DELIVERABLE REPORT

DELIVERABLE N^0:	D4.4
DISSEMINATION LEVEL:	PUBLIC
TITLE:	FINAL REPORT COMPLIANCE WITH LEGAL AND ETHICAL REQUIREMENTS (FORMULATING ETHICAL AND LEGAL REQUIREMENTS FOR ELASSTIC)
DATE:	21/04/2016
VERSION:	FINAL
AUTHOR(S):	ANTONIO SILVA (INCODE), MV FERNANDEZ (INCODE)
REVIEWED BY:	WP LEADER – DR. KLEIN (SIEMENS AG)
APPROVED BY:	COORDINATOR – ANS VAN DOORMAAL (TNO)

GRANT AGREEMENT NUMBER:	312632
PROJECT TYPE:	FP7-SEC-2012.2.1-1 RESILIENCE OF LARGE SCALE URBAN BUILT INFRASTRUCTURE – CAPABILITY PROJECT
PROJECT ACRONYM:	ELASSTIC
PROJECT TITLE:	ENHANCED LARGE SCALE ARCHITECTURE WITH SAFETY AND SECURITY TECHNOLOGIES AND SPECIAL INFORMATION CAPABILITIES
PROJECT START DATE:	01/05/2013
PROJECT WEBSITE:	WWW.ELASSTIC.EU
TECHNICAL COORDINATION	TNO (NL) (WWW.TNO.NL)
PROJECT ADMINISTRATION	UNIRESEARCH (NL) (WWW.UNIRESEARCH.NL)

Executive Summary

The purpose of the ELASSTIC project is to improve the resilience, safety, and security of large scale built infrastructures. One part of the project is to develop a measurement system composed of wireless sensors that monitors the structural integrity of the building compartments following a crisis event. This system shall deliver real time sensor information in case of incidents such as fire, explosion or earthquake, suitable to:

1) provide additional dynamical information e. g. about inaccessible parts of a building following a crisis event. This information shall be used as data source for a *smart evacuation system*
2) enable *first responders* at the scene to
    a) make quick and fact-based judgments for the accessibility and safe evacuation of the building;
    b) better protect their own personnel by avoiding rescue routes that are in building areas that are close to collapse.

The current document sets out to outline and analyze the high-level ethical and legal framework and derive legal requirements which apply to the ELASSTIC 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 evacuation of the buildings.

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 fire scenario. It then goes on to define the possible liabilities in cases of breach of these responsibilities. The document 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 document 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 fire uses case.

Contents

Executive Summary **2**

Contents **3**

1 Introduction **5**
1.1 purpose and scope of the document 5
1.2 METHODOLOGY 5
1.3 Structure of the document 6

2 Legal and ethical aspects of ELASSTIC **7**
2.1 Introduction 7
2.2 Large crowd gatherings 7
2.3 Responsibilities for emergency prevention and response 9
2.3.1 Fire building scenario 9
2.3.2 Technologies for evacuation system in ELASSTIC. 15
2.4 elasstic Liability 15
2.4.1 ELASSTIC Criminal Liability 15
2.4.2 ELASSTIC Liability under Civil Law 16
2.4.3 ELASSTIC Product liability 18
2.4.4 Reducing liability and exemptions from liability 20
2.4.5 Vulnerable Groups 20
2.5 Conclusion 22

3 Privacy and data protection **23**
3.1 Introduction 24
3.2 PRIVACY 24
3.3 DATA PROTECTION 26
3.3.1 Defenitions / Concepts 27
3.3.2 Scope 28
3.3.3 Grounds for legitimacy 30
3.3.4 Principles of Data Processing 31
3.3.5 Rights of the data subject 32
3.3.6 Automated Decisions and Profiling 33
3.3.7 Confidentiality and Security of processing 34
3.3.8 Liability 35
3.4 Review of the EU Data Protection Framework 36
3.4.1 Accountability 36
3.4.2 Privacy By Design 37
3.4.3 Data Protection Impact Assessment 39
3.5 e-Privacy Directive: Public Communications Networks IN ELASSTIC 43
3.5.1 Smartphone application 43

3.5.2 Liability of ELASSTIC Smartphone application 43

4 Conclusions 45

5 Reference 47

6 Acknowledgment 48

1 Introduction

1.1 PURPOSE AND SCOPE OF THE DOCUMENT

The purpose of the present document is to outline the legal and ethical framework which applies to the ELASSTIC 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 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 document is thus to provide a legal and ethical analysis of all the above-mentioned aspects, which will be further applied to the system developed in ELASSTIC.
Last but not least, the document also provides an examination of the legal and ethical aspects relatedto legal and privacy issues of ELASSTIC, in particular the data protection requirements which have to be complied with when performing the scenarios demonstrations.

1.2 METHODOLOGY

The current document is prepared on the basis of research into the applicable legislation, case-law and soft-law, materials from the four end-users (such as emergency services, police, bombiers, ambulances, etc) as well as academic literature in order to provide a comprehensive and comprehensible analysis of the legal and ethical framework of managing evacuation systems.

ELASSTIC has to validate the project from a legal and ethical point of view. This validation will be through ethical and legal criteria defined in the project and will take place according to the "design thinking" methodology in order to obtain a result that is measurable for every one of the selected criteria.

The logical structure of this validation is composed of the following steps:

- Step 1: identify ethical regulations both at national and regional level applicable to the project. This action is materialized in the deliverable 4.1.
- Step 2: Ensuring that ethical requirements identified in step 1 from the design phase of the project. This action is materialized by reviewing the various documents of the WP3, thus ensuring traceability of the ethical requirements during the project life cycle
- Step 3: Identification of the legal criteria to validate the project

- Step 4: Using the scenarios defined in WP1 as input, define use cases to validate the project from a legal and ethical point of view. Consider two use cases that will be a function of the degree of maturity that has the BIM (medium and long-term).
- Step 5: Proceed to the ethical and legal validation of the project
- Step 6: Depending on the results, draw conclusion and recommendations (deliverable 4)

