EVAGUIDE

Horizon 2020 Programme

Security Management Platform for enhanced situation awareness and real-time adaptive evacuation strategies for large venues for sports and entertainment

ETHICAL, LEGAL, REGULATORY AND SOCIETAL COMPLIANCE FRAMEWORK REPORT – INTERIM VERSION

Deliverable Identifier:	D2.3
Delivery Date:	September 30, 2019
Dissemination Level:	PU
Author(s):	TELESTO
Document version:	1.0
Contract Start Date:	December 1st, 2018
Duration:	24 months
Project coordinator:	TELESTO Technologies (GR)
Partners:	TEL (GR), EXUS (GR), CDI (GB), ESSMA (BE)
Contact Person EC:	Vincenzina VINCI

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under grant agreement no 831154.

Document Control Page

Title	Ethical, Legal, Regulatory and Societal Compliance Framework Report – Interim Version	
Editors	**Name**	**Partner**
	Lilian Mitrou	TEL
	Dimitris Drakoulis	TEL
	Dimitris Dres	TEL
Contributors	Nikos Siapkaras	TEL
	Marios Drakoulis	TEL
	Konstantinos Alexopoulos	TEL
	George Pelekanos	TEL
Peer Reviewers	**Name**	**Partner**
	Spyros Evangelatos	EXUS
	Cyril De Greve	ESSMA
Format	Text - Ms Word	
Language	en-UK	
Work-Package	WP2	
Deliverable number	D2.3	
Due Date of Delivery	30/09/2019	
Actual Date of Delivery	30/09/2019	
Dissemination Level	PU	
Rights	EVAGUIDE Consortium	
Date	30/09/2019	
Revision	30/09/2019	
Version	1.0	
Status	☒ draft ☒ Consortium reviewed ☒ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Edited By	Date	Description
0.1	TEL	27/2/2019	Initial draft
0.2	TEL	13/3/2019	Templating, introductory section
0.3	TEL	16/4/2019	Addition of chapter 2 about the balance between the rights and interests/ the protection of privacy and security
0.4	TEL	29/5/2019	Description of the data protection EU legal framework
0.5	TEL	24/7/2019	Addition of principles of data processing
0.6	TEL	12/9/2019	Addition of tools to comply with the legal framework
0.7	TEL	24/9/2019	Submission for review to the consortium
0.8	ALL	26/9/2019	Additions, corrections to the final draft
0.9	TEL	27/9/2019	Comments addressed
1.0	TEL	30/9/2019	Coordinator check and submission

Abbreviations

AI	Artificial Intelligence
CFREU	Charter of Fundamental Rights of the European Union
CFR	Charter of Fundamental Rights
CCTV	Closed-Circuit TeleVision
CJEU	Count of Justice of the European Union
CoE	Council of Europe
DPA	Data Protection Authorities
DPO	Data Protection Officer
DPWP	Data Protection Working Party
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ECJ	European Court of Justice
ENISA	EU Agency for Network and Information Security
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
LIA	Legitimate Interests Assessment
PNR	Passenger Name Record
RSS	Received Signal Strength
TFEU	Treaty on the Functioning of the European Union

TABLE OF CONTENTS

Executive Summary

EVAGUIDE aims to address the needs of the safety of large facility visitors during complex evacuation processes. In order to accomplish this scope and provide the foreseen services, EVAGUIDE platform needs to have access to personal data of the users (spectators/visitors) involved (e.g. location based information) asit is difficult to provide personalized evacuation guidance in case of an emergency, if there is no information available about the status of the users, their location etc.

Therefore, in order to advance the situational awareness and increase the safety standards, it is important to collect and process personal data in compliance with the relevant regulatory framework..

The purpose of this analyses (1st iteration) is to examine the legal, ethical, regulatory and societal issues associated with the use of the EVAGUIDE system and its capablity to collect, store, analyse and process personal data. In more details, a description of individual's rights and how may be tampered by new innovative solutions is presented, in line with the new legal framework (GDPR) that defines the obligations and rules on handling personal data and the available tools to comply with the new legal environment in the EU.

1. INTRODUCTION

1.1 Purpose of the deliverable

The use of new technologies, such as smart sensor environment, mobile apps, crowd management etc intends to ensure and improve the efficiency, speed and outreach of communication between the safety personnel and provide better situational awareness during emergencies or disasters.[1] On the other side such innovative solutions carry inherent privacy and data protection risks as they collect large amounts of personal data.

