently it is planned that the passive RFID tags will be active only in the range of 1 m and they will be detected only when the citizen passes through a gate that will be installed at the entrance of for example metro stations, for example. However, it is argued that the problem with passive RFID tags is that human bodies attenuate RF signals, which makes the placement of the antennae and tags of major importance. Thus, in the context of large crowds data can be lost, which could lead to inaccuracies of the collected data. In addition, RFID tags could be damaged easily, which again affects the quality of the data processed.[261]

Thus, the question which arises here is whether all RFID tags will be detected with sufficient accuracy when a large number of individuals, i.e. a crowd, passes through these gates and whether the whole RFID application will process the personal data correctly as required by Directive 95/46/EC. It must be borne in mind that in the case of evacuation, the accuracy of information on location, number of individuals, etc, is of critical importance since it is human life that is at stake. The RFID application must thus be reliable enough. In addition, measures have to be taken to ensure that the RFID application does not lead to unwarranted and unnecessary tracking of certain individuals which are detected by the application, especially outside the designated premises.

In terms of security risks related to RFID technologies, some have already studied the security problems in RFID enabled smart cards for public transport such as the Dutch OV-chipcard. Some of the problems that were identified referred to, *inter alia*, the possibility for individuals to be tracked, the ease with which the card could be cracked and data on it manipulated. In general it was concluded that security issues make or break large scale ICT applications.[262]

[259] Opinion 9/2011, p. 6; Point 7 of the Commission Recommendation
[260] Opinion 9/2011, p. 5
[261] E.R. Galea et al, "Collection of Evacuation Data for Large Passenger Vessels," in R.D. Peacock, "Pedestrian and evacuation dynamics," Springer 2011, p. 166-167
[262] B. Jacobs, "Architecture is politics: Security and Privacy Issues in Transport and Beyond," in S. Gutwirth et al (eds), *Data Protection in a Profiled World*, Springer 2010, p. 291 - 295

Last but not least, RFID applications operators which process personal data shall observe the principles set out in Directives 95/46/EC (also referred to as privacy targets in Annex II), 1999/5/EC and 2002/58/EC.[263]

4.5. e-Privacy Directive: Public Communications Networks

In the course of managing crowds it is essential that the responsible private and public actors have reliable channels of communication with each other. Currently all end-users make use of TETRA (terrestrial trunked radio). eVACUATE aims at improving the communication channel between the actors by designing a new communication system.

Where applicable, each end user of the system designed in eVACUATE should observe the national legislation which might apply to emergency communications. For example, in Belgium there exists a radio system for emergency and security communication, called ASTRID, which covers the whole of Belgium. This network for electronic communications is considered to be *sui generis*, i.e. neither public or non-public and the services which it provides are also *sui generis* and are thus regulated by that specific law.[264]

Although different national laws apply, some general provisions stemming from EU level legislation should be considered. In the first place, the integrity of the public telephone networks should be ensured so that uninterrupted access to emergency services can be provided.[265] Pursuant to the Universal Services Directive, Member States shall ensure that public telephone network operators make available the location of callers of the Single European Emergency Call Number 112 to authorities responding to emergencies to the extent that this is technically possible.[266]

Location data and location-based services

Thus, in the framework of emergency management processing the location of specific individuals could become desirable when rescue operations are undertaken. One of the possible means of locating individuals, besides video monitoring and RFID cards, is through a smartphone application, which will process the location data of the users of a terminal equipment.