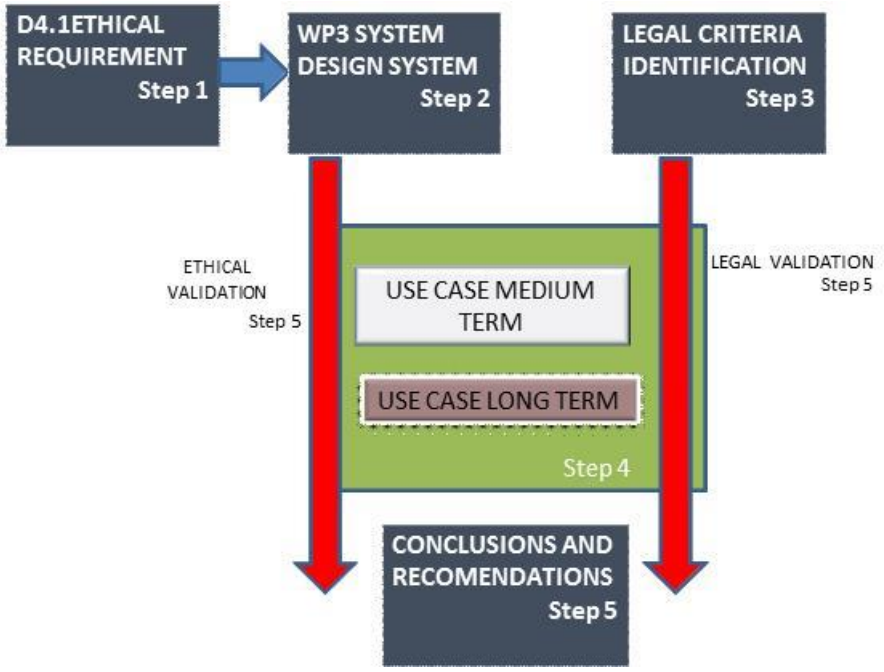

Figure 1: Ethical and legal rationale

1.3 STRUCTURE OF THE DOCUMENT

The document 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 diferent scenarios. Then the deliverable examines the needs of vulnerable groups as members of large crowds.
The document 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.

2 Legal and ethical aspects of ELASSTIC

2.1 INTRODUCTION

The purpose of this section is to examine the legal and ethical issues associated with evacuation systems. The responsibilities of the private and public actors (enterprises, region and local goverments, first responders, etc) 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.building evacuation) in situations where there are large crowd gatherings at different types of venues, taking as examples a fire building scenario.

2.2 LARGE CROWD GATHERINGS

Gatherings of large crowds (e.g. at football matches and concerts, busy metro stations and airports, large buildings) 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 [1] 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.” [2]

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.[3]

Moreover 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 the relevant measures to safeguard the lives of individuals.[4] In the context of emergency relief, the scope of

[1] 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

[2] J. D. Sime, p. 313

[3] 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)

[4] ECtHR, *Budayeva and others v Russia*, Applications nos. 15339/02, 21166/02, 20058/02, 11673/02 and 15343/02, 29.09.2008, par. 128

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.[5]
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)
    - Avoiding being discredited immediately
    - High-quality prior planning
    - Realizing, warning, taking charge
    - Triggering protective measures and relevant emergency
    - actions
    - Looking for information
    - Setting up a log book
    - Developing a team, separating crisis management
    - Avoiding irritating gestures
    - Getting a foothold on the communication landscape
    - Undertaking an integrated approach: a plan for action
    - Do not create an unmanageable landscape
- the reaction to a disaster once it has occurred (crisis stage),
    - Search and rescue
    - Emergy relief
    - Early recovery
- the mitigation measures after the crisis is over (post-crisis).
    - Medium and long term recovey
    - Community development
    - Disaster risk reduction
    - Envirmental concerns

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,[6] i.e. the crowd has lost control. For example, the crowd crisis could be caused by a security threat such as a disasters, a 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.”[7]
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.This represent a problem is Spain, Portugal, France, Italy and Germany because the roles are not defined.

[55] *Budayeva*, par. 137

[6] J. D. Sime, “Crowd facilities, management and communications disasters,” *Facilities, Vol. 17, Number 9/10, 1999, pp. 313 – 324,* p. 314

[7] Abbott and Geddie, p. 264

2.3 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. The following paragraphs provide an example of crowd safety measures and the different roles and duties of the various private and public entities engaged in crowd safety. The example is taken from the fire building scenario.

2.3.1 FIRE BUILDING SCENARIO

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

Step 1:

Within the project it has to be determined who the ELASSTIC controller for fire building scenario 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 ELASSTIC controller of the activity on one hand and the actors of the processor.

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). 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.

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.

Different crowd management policies are implemented at a large building. 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:
System modules:

- BIM (Buiding Information Model)
- Persons
- Sensors
- Evacuation system
- BMS (Building Management System)

Next items should be considered by in this scenario:

- To many / less persons than in reality
- Fire brigade gets wrong number of persons
- Based on smart phone infos: smart phone is laying on the desk
- Sensors not working
- Wrong threshold value
- Video camera is smoky
- BMS System not working & no power
- Doors can not be opened
- Wrong BIM architecture
- Different lay outs & rooms
- Wrong structural lay out
- Shut down electricity: at what time
- Evacuation system is not working
- Wrong input data
- Evacuation plan has not arrived the smart phones:
    - Is it allowed to send detailed person Infos to the evac system?
    - Handicapped persons

Planning for a fire scenario starts with careful research and forward thinking management. The steps are simple, but it takes time to find out what you could be facing and determine resources you need both inside the company and beyond.

1. **Step One Assess your needs**
   Certain strengths and weaknesses at your site will either help or hinder your emergency response. It's important to know what they are. Find out:
    - What fixed fire protection is provided? Is it in service?
    - Do employees know the locations of fire extinguishers and fire hose stations and how to use them?
    - What processing or storage hazards exist?
    - Are there staffing or equipment limitations?
    - Have you educated and trained key personnel?
    - Are drills and periodic staff training provided?

   Next, evaluate the impact of the hazards on your property, the general public, the environment or your ability to resume business after an emergency fire.

How could each one affect your day-to-day business operations? Consult with organizations outside the company, like municipal emergency planners or loss control consultants, to help you identify natural hazards common to your area.