The aim of this deliverable is to identify the ethical and legal issues that are posed with regard to EVAGUIDE system and the applications used to meet the objectives of the project. The identification of these issues is necessary to develop a system that takes into account the ethical and legal principles and thus is socially acceptable. Moreover the early identification of these issues is important not only to ensure compliance with the applicable law but also to design the system while taking into consideration the legal requirements set mainly by the data protection legislation. The EVAGUIDE solution is designed to collect and process personal data. In the course of research, development and deployment activities, the project partners have to embed the legal obligations from the outset into the design of technical solutions and products.

Compliance with the law applicable in EU and Member States is also a precondition for such systems to be deployable. The legal perspective provides a relevant set of requirements considering that decision makers (research partners and end-users) need to comply with existing laws, which are ultimately closely related to the fundamental values and rights.

The deliverable is focused on European legislation, which comprise the EU legal framework and the Council of Europe conventional provisions and recommendations. The aim of the present deliverable was to outline the high-level legal framework applicable to the EVAGUIDE project, both in its research phase and its validation phase. The lawfulness of data processing applications/ operations in the context of EVAGUIDE is considered both under the aspect of EVAGUIDE as research project and in the light of consideration, that the outcome of this research has to be compliant with the legislative framework to be socially acceptable and deployable.

The deliverable also focuses on the aspects of the responsibilities of the different actors (researchers, end-users) who are engaged in the crowd and crisis management. *It provides a preliminary discussion of whether the proposed applications strike a fair balance between the needs of the evacuation management, the privacy and data protection rights of individuals and the respective legal requirements.*

1.2 Structure of the Deliverable

The deliverable consists of the following sections:

[1] See L. Jasmontaite and D. Dimitrova, Online Disaster Management: Applicability of the European Data Protection Framework and Its Key Principles, Journal of Contingencies and Crisis Management Volume 25 Number 1 March 2017

- Section 2 – Definition and analysis of the fundamental rights of individuals, and the risks of interference posed by new technologies (e.g. video surveillance, smartphone apps etc) and the balance towards the protection of privacy and security.
- Section 3 – General description of the data protection legal framework (GDPR) that defines the rules on how to handle personal data
- Section 4 – Detailed reference to the tools/ elements that can be used by organizations/ authorities for better monitoring and ensuring compliance with the GDPR.
- Secction 5 – Summary of the deliverable's results

2. CONFLICTS AND BALANCES BETWEEN RIGHTS AND INTERESTS

2.1. Obligations to ensure safety and the right to life (and safety?)

Football matches usually entail relatively large crowds,. Ensuring the safety of persons who attend events such as a football game constitutes an obligation of both private and public actors involved. Private actors, such as a team/ stadium owner of games organizers, have to ensure safety both on a legal and on a contractual basis. At the same time public authorities, such as police authorities, are obliged to take all necessary and adequate measures to prevent threats and mitigate risks especially with regard to crowd assemblies taking place in public and/ or publicly accessible facilities.

These obligations have both a preventive and a re-active character. They refer to the adoption of measures to prevent disasters with impact on the people attending a public event and to manage crisis such as crowd disasters caused by security threats (such as bomb attacks or fire), natural (e.g. earthquakes) or manmade disasters (e.g. terrorist attacks) or unruly/ unlawful behaviour (actions of hooligans). The obligation to (re)act includes also the post-crisis stage.

Especially in cases of crowd disasters, crowd management is intended to safeguard the life of individuals under risk. In this context ensuring the safety of the crowd and concretely speaking of each person which forms part of the crowd responds to the obligation to protect the (right to) life. The state authorities have both positive and negative obligations to protect inter alia the life of the individuals. These obligations derive from European Conven----tion on Human Rights (Article 2 ECHR), applicable to States that have ratified it as well the Charter of Fundamental Rights of the European Union (Article 2 CFREU). Similar provisions can be found in national constitutional provisions, for example in the German Federal Constitution[2].

The right to safety has to be conceived as a condition for ensuring the right to life and as a condition of dignity and freedom. The - relatively recent - “invention” of a “fundamental right to security”[3] has done nothing to resolve the problems of security. The existence of a “fundamental right to security” in a general sense, however, is negated by the argument that constitutional texts and jurisprudence recognize only a much narrower right to physical integrity of the person and provide for a number of possible grounds for legitimate restrictions on other fundamental rights. The concept of public safety as an obligation to protect rights is grounded on the positive obligation of the state and its agents to guarantee the rights of a person as an individual and member of society and ensure the unhindered and efficient exercise thereof. Regardless of its conception either as the result of the demand on the state to undertake positive actions to protect the rights of life, personality, property or as a public good, security constitutes a limitation of freedom and privacy that is not allowed to affect their core.