Pursuant to the e-Privacy Directive, location data "*means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic*

[263] Recitals 10 and 11 of Commission Recommendation
[264] http://www.astrid.be/templates/content.aspx?id=1224&LangType=1033; also Article 12(1) Loi relative aux radio-communications des services de secours et de securite (1), 8 Juin 1998 (Belgium).
[265] Article 23 Universal Services Directive
[266] Article 26 (3) Universal Service Directive

communications service."[267] More precisely, location data may include information on the latitude, longitude and altitude of the terminal equipment; to its movement; to the level of accuracy of the location information; to the time the location information was recorded, as well as to the identification of the network cell in which the terminal equipment is located at a certain moment.[268]

According to the Article 29 Working Party location data qualifies as personal data since they relate to an identified or identifiable individual.[269] Thus, within the framework of the e-Privacy Directive, as long as location data refers to the "geographic position of the terminal equipment of a user of a publicly available electronic communications service," it is always personal data.[270]

Within the definition of location data one could also fit certain types of traffic data. Traffic data is "*any data processed for the purpose of conveyance of a communication on an electronic communications network or for the billing thereof*."[271] Since traffic data may refer, *inter alia*, to the location of the terminal device at the beginning and end of a communication they are at the same time also location data.[272] If location data are processed to convey an electronic communications network, they would be classified as traffic data.[273]

However, the term of location data is broader than traffic data. Location data also covers data which are "not processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof."[274] Pursuant to Article 9 of the e-Privacy Directive, they qualify as location data other than traffic data and they are processed for the provision of value added services.[275] Value added services are defined as "any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof" and are based on the location of the user.[276] A prerequisite for the provision of the service is the consent of the user.[277] These services are termed as *location-based services*.

[267] Article 2 (c) Directive 2002/58/EC
[268] Recital 14 Directive 2002/58/EC
[269] Article 29 Data Protection Working Party, "Opinion on the use of location data with a view to providing value added services," WP 115 (2005), p. 3
[270] E. Kosta, "Consent in European Data Protection Law," Nijhoff Publishers 2013, Nijhoff Studies in EU Law, Vol. 3, p. 328
[271] Article 2 (b) Directive 2002/58/EC
[272] E. Kosta, p. 327; Recital 15 Directive 2002/58/EC
[273] E. Kosta, p. 327
[274] Article 2 (b) Directive 2002/58/EC
[275] Article 9 Directive 2002/58/EC
[276] Article 2 (g) Directive 2002/58/EC; E. Kosta, p. 328
[277] Article 9 and Recital 35 Directive 2002/58/EC

Location-based services are characterized as information services which use the location of users via mobile network cells or satellites in order to provide services that are tailored to the precise geographical location of the user.[278] However, location based services refers not only to value added services which process location data other than traffic data, but it also covers a broad range of services that are provided via different wireless technologies and are based on location information, "falling both within and beyond the definition of location data of the e-Privacy Directive."[279] Therefore, the location based services could refer to both services that are delivered via public communications networks or publicly available electronic communications services.[280]

Nevertheless, pursuant to Article 9 (1) of Directive 2002/58/EC, the Directive governs only those location based services that process location data other than traffic data provided over a public communications network or in a publicly available electronic communications service and excludes services provided over private networks, such as enterprise networks.[281] Thus, sometimes services fall into a grey zone and it might not be easy to decide whether they are regulated by Article 9 of the e-Privacy Directive.[282] Amongst the relevant examples are the RFID applications or sensor-based technologies.[283] As mentioned above, pursuant to Article 9 of the e-Privacy Directive, the processing of location data other than traffic data for the provision of location based services should be based either on the consent of the user or otherwise the location data should be rendered anonymous.

However, Member States shall make sure that there are transparent procedures which would allow providers of public communications networks or services to override "the elimination of the presentation of calling line identification" as well as the requirement for consent of the terminal equipment user for the processing of location data on a per-line basis in cases of emergency in order to respond to emergency calls. This exemption applies to entities which handle emergencies and which are recognized as such by the Member States.[284] Further, Member States may restrict certain provisions of the Directive, such as those on traffic data and location data other than traffic data only when the measure is