Carefully research the history of emergencies at your facility. This can be very helpful for developing strategies. In the past, how did the response plan work as a result of incidents like hazardous materials spills, fire protection impairments and utility interruptions and poor equipment maintenance? Was the cause related to human error? What worked well? What could be improved? What changes would you make if it happens again?

Prioritize all the emergencies your facility has experienced from the most to the least severe. How frequently might they reoccur and how severely?

Use internal resources. They can be invaluable for this challenging effort. An Emergency Response Planning Committee not necessarily the people who will respond to the emergency can bring expertise from areas such as

- operations
- maintenance
- transportation
- engineering
- public relations
- risk management
- environmental health and safety
- human resources
- security
- legal
- labor relations

Others on staff often make good emergency responders and help reduce training time. Some can help train people or serve as leaders. Examples are volunteer firefighters and heavy equipment drivers. Crane operators, plumbers and electricians can be valuable, too.

Take a look at anything offsite that could expose your facility to emergencies. These hazards (also called "exposures") can be related to environmental problems, neighboring properties, and limited outside access to your property, such as roadway obstructions or dirt roads that easily become impassible during a rainstorm. Other examples of offsite hazards include poor or interrupted utility supplies, seasonal brush or forest fires, or frequent arson strikes. Security-related problems on and offsite can affect your facility. In what ways could each affect your facility?

Identify combustible or lightweight construction and other features such as the age of your building. Does each building meet existing code requirements? Have they been well maintained? Has there been a history of roof, wall or floor leaks?

Identify operations from raw materials coming in the door, to transportation and distribution of finished goods like these:

- Hazardous materials used in processing such as flammable liquids; toxic, corrosive or reactive materials; and combustible metals;
- Fixed equipment and storage hazards such as hydraulic oil-operated equipment, dust- or lint-producing equipment, flammable or combustible coolants, vapor or fume producing materials;
- Fuels and other energy sources used onsite such as natural gas, propane, electrical, flammable as well as other prepiped and cylinder gases;
- Warehouse storage (products/materials stored) and types of storage like rack, solid or palletized;
- Critical production equipment that would need special consideration during an emergency; and
- Access to rail, truck, and over-the-road transportation to move products and equipment.

Identify protection including:

- Fire protection available such as public water supplies, fire pumps and tanks, booster pumps, gravity tanks, and nearby, open bodies of water;
- Types of fixed automatic fire protection equipment such as sprinklers, gaseous suppression, foam, dry chemical and water mist;
- Types of manual suppression equipment like fire hose stations and fire extinguishers;
- Levees and flood walls;
- Sump pumps, curbs and drains;
- Sand, sandbags, portable barriers, emergency generators and portable pumps.

2. Step Two Create a written policy

This should contain three statements:

- The Purpose declares the company's intent and objectives. It also specifies planned limitations to responding to certain site-specific incidents.
- The Policy outlines the plan and top management's commitment. Review the plan at least annually to assure that changing conditions are included and kept current, and that personnel are available and qualified to respond.
- Responsibility designates people by name or title who generate and maintain the emergency response plan.

3. Step Three Plan levels of response

Create specific job assignments similar to the ones below and provide training accordingly. Some leading corporations, like airports or big manufacturing facilities, might use much larger staffs. A smaller business comprising maybe a warehouse and office might need only one person for the entire task.

The Emergency Coordinator launches the plan, and organizes training to respond efficiently during and after an emergency. Major responsibilities are to analyze each department's site-specific hazards, outline all scenarios every emergency could take, strategize protection, and determine responsibilities. To fulfill these responsibilities, the coordinator also:

- Arranges pre-incident planning with the fire service or other public agencies to set up a plan of action in event of a fire or other emergency;
- Establishes step-by-step response procedures for handling all emergencies, particularly fire;
- Directs emergency actions during the emergency;
- Makes sure the other members are in place and performing their assigned duties; and
- Assures that emergency materials are available prior to the specific season.

The Notifier calls the fire department his or her first priority. This person also keeps a current list of personnel and alternates, contacts personnel for all emergencies and notifies outside personnel such as fire, medical and rescue operations.

The Sprinkler Control Valve Operator knows where all valves are located and is responsible for operating them in the event of a fire. As long as it is safe to do so, this person:

- Goes to the valve that controls sprinklers protecting the fire area, makes sure the valve is open by physically testing it and stands by it until the person in charge orders it shut (essential step);
- Examines sprinkler control valves for damage after an earthquake, explosion or building collapse; and
- Closes only those valves needed to isolate broken piping, after checking with the person in charge and following all proper fire protection impairment procedures.

The Fire Pump Operator goes to the pump room when the fire alarm sounds and checks that the pump has started automatically. If not, he or she starts the pump and keeps it operating until instructed to shut it down by the person in charge. It's important for this person to be familiar with the operation and care of the pump, and trained in starting pumps manually and understanding the importance of pumps in relation to fire protection.

The Pipe Fitter knows about the piping distribution networks and can shut off supplies of flammable gases, liquids and other hazardous materials in an emergency. Duties:
Know where primary and secondary shutoffs are located and how they operate.

- Keep drains clear and restore sprinkler protection where necessary.
- Isolate, drain and repair any piping damaged by previous windstorms, explosions, collapses or earthquakes.
- Be familiar with equipment controls.

The Salvage Team gets the facility back in business as soon as possible after an emergency. Duties:

- Be able and ready to start salvage during and after the emergency. Actions should be immediate. Damage can worsen as time passes.
- Know how to salvage and clean equipment and stock
- Concentrate on valuable stock and equipment. Mopping up to remove dampness and drying out wet areas are typical tasks.
- Give priority to any major damage to vital equipment or processes.

It's important to contact contractors for repairs and rebuilding. Suppliers of spare parts should be immediately notified.

Watch Service personnel are a very important part, because they are often the only ones around when the facility is closed or when most personnel are offsite. These are the times watch services or security personnel will be required to fill positions. They should receive the same training:

- Know the procedures during and after an emergency and follow them carefully.
- Sound the fire alarm.
- Notify the fire service in event of fire.

- Check sprinkler control valves and fire pumps.
- Direct fire service personnel to the area of fire origin.
- Notify facility officials.