2.2 Interference with fundamental rights

The measures both to prevent disaster incidents and to ensure efficient and safe evacuation procedures in case a crowd disaster has occurred, may have implications for the individuals and interfere with their fundamental rights, mainly the right to privacy and communication secrecy and

[2] Articles 1, 2, and 14 Grundgesetz für die Bundesrepublik Deutschland of 23 May 1949 (BGBI. S.1),)
[3] Isensee, Das Grundrecht auf Sicherheit, Berlin 1983)

the right to data protection. This is especially the case when such measures involve location tracking, monitoring and surveillance through the use of smartphone applications or video surveillance apparatus etc. The risks for these rights escalate in case that the systems used contain or allow the integration, combination and fusion of information collected through different sources and in some cases for different purposes (e.g. profiling - the use of data to evaluate certain aspects related to the individual).

2.2.1.The right to privacy

The right to privacy is a fundamental right that is recognised in international, European and national laws. 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).

The notion of privacy could be defined as freedom of unwarranted and arbitrary interference from public authorities or private actors/bodies into activities that society recognizes as belonging to the realm of individual autonomy (private sphere)[4]. The European understanding of privacy as reflected in the regulatory framework is strongly influenced by the so-called dignity approach, which is strictly related to the moral autonomy of the persons. Dignity has become a universal, fundamental and inescapable term of reference even though it should always be seen against the specific cultural and historical background. The EU's Charter of Fundamental Rights, has brought about the constitutionalisation of the person starting from personal freedom and dignity. Dignity and inalienable rights residing with the individual are the hallmarks of the European regulatory approach. The European approach to privacy is largely grounded to the dignity of the person, who operates in self-determination as a member of a free society (German Federal Constitutional Court, Census case, 1983). Dignity as related to privacy is a concept summarizing principles such as protection of individual's personality, non commodification of the individual, noninterference with other's life choices, and the possibility to act autonomously and freely in society[5] .

At European level the legal *content* of privacy can be securely derived from the pertinent case law of the European Court of Human Rights in Strasbourg (ECtHR), in relation to right to private life (Art. 8 ECHR), to which the European Signatory Parties have to comply with taking all necessary and appropriate legal measures on national level. The Court did not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". It has rather opted for a case to case approach: so it covers the physical and psychological integrity of a person (X. and Y. v. the Netherlands) or it can sometimes embrace aspects of an individual's physical and social identity (Mikulic v. Croatia). Within the private life sphere fall also gender identification, name and sexual orientation. Privacy encompasses numerous dimensions, including, inter alia, privacy of the individual or bodily privacy, of personal behavior (e.g. political, religious and sexual activities or freedom from systematic monitoring).

[4] EU Network of Independent Experts on Fundamental Rights — CRF-DF, Commentary of the Charter of Fundamental Rights of the European Union, June 2006.

[5] De Hert, P. Balancing security and liberty within the European Human Rights Framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11, Utrecht Law Review, 1, 68, 2005.

Privacy in the European approach refers also to personal information and personal communication. With the development of new information and communication technologies we identify a new aspect of privacy, the so called informational privacy. The scope of the right to privacy has further expanded in tandem with technological advances to 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, while recently there is a tendence in theory to encompass also the so called group privacy (e.g. groupings or profiles over which we have no control).

2.2.2 Privacy in public and publicly available information

Measures of surveillance can constitute an interference with fundamental rights, such as the right to privacy, especially if such measures are of a secret or preventive nature[6]. The right to privacy protects private life even "in public" and – according to the jurisprudence of the Strasburger Court it covers also the processing of data relating to the private life of individuals, with a broad interpretation of private life. According to legal theory and jurisprudence people enjoy also 'privacy in public, i.e. they do not lose per se their right to privacy in public spaces. As emphasized by the Article 29 Data Protection Working Party (DPWP) (since 2018 the European Data Protection Board (EDPB[7])). a considerable portion of the information collected by means of video surveillance, concerns identified and/or identifiable persons, who have been filmed as they moved in public and/or publicly accessible premises. Such an individual in transit may well expect a lesser degree of privacy, but not expect to be deprived in full of his rights and freedoms as also related to his own private sphere and image[8].