[278] J. Hladjk, "Location Based Services: European Data Protection Rules for Mobile Commerce," *Privacy and Security Law, BNA 15.06.2009,* p. 1
[279] E. Kosta, p. 329
[280] E. Kosta, p. 329
[281] Generally speaking, Directive 2002/58/EC doesn't apply to networks and services addressed to "closed-user groups". This includes e.g. networks (for example WIFI) made available to users on a university campus, an airport or a cruise ship.
[282] E. Kosta, p. 329
[283] E. Kosta, p. 330
[284] Article 10 (b) Directive 2002/58/EC;

necessary, appropriate and proportionate to safeguard for example public security.[285] In cases of emergency there might be different actors involved. As concerns the responsibilities of the different actors in the delivery of value added services, the mobile operators' processing activities are regulated by the e-Privacy Directive, while third parties' processing is regulated by Directive 95/46/EC.[286] Thus, both the e-Privacy Directive and Directive 95/46/EC might become applicable, whereby the latter serves as *lex generalis* and the former as *lex specialis* as it particularizes and complements Directive 95/46/EC.[287] Therefore, in cases of emergencies when the matter is not regulated by Directive 2002/58/EC, it will be regulated by Directive 95/46/EC and one could try to find a legal basis for the processing in Articles 7 and 8 of the said Directive.

In addition, the processing should be carried out only by "persons acting under the authority of the provider of the publicly available communications service or of the third party providing the value added service" and shall respect the purpose limitation principle and not processed for longer than necessary for the provision of the service.[288]

4.5.1. Smartphone application

One of the possible means of locating individuals and even sending them evacuation instructions is through a smartphone application, which individuals could download. If the communication of information via such a smartphone application takes place over publicly available communication networks, then the provisions of the e-Privacy Directive would apply.[289]

When such an application is provided for purposes of civil protection, it could be considered as an e-Government service. E-Government refers to "*the use of information and communication technologies in public administrations combined with organisational change and new skills in order to improve public services and democratic processes and strengthen support to public policies*."[290] Examples of e-Government initiatives are the Transport for London initiatives such as the travel information services, the electronic travel information,

[285] Article 15 (1) Directive 2002/58/EC
[286] E. Kosta, p. 331 – 332; Article 29 Data Protection Working Party, "Opinion on the use of location Data with a view to providing value added services," WP 115, (2005), p. 4
[287] J. Hladjk, "Location Based Services: European Data Protection Rules for Mobile Commerce," Privacy and Security Law, BNA 15.06.2009, p. 2
[288] Article 9 Directive 2002/58/EC
[289] Recitals 7 and 12, 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), hereinafter the e-Privacy Directive.
[290] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0567:FIN:EN:PDF, p. 7

and on-line consultations.[291] If the e-Government service (e.g. smartphone application) is provided over a publicly available communications network, then the provisions of the e-Privacy Directive should apply.

Emergency services are amongst the important and significant public services as they protect the lives of citizens.[292] In general public services should be all – inclusive, i.e. be available and accessible to all, independently of the skills or income of the recipients.[293] Therefore, it should be ensured that such an emergency service as the smartphone app would be accessible to all members of the crowd. Thus, opportunities for sending SMS to those not in possession of smartphones should be considered or other methods for reaching out to all the present individuals should be developed.

Liability of service providers

In principle, when information is communicated via electronic means, liability could ensue for the wrongful content of information (e.g. sending misleading evacuation instructions). On EU level the e-Commerce Directive regulates the liability of intermediary service providers. More precisely, it contains provisions on the exemptions from liability of the intermediary service providers in certain cases.[294]

The first one is the situation in which the intermediary service provider acts a mere conduit. This implies that the intermediary service provider only transmits the information in a communication network or provides access to the communication network. In this case he will not be held liable if the intermediary service provider:

a) does not initiate the transmission;
b) does not select the receiver of the transmission; and
c) does not select or modify the information contained in the transmission.[295]

This would be the case even if the activities of the intermediary service provider involve "*the automatic, intermediate and transient storage of the information*" for the purposes of the transmission of information.[296]

Second, the exemption applies if the intermediary service provider engages in a transmission of information in a communication network which involves "*the automatic, intermediate and transient storage of the information*" for the purposes of making the further