Firefighting Teams, typically used in larger organizations, are selected and trained to fight a fire until the fire service arrives or until the fire grows beyond their level of training. Trained personnel must:

- Know where fire extinguishers and hose stations are located and how to operate them.
- Know the types of extinguishers to use on different kinds of fires and how to operate each type of extinguisher. Extinguisher types include carbon dioxide (and other gaseous suppression agents such as Halon), dry chemical, foam, pump tank and stored pressure water-filled.
- Receive training on the use of hose lines to handle and operate them quickly, efficiently and safely.
- Understand the function of fire doors. Periodically make sure all of them operate properly. Make sure they have closed properly during the emergency.

The Electrician may be essential to larger companies. The Electrician must:

- Know the location of all switches, portable generators, extension cords and emergency power equipment in the assigned area.
- Be thoroughly trained on the potential electrical hazards during a fire or other emergency.
- Be accountable for shutting down electrical fans or handling ventilating equipment according to a prearranged plan. Shutting off the HVAC is important for eliminating a fresh supply of air to the fire and preventing smoke, soot and heat from spreading throughout the property.
- Be able to set up temporary power or lighting if utility power is lost.
- Be able to cut off power, in event of a flood to basements, ground floors or below grade areas.

Prefire Planning. One of the most important parts of developing a response plan is your prefire plan with the public fire service. Good prefire planning involves conducting a site visit with the fire service on your property so that if an emergency strikes, your personnel and firefighters will act as a team. Firefighters need to be familiar with the layout and hazards of your facility. It's important for everyone involved to know exactly who does what, where and when.

Throughout the site visit, you will need a site plan showing the layout of the property and a checklist of items involving the level of response both your staff and firefighters will need. A certain amount of coordinated training might be involved.

4. **Step Four Train your personnel**

   Educate personnel for each level of response you need for the firefighting team. It's important to establish drills with the onsite team and coordinate them with the public fire service and other outside agencies.

5. **Step Five Do the audits**

Changes will occur and, as they do, they need to be well managed. Audits of your equipment, storage and property help determine past and evolving changes and future plans. It's important to do at least two things:

- Plan audit intervals. They should be done at least once a year.
- Develop a process to assure that changes in construction, occupancy, protection and exposures will be accounted for. Make sure they are communicated to the person in charge of the Emergency Response team.

2.3.2 TECHNOLOGIES FOR EVACUATION SYSTEM IN ELASSTIC.

In the course of crowd management, the responsible staff makes use of different equipment when managing crowds, in ELASSTIC we have:
BIM

- Wireless sensor networks
- Sensors for monitoring building infrastructures
- Sensors for occupancy detection
- Evacuation system

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.

2.4 ELASSTIC 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.[8] 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).[9]

2.4.1 ELASSTIC 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.

8 J. R. Silvers, "Risk Management for Meetings and Events," Events Management Series, Elsevier 2008, p. 56

9 Ibid, p. 59 and 62-63.

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.[10]

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.[11]

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 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).[12] 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.[13]

2.4.2 ELASSTIC 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.”[14]

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

10 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

11 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

12 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

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

14 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

negotiating parties suffers damages in the negotiations phase due to a wrongful act of another negotiating party.[15]

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 spectators at a stadium); the said duty of care must be breached which means the responsible person must have failed to fulfil 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.[16] 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, building managers 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.[17] 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.[18]

However, also member of the crowds themselves could be held liable for negligent or provocative behaviour. 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."[19] The disorderly behaviour of an individual in public is also criminalized.[20]

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.[21]

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.

---

15 Ibid, p. 50

16 J. Dumortier et al, "D.7.1 Legal Requirements for Trust in the IoT," uTRUSTit – Usable Trust in the Internet of Things, p. 51

17 J. R. Silvers, "Risk Management for Meetings and Events," Events Management Series, Elsevier 2008, p. 56-57

18 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

19 Part I, Article 2 of the UK Public Order Act 1986

20 Part I, Article 5 (1) of the UK Public Order Act 1986

21 http://www.liverpoolecho.co.uk/news/liverpool-news/merseyside-police-officer-who-investigated-3424138

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 between the parties or a special relationship (e.g. parents – children).[22] 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.[23]

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.[24] 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.[25] Moreover, again in France, the rescuer might claim damages from the party he rescued which he sustained in the course of the rescue.[26]

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 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.

2.4.3 ELASSTIC 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.

22 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

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

24 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

25 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

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

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.[27]

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."[28] The Council Directive was amended by Directive 1999/34/EEC. Pursuant to the amending Directive product is defined as "all movables even if incorporated into another movable or into an immovable. "Product" includes 'electricity.'" 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." The Directive also sets up a regime of joint and severable liability.

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. 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 and used by the injured party for personal use and [29] has lower value than 500 €. A product is defective when it "does not provide the safety which a person is entitled to expect, taking all circumstances into account." These circumstances include, inter alia, the presentation of the product, the use to which the product would be reasonably expected to be put, as well as the time of the launching of the product.However, the Directive explicitly excludes the subsequent circulation of a better product as a criterion to determine defectiveness. 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.

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

If a product is developed within the framework of ELASSTIC 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. 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.

[27] Ibid, p. 51-52

[28] 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

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

2.4.4 REDUCING LIABILITY AND EXEMPTIONS FROM LIABILITY

In principle to reduce liability, an entity needs insurance.[30] In the case of passenger ships insurance of at least 250.000 units of account per passenger on each distinct occasion is compulsory.[31] 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.[32]
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, 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. 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. 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.
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. 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.
Further limitations of liability could result also from the negligent or faulty behavior of members of the crowd. Building managers 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.[33]

2.4.5 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.[34]
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

---

30

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

31 Article 4bis 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.

32 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

33 Article 6 of Athens Convention

34 Article 21 Charter of Fundamental Rights of the European Union

disabilities. In principle, the rights of the disabled are also protected by way of respect for human dignity.[35]

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. 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.[36] In some instances people might not be able to escape without the help of an assistant or caretaker. This might slow down 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 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.[37]

Therefore, when planning emergency response, one must consider the needs of the people with different disabilities and how their needs could be met in order to provide effective response.Trained staff is essential for a successful evacuation of people with disabilities.[38]

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 [39] 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.[40]

---

[35] 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

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

[37] Ibid, p. 37-39

98S. 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

[38] Ibid, p. 93

[39] 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

[40] 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

[40] Ibid, p. 93

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 departure of the ship.[41] As concerns airports, passengers with reduced mobility (PRM) are to be provided with assistance by the air company.[42] 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.[43]
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.[44] Therefore in crowd evacuation scenarios care and adequate assistance must be given to the needs of the children.