Audio/image data are considered to be personal data, if they refer to identified or even identifiable persons. Both Data Protection Authorities and courts have accepted that the operation of CCTV or other monitoring systems in public places violates the right to personality of the citizens, because it 'puts them under control and unjustifiably restricts their freedom and hinders the free development of their participation in social and political activities'. In particular, it is accepted both by legal theory and jurisprudence that CCTV surveillance has the potential to discourage people from exercising their rights to freedom of expression and freedom of association in public places.

Consideration is also to be given here to the right to free movement of individuals who are lawfully within a State's territory, which is safeguarded by Article 2 of Additional Protocol No. 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Individuals have the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards to their movement and conduct, as well as without being the subject of detailed monitoring such as to allow tracking their movement[9].

---

[6] Kugelmann D. and Kosin C., Surveillance Powers of the Police and the Protection of Personal Data, in R. Alleweldt, G. Fickenscher (eds.), The Police and International Human Rights Law, Springer 2018, pp. 155 ff.

[7] The European Data Protection Board (EDPB) is an independent body with legal personality, responsible for ensuring the consistent application of the General Data Protection Regulation (GDPR). It is composed by representatives of the national Data Protection Authorities of the Member States. The EDPB succeeds the Article 29 Working party set up under Article 29 of Directive 95/46/EC.

[8] DPWP, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.

[9] DPWP, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance

Before 2000, it was relatively common to declare that the right to privacy (understood here as synonymous to the right to respect for private life) had evolved through the years, and had gradually come to include the protection of personal data, regarded as a sort of informational dimension of privacy, reflecting the approach of control on the (use of) personal information[10].

The formulation used by the Court in case Rotaru v. Romania that "public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities"[11] suggests that unsystematic processing of publicly available information does not necessarily fall within the scope of the protection of private life. As Koops notes the leading ECHR data-processing cases concern storage (with or without subsequent use) of data, leaving open the question whether the mere searching for and consultation of data, without storing or using them, constitutes an interference[12]. In both Peck and Friedl, as well as in Marper v UK, the ECtHR made it clear that much depends on the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained[13].

2.2.3 Right to data protection

Whenever information processing for security purposes is involved, it is necessary to take into account the right to data protection. This is a fundamental right enshrined in Article 8 of the EU Charter of Fundamental Rights, and differentiated from the right to respect for private and family life, home and correspondence enshrined in Article 7 of the same instrument, which guarantees the protection of an individual's private sphere against intrusion from others, mainly from the state.

Whereas Article 7 of the Charter echoed Article 8 of the ECHR by likewise establishing a right to respect for private life, the Charter's Article 8 enshrined a new right to personal data protection. Article 8 on 'Protection of personal data' provides, in its first paragraph, that 'everyone has the right to the protection of personal data concerning him or her'. Art. 8(2) Charter of Fundamental Rights (CFR) elevates a fair number of core data protection concepts into the EU fundamental rights (requirements for lawful data processing such as fairness, purpose specification, consent, etc.), as well as certain rights for the individuals concerned and independent supervision of "these rules". Art. 8(2) CFR provides that any processing of personal data must be legitimate on the basis of either the concerned individual's consent or law. Hence, the new right to data protection also protects against the processing of personal data where there is no legitimate basis. In the second paragraph, it provides also that "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified". In the third paragraph, it states that "compliance with these rules shall be subject to control by an independent authority".

[10] Fuster Gonzalez G and Gutwirth S., Opening up personal data protection: A conceptual controversy, Computer Law and Security Review 29 (2013), pp. 231 ff.

[11] ECtHR, Rotaru v. Romania, App.no. 28341/954 May 2000

[12] Koops, B.J. 'Police investigations in Internet open sources: Procedural-law issues', Computer Law& Security Review 29 (2013), p. 654-665

[13] Edwards L. and Lachlan Urquhart L. Privacy in public spaces: what expectations of privacy do we have in social media intelligence? International Journal of Law and Information Technology, 2016, 24, pp. 279–310, 301

Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) establishes the principle that "everyone has the right to the protection of personal data".[14] The Lisbon Treaty introduced a specific legal basis for the adoption of rules on the protection of personal data that also apply to judicial cooperation in criminal matters and police cooperation, requiring regulators to lay down rules relating to the protection of individuals with in these contexts.

Concerning the relation of privacy and data protection the Strasbourg Court has provided a very flexible jurisprudence, adapting the traditional private life rule to the challenges and risks of data processing. The court did effectively considered data protection cases through the prism of privacy (art. 8 ECHR) and it has developed criteria (nature of data, context and extent of processing, risks and harms for the individuals) to assess whether an issue of data protection touches or not upon the right to privacy. Not every processing of personal data, covered by data protection legislation, necessarily affects privacy. In the cases that the ECtHR has acknowledged that a data protection issue is also a privacy issue, it has granted some of the guarantees foreseen in data protection legislation, such as the right to access to personal files, claims regarding the deletion of personal data contained in public dossiers, the correction of data and it has endorsed the principle of purpose limitation, when it ruled that personal data cannot be used beyond normally foreseeable use, as well as the principle that governmental authorities may only collect relevant data based on concrete suspicions.