[291] http://www.tfl.gov.uk/assets/downloads/e-gov.pdf, p. 16
[292] C, Ng and D. Chiu, "e-Government integration with web services and alerts: A case study on an emergency route advisory system in Hong Kong," *Proceedings of the 39th Hawaii International Conference on System Sciences – 2006*, p. 1
[293] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0567:FIN:EN:PDF, p. 7
[294] Chapter II, Section 4 of the e-Commerce Directive
[295] Article 12 (1) e-Commerce Directive
[296] Article 12 (2) e-Commerce Directive

transmission of the information more efficient to recipients upon their request. Again this is conditional upon the following:

a) does not modify the information;
b) complies with conditions on access to the information;
c) complies with rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
d) does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information; and
e) acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.[297]

Third, the exemption applies in the case of hosting. Hosting is "*the storage of information provided by a recipient of the service*." To benefit from the exemption, the intermediary service provider must meet the following requirements:

a) does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.[298]

In addition, the recipient of the service acts under the authority or control of the provider.[299]

Still, in all of the above-mentioned cases a court or a national administrative authority could order the termination or the prevention of an infringement.[300] In the case of hosting, Member States may establish procedures for the removal or disabling of access to information.[301]

[297] Article 13 (1) e-Commerce Directive
[298] Article 14 (1) e-Commerce Directive
[299] Article 14 (2) e-Commerce Directive
[300] Article 12 (3) ; 13 (2) and 14 (3) e-Commerce Directive
[301] Article 14 (3) e-Commerce Directive

5. Pilot Demonstrations and Validation

While the previous section discussed the privacy and data protection provisions in light of their implications for the operational phase of the eVACUATE solution. These provisions also apply to the research phase of the project.

The eVACUATE project has envisaged conducting pilot demonstrations to validate the system developed in eVACUATE at the premises of the four end-users: at the Athens airport, at the metro in Bilbao, at the Anoeta stadium in San Sebastian, and at an STX cruise ship. During the pilot demonstrations personal data might be processed.

In order for the demonstrations to be compliant with their data protection obligations, the project partners will have to take the following steps:

Step 1:

Within the project it has to be determined who the controller for each of the four pilot demonstrations will be. This will be the partner who will define the purposes and means of the data processing operations (e.g. the CCTV filming, the subsequent processing and analysis of the video footage, etc). The other partners of the consortium who are involved in data processing activities during the demonstrations will probably be designated as processors. If external parties to the project are involved (e.g. national civil protection authorities, police, telecom operators, etc) they should also be assigned the roles of processors (or recipients of data, or third parties).

Step 2:

A controller-processor agreement has to be concluded between the controller of the activity on one hand and the processor(s).

Step 3:

The rights of the volunteers, i.e. the data subjects have to be guaranteed. To provide them with complete information, it is recommended that a privacy statement is provided to them, which will contain information on the activity, the controller, the data processed, their storage, the rights of the volunteers, the retention of data, access to it, the authority to which they can turn to submit a complaint in case of a breach, etc.

Step 4:

Currently, under Directive 95/46/EC the controller(s) has to submit a notification to the local national data protection authority in advance before the demonstrations (i.e. the

Greek, the Spanish and the French Data Protection Authorities).[302] However, if the Proposed General Data Protection Regulation enters into force, then the controller or processor shall consult in advance the Data Protection (supervisory) Authority only if the data protection impact assessment concludes that the operation presents specific risks or if the supervisory authority considers it necessary to carry out a prior consultation on processing operations which present specific risks, as specified and made public by the supervisory authority.[303]

Step 5:

Last but not least, all the actors involved in the demonstrations, whether internal or external to the consortium, will have to meet one of the legal bases for the processing of personal data. It is likely that one of the applicable legal basis will be the consent of the volunteers.