.

2.5 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.
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.

[41] 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

[42] 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

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

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

3 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.[45]

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 building of ELASSTIC 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." [46].

It might also lead in effect to increased tracking, monitoring and profiling. [47] 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 discrepancy between the suggested pre-defined scenarios and the actual situation and facts. [48]

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.

---

[45] 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

[46] .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.

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

[48] 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

3.1 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." 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. [49] Moreover, it extends further than private life, i.e. it covers different freedoms which protect one's privacy in public places. [50] 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 [51].

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 which have passed the privacy test. [52] 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. [53]

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.

3.2 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);

---

[49] 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

[50] 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

[51] 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.

[52] 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.

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

[53] 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.

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.[54]

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). [55] 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-determined'." [56] It thus grants the individuals the power to take decisions concerning the collection, disclosure and use of their personal data. [57] 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. [58]

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, [59] surveillance, interception of communications, [60] 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).[61]

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 must 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. be

---

[54] 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

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

[56] 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

[57] A. Rouvroy and Y. Poullet (2009), p. 56.

[58] Ibid, p. 57

[59] S. and Marper v UK, ECtHR

[60] Kruslin v France, ECtHR

[61] 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

accessible and foreseeable to the persons concerned and the manner and scope and purpose of the data processing activities must be sufficiently precise. [62]

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.'" [63]

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. [64] Thus, a new technology should be efficient and effective in meeting the declared aim.[65]

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.

3.3 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 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

[62] Kruslin v France, ECtHR, 11801/85, 24 April 1990, Series A no.176-A, par. 27 and 30

[63] S. and Marper v UK, ECtHR, par. 101

[64] F. Coudert (2009), p. 150

[65] P. de Hert and D. Wright (eds), "Privacy Impact Assessment," Springer 2012, p. 63

the EU and thus bring about harmonization of the data protection provisions.[66] Relevant aspects of the proposed regulation will be examined.

3.3.1 DEFENITIONS / 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." [67] The purpose of the Directive is to serve as a protection of natural persons and therefore, the scope of the definition is interpreted broadly.[68] Thus, the definition refers to any data that could lead to the identification of the natural person/data subject, whether directly or indirectly.[69]

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 must comply with the Data Protection Directive.[70]

As concerns data rendered anonymous, by definition they do not fall under the Directive as long as "the data subject is no longer identifiable." [71] 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.[72] 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.[73]

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

[66] 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

[67] Article 2 (a) Directive 95/46/EC

[68] 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

[69] Article 2 (a) Directive 95/46/EC

[70] Article 29 Data Protection Working Party, "Opinion 5/2009 on online social networking," 12 June 2009, p. 5

[71] Recital 26 Directive 95/46/EC

[72] Article 29 WP, Opinion 4/2007, p. 16 and 21

[73] Article 29 WP, Opinion 4/2007, p. 14

the means and purposes of the data processing activity. [74] The controller, before commencing a personal data processing activity, is obliged to notify the data processing operation to the data protection authority [75] and ensure that all the data protection principles are complied with. [76] 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). [77]

For ELASSTIC 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 ELASSTIC 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. [78]

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. [79] 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. [80]

3.3.2 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.[81] In particular, when sound and image data (e.g. video surveillance) is processed for the above mentioned purposes, the Directive is not applicable. [82] 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.[83] 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. [84] In other Member States, e.g. Germany, if a public authority wants to install CCTV cameras, the regional

[74] Article 2 (d) Directive 95/46/EC

[75] Article 18 (1) Directive 95/46/EC

[76] Article 6 (2) Directive 95/46/EC

[77] Rouvroy, p. 18

[78] Article 2 (e) Directive 95/46/EC

[79] Article 2 (f) Directive 95/46/EC

[80] Article 2 (g) Directive 95/46/EC

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

[82] Recital 16 Directive 95/46/EC

[83] Article 29 Working Party, Opinion 4/2007, p. 24

[84] Article 3 (2) (c) Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data

police law would apply, which means that there are 16 different legal regimes. [85] 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.[86]

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, [87] in the Council of Europe Convention 108/81148 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. [88]

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." [89] 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. [90]

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 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. [91]

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.

---

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

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

[87] 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

[88] 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

[89] Recital 59 COM (2012) 11 final

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

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

3.3.3 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.[92]

In the framework of ELASSTIC 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.[93] In any case, any personal data processing operation in ELASSTIC 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.[94] 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 pregnant woman in order to save his/her life (e.g. metro

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

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

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

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. [95]

3.3.4 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." [96] Thus, the principle is composed of two elements - purpose specification and compatible use. [97] 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." [98] Purpose specification is a pre-requisite for assessing the application of the other data qualit]y requirements, such as the proportionality principle, accuracy, data minimization, retention periods, etc. [99]
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. [100] 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 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.[101]
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

[95] 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

[96] Article 6 (1) (b) Directive 95/46/EC

[97] Article 29 Data Protection Working Party, "Opinion 03/2013 on purpose limitation," 2 April 2013, p. 3

[98] 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

[99] WP 29, Opinion 3/2013, p. 4

[100] F. Coudert (2009), p. 149

[101] Bundesverfassungsgericht judgment, 1 BvG 1215/07, 24.04.2013

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. fulfil 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." [102] 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.[103] 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.[104] 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.

Last but not least, any data processing activity must be fair and lawful, 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. 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.

3.3.5 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,[105] 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;[106] the right to object to the processing of data relating to him/her;[107] and the right to judicial remedy in cases of breach.[108] Therefore, each controller involved in the processing of personal data in ELASSTIC (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.