[302] Article 18 (1) and (2) Directive 95/46/EC
[303] Article 34 Proposed General Data Protection Regulation

6. Conclusion

The aim of the present deliverable was to outline the high-level legal and ethical framework applicable to the eVACUATE project, both in its research phase and its validation phase. The deliverable focused on the aspects of the responsibilities and liabilities of the different private and public actors who are engaged in the management of large crowd gatherings and the relevant safety measures they are supposed to put in place, including those that accommodate the needs of the vulnerable groups. The analysis was built on examples from the four use-case scenarios: the Athens International Airport (AIA), STX cruise ship, Anoeta stadium in San Sebastian (ASRS) and the metro in Bilbao (METB). The safety measures taken at the different venues, however, have to comply also with the requirements stemming from the privacy and data protection legislation. Therefore, the necessary balance has to be struck between safety and privacy and data protection.

On the basis of the analysis above, the following list of ethical and legal requirements have been derived:

1. Operational phase
    - Safety and security measures

    The responsible actors, both private and public, have to comply with their internal safety and security provisions, which are based on their internal regulations and local laws to which they are subject. These safety provisions refer both to measures to prevent a crowd disaster from occurring and to measures to mitigate the disaster to reduce casualties.

    In addition, in the cruise ship scenario, the safety regulations contained in the International Convention for the Safety of Life at Sea and the annexes to it, have to be complied with by cruise ships whose flag state is a signatory to the Convention. Cruise ships sailing in US waters have to further comply with the US regulations.

    In the stadium scenario, the UEFA Safety and Security Regulations have to be complied with.

    - Vulnerable groups

      The needs of vulnerable groups, such as the disabled, have to be accommodated as much as possible in the crowd management process.

    - Privacy and Data Protection

        a. Every personal data processing operation (video surveillance, RFID tickets, smartphone applications) must have a clearly designated controller. In the framework of eVACUATE, due to the numerous

actors involved in crowd management, different controllers are expected to compose the "Smart Spaces" and thus every one of them must be clearly identified.

b. Every personal data processing operation must have a legal basis, e.g. the consent of the data subject. If consent is the applicable legal basis, then it must be freely given, specific and informed.
c. When CCTV monitoring is used, the national legislations on CCTV must be observed (installation of cameras, retention period, etc).
d. The controller has to ensure compliance with all the principles of data protection: data minimization, purpose limitation, adequate retention period, data accuracy, security and confidentiality of processing.
e. Before personal data processing operations commence, the controller must justify the necessity and proportionality of each operation. The margin of appreciation of the authorities responsible for crowd management is wider in cases of evacuation in comparison to the prevention stage.
f. The controller must guarantee the rights of data subjects (information, objection to processing, right to access, rectification, erasure or blocking).
g. The controller must carry out a Privacy and Data Protection Impact Assessment of the RFID tickets and submit it to the supervisory authority at least 6 weeks before the application becomes operational.
h. The partners of eVACUATE should implement the principle of Privacy by Design in the eVACUATE product.

2. Research phase

   The partners of the eVACUATE project have to follow the five steps outlined in section 5 in order to comply with their data protection obligations.

7. Annex A – List of Acronyms

Acronym	Meaning
ADA	Americans with Disabilities Act
ADO	Airport Duty Officer[304]
AHFC	Airport Hellenic Fire Corps[305]
AIA	Athens International Airport
ASOC	Airport Services Operations Centre[306]
ASRS	Anoeta Stadium Real Sociedad
AmI	Ambient Intelligence
BATs	Best Available Technologies
CCTV	Closed Circuit television
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
HCAA	Hellenic Civil Aviation Authority[307]
ICT	Information and Communication Technologies
IMO	International Maritime Organization
METB	Metro Bilbao
PDPIA	Privacy and Data Protection Impact Assessment
PETs	Privacy Enhancing Technologies
PRM	Persons with Reduced Mobility
PRMC	Persons with Reduced Mobility Contractor
RFID	Radio Frequency Identification
TFEU	Treaty on the Functioning of the European Union
TEU	Treaty on the European Union
UEFA	Union of European Football Associations
UN	United Nations

[304] At Athens International Airport (AIA)
[305] At AIA
[306] At AIA
[307] At AIA

8. Annex B – List of Sources

Academic literature and Reports

J. L. Abbott and M.W. Geddie, "Event and venue management: minimizing liability through effective crowd management techniques," Event Management, Vol. 6, pp. 259-270

J. Alhadeff et al, "The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions," SSNR, September 26, 2011, http://ssrn.com/abstract=1933731

D. Bigo, S. Carrera, B. Hayes, N. Hernandez and J. Jeandesboz, "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders. An evaluation of Current and Forthcoming Proposals," CEPS Papers in Liberty and Security, No 52/December 2012

G. Buttarelli, "Legal Restrictions – Surveillance and Fundamental Rights," New technical Means of Surveillance and the Protection of Fundamental Rights – Challenges for the European Judiciaries, Vienna June 19th 2009, Justizpalast/Palace of Justice

A. Cava and D. Wiesner, "Rationalizing a decade of Judicial responses to exculpatory clauses," 28 Santa Clara Law Review 1988

A. Cavoukian, "Privacy By Design,"
http://www.ipc.on.ca/images/Resources/privacybydesign.pdf

A Cavoukian, Chibba M., Stoianov A, "Advances in Biometric Encryption: Taking Privacy By Design from Academic Research to Deployment," Review of Policy Research, Vol. 29, Number 1, (2012)

E. Claes et al (eds), "Privacy and the criminal law, Intersentia, 2006

P. Cooke, DAN Legal Network National Coordinator for Britain in "The Good Samaritan Law across Europe," the DAN Legal Network, National Coordinators Committee.

F. Coudert, "Towards a new generation of CCTV networks: Erosion of data protection safeguards?, "Computer Law and Security Review 25 (2009)

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

B. Crettez and R. Deloche, "On the optimality of a duty-to-rescue rule and the cost of wrongful intervention," International Review of Law and Economics, Vol. 31, Issue 4, December 2011

S. A. DiPolito, "Casenote: Title III of the Americans with Disabilities Act Applies to Foreign Cruise Ships; But qhat exactly is required?," *Mercer Law Review Spector, Vol. 57, 2006*, http://www2.law.mercer.edu/lawreview/getfile.cfm?file=57309.pdf

J. Dumortier et al, "D.7.1 Legal Requirements for Trust in the IoT," uTRUSTit – Usable Trust in the Internet of Things

J. Dumortier, "ICT-Recht" Leuven: Acco, 2010

L. Ellis, “Notes: Talking about my generation: Assumption of risk and the rights of injured concert fans in the twenty-first century,” 80 Texas Law Review 607, 2001-2002

M. L. Gras, “The Legal Regulation of CCTV in Europe,” Surveillance and Society 2004, CCTV Special 2 (2/3), pg. 219

S. Gutwirth et al (eds), Reinventing Data Protection?, Springer 2009

S. Gutwirth et al (eds), Data Protection in a Profiled World, Springer 2010

S. Gutwirth, Y. Poullet, P. de Hert and R. Leenes (eds), “Computers, Privacy and Data Protection: An Element of Choice,” Springer 2011

S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet (eds), “European Data Protection: Coming of Age,” Springer 2013

S.M.V. Gwynne, “Conventions in the Collection and Use of Human Performance Data,” Hughes Associates, Inc, NIST GCR 10-928, http://www.nist.gov/el/fire_research/upload/NIST_GCR_10_928.pdf

P. de Hert et al, “Deliverable D 7.2: Biometrics in Europe: Inventory on Biometric Data and Privacy Legislation,” Biometric European Stakeholders Network, November 2010