[102] Article 6 (1) (c) Directive 95/46/EC

[103] Article 6 (1) (d) Directive 95/46/EC

[104] Article 6 (1) (e) Directive 95/46/EC

[105] Article 10 and 11 Directive 95/46/EC

[106] Article 12 Directive 95/46/EC

[107] Article 14 Directive 95/46/EC

[108] Article 22 Directive 95/46/EC

3.3.6 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.."[109] Member States shall allow a person to be subjected to such a decision if the decision is authorized by law and provides adequate safeguards. [110]

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 changed to profiling. [111] 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" [112] 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. [113] However, the processing under Article 20 may not be based solely on special categories of data.[114] In any case, if profiling takes place, the data subject should be informed of its existence and its envisaged effects. [115]

It is argued that for purposes of preventing crowd disasters, applications such as video surveillance technologie 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" [116] 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. [117]

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." 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:

[109] Article 15 Directive 95/46/EC

[110] Article 15 (2) (b) Directive 95/46/EC

[111] Article 20 (1) Measures based on profiling, COM (2012) 11 final

[112] Article 20 (2) (b) COM (2012) 11 final

[113] Article 20 (2) (c) COM (2012) 11 final

[114] Article 20 (3) COM (2012) 11 final

[115] Article 20 (4) COM (2012) 11 final

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

[117] Ibid, p. 379

"the most critical implications of next-generation biometrics are that future biometric recognition could take place remotely, covertly and/or from a distance and may produce material with a high degree of sensitive (and surplus) information."[118]
This richness of the extracted information or features allows one to engage in pattern recognition activities.[119] 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.[120]
Sometimes the criteria for defining abnormal behavior might be per se discriminatory.[121] 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.[122]
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. The WP 29 Working Party refers to it as a "dynamic-preventive surveillance." [123] 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.[124]
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.'" [125] This problem becomes even more pertinent if alerts are stored and interlinked with each other, in particular if they concern the same individual who is present on the premises under surveillance regularly.

3.3.7 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.[126] 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

[118] 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

[119] A. Yannopoulos, p. 89

[120] Finn, "Seven Types of Privacy," p. 24

[121] G. Buttarelli, p. 9

[122] A. Yannopoulos, p. 102

[123] WP 29 (2004), p. 4

[124] F. Coudert 2010, p. 377 and 379

[125] G. Buttarelli, p. 9; also WP 29 (2004), p. 6 and Article 2 Additional Protocol No 4 European Convention on Human Rights

[126] Article 16 Directive 95/46/EC and Article 27 COM (2012) 11 final

disclosure or access. These measures are applicable both to the controller and the processor if there is one.[127] 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.[128]

3.3.8 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.[129] Further, the controller has to ensure that the data subjects can exercise their rights,[130] that the principles of confidentiality and security of processing are complied with,[131] as well as that the supervisory authority is notified of the data processing activity.[132] The designation of responsibilities is essential since pursuant to Directive 95/46/EC in the case of breach of the responsibilities of the controller(s) and where applicable the processor(s) these can be held liable severally or jointly.[133]

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.[134] 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.[135]

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."[136] In cases of infringement, the Member States may impose sanction in order to ensure the full implementation of the Directive.[137] Pursuant to the Proposal for a General Data Protection Regulation, the supervisory authority would be entitled to impose fines for personal data processing breaches.[138]

---

[127] Article 17 Directive 95/46/EC

[128] Judgment of the German Constitutional Court, BvG 370/07

[129] Article 6 (2) Directive 95/46/EC

[130] Article 10, 11, 12 and 14 Directive 95/46/EC

[131] Article 16 and 17 Directive 95/46/EC

[132] Article 18 Directive 95/46/EC

[133] Article 23 Directive 95/46/EC ; Article 77 (1) and (2) COM (2012) 11 final

[134] 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.

[135] Article 23 (2) Directive 95/46/EC; Article 77 (3) COM (2012) 11 final

[136] Article 22 Directive 95/46/EC

[137] Article 24 Directive 95/46/EC

[138] Article 79 COM (2012) 11 final

3.4 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.[139] 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 will be discussed in the following two sections. It would also introduce the obligation to conduct Privacy Impact Assessments.

3.4.1 ACCOUNTABILITY

Accountability has developed as one of the general principles in a number of data protection frameworks,[140] 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.[141]

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."[142] Thus, ideally, the controller would minimize the risks associated with personal data processing and have a better reputation.[143]

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.[144]

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

---

[139] 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

[140] 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;

[141] Article 22, COM (2012) 11 final

[142] Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010, executive summary;

[143] Ibid, p. 5

[144] 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

throughout the whole processing activity, thus implying that accountability should be "an ongoing activity."[145] 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 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.[146]
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. [147] 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.[148]
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.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.[149] Last but not least, the principle of accountability should be applicable to both public and private controllers and should be scalable. [150]

3.4.2 PRIVACY BY DESIGN

The proposed Regulation has formally incorporated in the European Union data protection framework the principle of privacy by design. [151] Pursuant to that principle, technological data protection and privacy safeguards should be embedded into the design and operation of information and communication technologies (ICT). [152] 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

[145] P. Hustinx, "Accountability in the Proposed Regulation," Brussels, 3 December 2012

[146] J. Alhadeff et al, p. 4 and 15; Article 22 (2) COM (2012) 11 final

[147] 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

[148] Article 29 Working Party, Opinion 3/2010, p. 7 and 16, J. Alhadeff, p. 22

[149] Article 29 Working Party, Opinion 3/2010, p. 6

[150] Article 29 Working Party, Opinion 3/2010, P. 19

[151] Article 23, COM (2012) 11 final

[152] 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

number of individuals. [153] According to the wording of Article 23 of the Proposed Regulation, the implementation of privacy by design in technologies will become mandatory. [154]
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. [155] The latter refers to privacy features which are activated automatically.[156] The responsibility for protection personal data, in addition to the role of the controller, thus applies also to producers of technology [157] and to the processors of personal data. [158]
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 concerns physical design, the physical infrastructure where data are stored and processed must be secure. [159]
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.[160]The Article 29 WP refers also the principles of data confidentiality, data quality and use limitation.[161]
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).[162] PETs refer to technologies which minimize personal data use, maximize data security and empower individual users. [163] The importance of security has been confirmed by the German Constitutional Court, which established the principle of confidentiality and integrity of information