P. de Hert and D. Wright (eds), “Privacy Impact Assessment,” Springer 2012

M. Hildebrandt and S. Gutwirth (eds), Profiling the European Citizen: Cross-Disciplinary Perspective, Springer 2008

J. Hladjk, “Location Based Services: European Data Protection Rules for Mobile Commerce,” Privacy and Security Law, BNA 15.06.2009

K. Janssen, “The availability of spatial and environmental data in the European Union. At the crossroads between public and economic interests,” Alphen a/d Rijn: Kluwer Law International 2010

J. Hofstetter and W. v. Marschall, “Comments: Amendment of the Belgian Code Penal: The duty to rescue persons in serious danger,” 11 American Journal of Comparative Law, 1962

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

P. Hustinx, “Accountability in the Proposed Regulation,” Brussels, 3 December 2012

Maitre F. Jaeck, Attorney at Law, DAN Legal Network Executive Director and National Coordinator for France

J. E. Kastenburg, “A Three Dimensional Model of Stadium Owner Liability in Spectator Injury Cases,” Marquette Sports Law Review, Volume 7, Issue 1 Fall, Article 5, 1996

E. Kosta, “Consent in European Data Protection Law,” Nijhoff Publishers 2013, Nijhoff Studies in EU Law, Vol. 3

C. Kuner, , "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law," Privacy & Security Law Report, 11 PVLR 06, 02/06/2012, Bloomberg, BNA

R.D. Peacock, "Pedestrian and evacuation dynamics," Springer 2011

A Rouvroy, "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence," Studies in Ethics, Law, and Technology, Berkeley Electronic Press, 2008. Available at SSRN: http://ssrn.com/abstract=1013984

J. R. Silvers, "Risk Management for Meetings and Events," Events Management Series, Elsevier 2008

J. D. Sime, "Crowd facilities, management and communications disasters," Facilities, Vol. 17, Number 9/10, 1999, pp. 313 – 324

S. Venier and E. Mordini, "Second - generation biometrics," in Privacy, data protection and ethical issues in new and emerging technologies: Five case studies, eds. Rachel Finn and David Wright (PRESCIENT consortium, 25 November 2011)

"EU study on the Legal Analysis of a Single Market for the Information Society: New Rules for a New Age?," DLA Piper, November 2009

Legislative Sources and Legislative Proposals

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, P 31-50

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

Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, O. J. L 210, 07/08/1985 P. 0029 – 0033

Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), O.J. L. 178

Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, O.J. L 217/18 – 26

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), hereinafter the e-Privacy Directive.

Loi relative aux radio-communications des services de secours et de securite (1), 8 Juin 1998 (Belgium)

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

Protocol No. 12 of the Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 2000

Charter of Fundamental Rights of the European Union

Council of Europe Convention 108/81

Additional Protocol No 4 European Convention on Human Rights

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

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

Grundgesetz fuer die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBI. S.1), zuletzt geaendert durch das Gesetz vom 11. Juli 2012 (BGBI. S. 1478)

Belgian Act of 21 March 2007 governing the installation and the use of surveillance cameras

The UK Public Order Act 1986

UEFA Safety and Security Regulations, Edition 2006

Cruise Vessel Security and Safety Act of 2010, which adds par. 3507 to Chapter 35 of title 46, United States Code

International Convention for the Safety of Life at Sea, 1974, annex thereto and the 1988 Protocol relating thereto

Case-law

Judgement 1BvG 370/07, the German Constitutional Court

Judgment, 1 BvG 1215/07, 24.04.2013, the German Constitutional Court

Court of Justice of the European Union, C – 275/06, Promusicae, Opinion of the General Advocate J. Kokott, 18 July 2007

Kruslin v France, ECtHR, 11801/85, 24 April 1990, Series A no.176-A

Rotaru v Romania, EctHR, 4 May 2000, application no. 28341/95

S. and Marper v UK, ECtHR, 4 December 2008

Budayeva and others v Russia, ECtHR, Applications nos. 15339/02, 21166/02, 20058/02, 11673/02 and 15343/02, 29.09.2008

Others

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

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "European Disability Strategy 2010 – 2020: A Renewed Commitment to a Barrier-Free Europe," COM (2010) 636 final, Brussels, 15.11.2010

National Disability Authority (NDA), "Promoting Safe Egress and Evacuation for People with Disabilities," ISBN: 978-1-870499-18-7

The European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the data protection reform package," 7 March 2012

Article 29 Data Protection Working Party, "Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance," 11 February 2004

Article 29 Data Protection Working Party, "Opinion on the use of location Data with a view to providing value added services," WP 115, (2005)

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

Article 29 Data Protection Working Party, Working Party on Police and Justice, "The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data," Adopted on 1 December 2009

Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking," 12 June 2009

Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010

Article 29 Data Protection Working Party, “Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications,” 11 February 2011

Article 29 Data Protection Working Party, “Opinion 03/2013 on purpose limitation,” 2 April 2013

Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011

EDPS Comments on DG CONNECT'S Public Consultation on Improving Network and Information Security (NIS) in the EU, 10 October 2012

Prof. Dr. T. Mayen and Dr. F. Hoelscher, “Zur Abgrenzung der Aufgaben von Veranstalter, Stadt Duisburg und Polizei bei der Loveparade 2010: Kurzgutachterliche Stellungnahme im Auftrag des Ministeriums fuer Inneres und Kommunales des Landes Nordrhein-Westfalen,“ Dolde Mayen & Partner

Cabinet Office, “Responding to Emergencies: the UK central government response: Concept of Operations,” https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192425/CONOPs_incl_revised_chapter_24_Apr-13.pdf

Cabinet Office, “Expectations and Indicators of Good Practice Set for Category 1 and 2 Responders,” The Civil Contingencies Act (2004), its associated Regulations (2005) and guidance, the National Resilience Capabilities Programme, and emergency response and recovery; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61088/expectations_set-parts1to3.pdf

Belgian House of Representatives Parliamentary Commission of Inquiry: (Extracts from Part V (Conclusions) of the Report of the Parliamentary Commission of Inquiry to the Belgian House of Representatives of 9 July 1985 (translated from the House of Representatives document); Terms of reference: The causes, circumstances and lessons to be drawn from the tragic events occurring during the Liverpool/Juventus match on Wednesday 29 May 1985; in Home Office, Committee of Inquiry into Crowd Safety and Control at Sports Grounds: Final Report, Chairman Mr. Justice Popllewel: Presented to Parliament by the Secretary of State for the Home Department and the Secretary of State for Scotland by Command of Her Majesty, January 1986, London, Her Majesty’s Stationery Office; Chapter 1 and Appendix D

Home Office, The Hillsborough Stadium Disaster 15 April 1989, Inquiry by the RT Hon Lord Justice Taylor, Final Report, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, January 1990

http://www.cnil.fr/les-themes/videosurveillance/fiche-pratique/article/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de/

http://www.earthobservations.org/documents/geo_vi/07_Implementation%20Guidelines%20for%20the%20GEOSS%20Data%20Sharing%20Principles%20Rev2.pdf

http://www.earthobservations.org/geoss_dsp.shtml

http://ec.europa.eu/environment/seis/what.htm

http://copernicus.eu/

http://copernicus.eu/pages-principales/infrastructure/

http://copernicus.eu/pages-principales/infrastructure/data-access/

http://copernicus.eu/pages-principales/services/emergency-management/

http://emergency.copernicus.eu/mapping/ems/ems-mapping-service

http://emergency.copernicus.eu/mapping/ems/who-can-use-service

http://www.astrid.be/templates/content.aspx?id=1224&LangType=1033

http://www.welt.de/vermischtes/weltgeschehen/article13479369/Duisburger-Loveparade-Genehmigung-rechtswidrig.html

http://www.wdr.de/tv/westpol/sendungsbeitraege/2013/0707/loveparade.jsp

http://www.bbc.co.uk/news/uk-19545126