[153] 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

[154] Article 23 COM (2012) 11 final

[155] 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

[156] 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

[157] 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

[158] EDPS Opinion, 7 March 2012, p. 29, where the EDPS calls on the Commission to explicitly add the role of processors

[159] http://privacybydesign.ca/about/trilogy/

[160] http://www.ipc.on.ca/site_documents/pbd-resolution.pdf; http://privacybydesign.ca/about/principles/

[161] Article 29 Working Party, p. 14/15

[162] EDPS Comments, 10 October 2012

[163] Cavoukian A., "Privacy By Design," http://www.ipc.on.ca/images/Resources/privacybydesign.pdf, p. 3; Als o, in its Judgement 1BvG 370/07, the German Constitutional Court established the principle of confidentiality and integrity of IT systems, p. 3

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. [164] With regards to BATs, the EDPS recommends that entities use the most updated technology which implements the highest degree of data protection settings. [165]

Thus, the ELASSTIC 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.

3.4.3 DATA PROTECTION IMPACT ASSESSMENT

Pursuant to Article 33 of the proposed regulation the ELASSTIC building managers 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." [166] 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.[167] In principle the ELASSTIC 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. [168]

3.4.3.1 *RFID PRIVACY AND DATA PROTECTION IMPACT ASSESSMENT (PDPIA) IN ELASSTIC*

Even though the Proposed Regulation has not passed, pursuant to a Commission recommendation ELASSTIC should develop a framework for privacy and data protection impact assessment for RFID tags, which was endorsed by the Article 29 Working Party.[169]

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.

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. 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 basis for dialogue with the competent

[164] 1BvG3 70/07, also par. 180

[165] EDPS Comments, 10 October 2012

[166] Article 33 (1) COM (2012) 11 final

[167] Article 33 (2) (a) to (e) COM (2012) 11 final

[168] Article 33 (3) and (4) COM (2012) 11 final

[169] 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

authorities (local, national and regional) . One of the essential components of the PDPIA is to identify and assess the risks that a certain RFID application could cause. Thus, the ELASSTIC PDPIA should based on a “privacy and data protection risk management approach.”
In addition, the use of RFID applications should be transparent and thus RFID ELASSTIC 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.
The ELASSTIC PDPIA should be characterized as a process, which should ideally begin at the earliest possible stage so that the outcome of the application could be influenced. Pursuant to the framework developed for PDPIA by ELASSTIC and endorsed by Article 29 Working Party, the process should have two phases. During the initial phase, the ELASSTIC 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.
ELASSTIC PDPIA for RFID application should be conducted after ELASSTIC operator/controller has defined the RFID application and specified the categories and sensitivity of the data as well as the personal data processing activity. According to EU recomendations, there would be potentially 7 categories of information in the RFID – whether data are for individuals with a disability, pregnant women, etc. The 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 ELASSTIC cannot be completed yet.

3.4.3.2 *ELASSTIC ELEMENTS OF A PDPIA FOR RFID*

As mentioned above, the ELASSTICPDPIA 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.

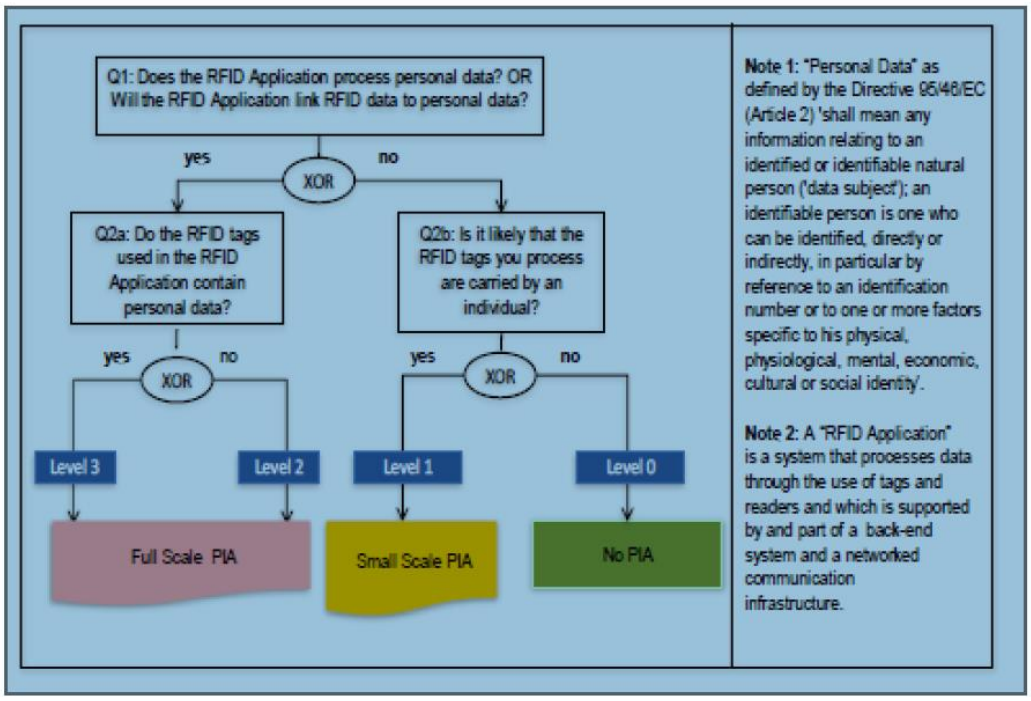

Figure 1 A Decision Tree format in view of determining whether a full-scale or a small-scale PDPIA is necessary

According to the initial information on the RFID application in ELASSTIC, 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 will be classified as special categories of data or sensitive data under Article 8 (1) of Directive 95/46/EC, as this 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. The potential legal basis for processing of this information could be consent and/or legitimate interests of the data subject. If other personal data is processed, e.g. a unique number, this would also qualify as personal data and thus a relevant ground for processing it must exist (i.e. in Article 7 Directive 95/46/EC).

The ELASSTIC PDPIA will 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 ELASSTIC 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.

During the risk assessment phase the ELASSTIC 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. 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.

When carrying out ELASSTIC 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. The ELASSTIC PDPIA Framework operators will describe the process visually in the following way.

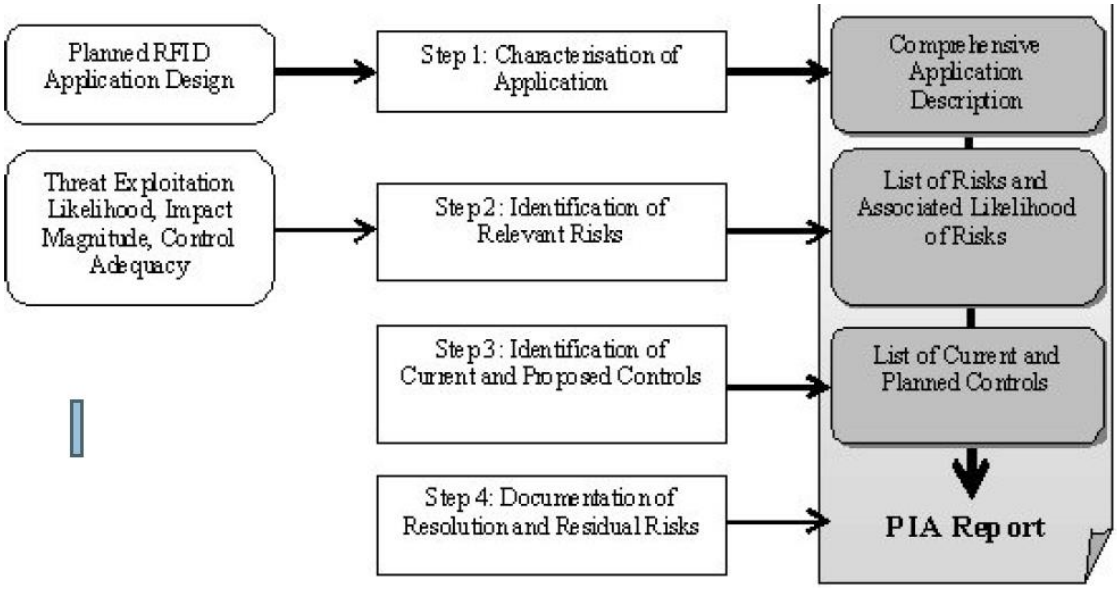

Figure 2 Steps that should be followed by the operator of an RFID application

As is shown above, the steps that the ELASSTIC operator of ELASSTIC RFID application will take be the following: detailed description of the application, 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 ELASSTIC 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 As is shown above, the steps that the operator of an RFID application should take are the following: detailed description of the application, 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.

Once the PDPIA is completed by the ELASSTIC 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. In addition, the ELASSTIC 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 ELASSTIC PDPIA. It is recommendable that in the process of conducting a PIA the stakeholders (first responders, police, etc) are consulted.

Last but not least, ELASSTIC 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.

3.5 E-PRIVACY DIRECTIVE: PUBLIC COMMUNICATIONS NETWORKS IN ELASSTIC

In the course of managing crowds it is essential that the responsible private and public actors have reliable channels of communication with each other.
Where applicable, ELASSTIC should observe the national legislation which might apply to emergency communications where will be installed. Although different national laws apply, some general provisions stemming from EU level legislation will 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. 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.

3.5.1 SMARTPHONE APPLICATION

At medium/long term one of the ELASSTIC possible means of 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 will apply.
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.”
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. 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. 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.

3.5.2 LIABILITY OF ELASSTIC SMARTPHONE APPLICATION

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.

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

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.

Second, the exemption applies if the ELASSTIC smartphone application 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 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.

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. In the case of hosting, Member States may establish procedures for the removal or disabling of access to information.

4 Conclusions

The aim of the present deliverable was to outline the high-level legal and ethical framework applicable to the ELASSTIC project. 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 ELASSTIC 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. ELASSTIC operational phase
Safety and security measures
The ELASSTIC operators and public authorities, 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.

- 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
  - Every personal data processing operation (video surveillance, RFID, smartphone applications) must have a clearly designated controller. In the framework of ELASSTIC, 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.
  - 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.
  - When CCTV monitoring is used, the national legislations on CCTV must be observed (installation of cameras, retention period, etc).
  - The ELASSTIC 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.
  - Before personal data processing operations commence, the ELASSTIC 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.

- The ELASSTIC controller must guarantee the rights of data subjects (information, objection to processing, right to access, rectification, erasure or blocking).
- The ELASSTIC controller must carry out a Privacy and Data Protection Impact Assessment of the RFID and submit it to the supervisory authority at least 6 weeks before the application becomes operational.
- The partners of ELASSTIC should implement the principle of Privacy by Design in the ELASSTIC product.

2. ELASSTIC research phase

The partners of the ELASSTIC project have to follow the five steps outlined in section 2.3 in subsection fire building scenario in order to comply with their data protection obligations.

5 Reference

Title	Author	Version	Date
Effective crowd management	NRF	4	2014
Mass. Crowd Manager Regulations and Training Program	Public safety	2	2011
Fire scenarios	Marc Casellnou	1	2015
High level ethical and legal framework, formulating ethical and legal requirements for evacuate	Diana Dimitrova (ICRI/KUL), Bjorn Coene (ICRI/KUL)	0.2	2013
Emergency Planning's Five Key Steps	Michael Morganti	1	2013

6 Acknowledgment

"This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312632".

http://cordis.europa.eu/fp7/cooperation/home_en.html

http://ec.europa.eu

PROJECT PARTICIPANTS:
TNO – NEDERLANDSE ORGANISATIE VOOR TOEGEPAST NATUURWETENSCHAPPELIJK ONDERZOEK (NL)
ARCADIS NEDERLAND BV (NL)
FRAUNHOFER-INSTITUT EMI (DE)
INSTITUTO CONSULTIVO PARA EL DESARROLLO SL (ES)
JA JOUBERT ARCHITECTURE (NL)
NORTH BY NORTH WEST ARCHITECTES SARL (FR)
SCHÜBLER-PLAN INGENIEURGESELLSCHAFT MBH (DE)
SIEMENS AG (DE)
UNIRESEARCH BV (NL)