Data protection often refers to one specific form of privacy – informational privacy. Data protection is related to the rise and growth of computer-based information technology that enables collection, processing and storage of (huge amounts of) personal data, i.e. any information that refers to an identified or identifiable natural person. Data protection is a process that implicates legislation, technologies, organizations and individuals.

As concepts, privacy and data protection are related to one another. The concept of data protection was developed almost four decades ago in order to provide legal protection to individuals against the inappropriate use of information technology for processing information relating to them. It was designed to provide safeguards whenever information technology would be used for processing information relating to individuals.[15]

If privacy is a concept and a right, then data protection is not only a separate right, but in-a-way also a legal process by which the right to informational privacy is upheld.
Data protection, on the other hand is procedural and legalistic in nature as it refers to policy, legal and administrative aspects of personal data processing.[16] The European Court of Human Rights (ECtHR) considers the mere storing of personal information as an interference with the right of privacy,

[14] Article 16 states "e*veryone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities*".

[15] Hustinx P. "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation", 2013

[16] See PACT Project, Discussion Paper about the Theoretical Foundations of PACT. Research Paper 2, 2012, p. 4ff.

whether or not the state subsequently uses the data against the individual (European Court of Human Rights, Amann v. Switzerland[17]).

2.2.4 Communications' secrecy and freedom

Privacy and freedom of communication are strictly interrelated, at least in the European approach. The European Convention on Human Rights (ECHR), guarantees everyone's "right to respect for his private and family life, his home and his correspondence" (Art. 8). The Charter adopts in Art. 7 the same wording with the exception of the term "correspondence," which is replaced by "communications," in order to "take account of developments in technology"[18]. In recent years the prevalence of the expression "telecommunications" has been steadily replaced by the term "(electronic) communications," which, in the wording of the relevant European Union regulatory framework, refers to the "conveyance of signals on electronic communications networks" (Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services). The use of this expression makes it clear that the form and the content of any communicative exchange is as central to [tele] communications as the technological system in place to enable it. An exchange of signals or data between technological devices includes or generates mechanisms to monitor and store the information being exchanged. The digitalization of data and communication structures makes it possible to scrutinize and manipulate previously unimaginable amounts of information.

Communicating with others and using communication services falls within the protected zone of (communicational) privacy. Governmental regulations that chill communication or inhibit the use of communications services amount to an interference with an individual's right to respect for their private life[19]. As asserted by the European Court of Human Rights in the case Malone vs. United Kingdom, data related to the source, the destination, and in general to the conditions of communication are an "integral element of the communications made." The court has accepted (Copland vs. UK) that information derived from the monitoring of internet use should be similarly protected under Art. 8 of the ECHR.[20] The relevant European statutes, which regulate the use of such transactions, cover traffic data either "in a technology neutral way," (i.e. the e-Privacy Directive, which addresses traditional circuit-switched telephony, as well as packet-switched internet transmission) or in a functional way (i.e. the Data Retention Directive, which dealt with any data necessary to identify the subscriber or user, as well as the source and the destination of a communication). The informative value and the usability of traffic data is extremely high, as they can be analyzed automatically, combined with other data, searched for specific patterns, and sorted according to various criteria[21].

[17] European Court of Human Rights CASE OF AMANN v. SWITZERLAND(Application no. 27798/95) JUDGMENTSTRASBOURG16 February 2000

[18] EU Charter, Art. 7 Explanatory Notes.

[19]Data Protection Working Party. 2005. Opinion 113/2005 on the proposal for a Directive on the retention of data processed in connection with the provision of public electronic communication services. Available at http://ec.europa.eu..

[20] Mitrou L. The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive, in Haggerty D. and Samatas M., Surveillance and Democracy, 2010, pp. 127ff

[21] Breyer P., Telecommunications data retention and human rights: The compatibility of blanket traffic data retention with the ECHR." European Law Journal 11 (3):365–75.

The claim to anonymity, inherent in the right to privacy, is essential to freedom of communication via electronic networks, but, at the same time, it runs against public policy objectives. Privacy also comprises one's ability to remain anonymous in certain contexts, such as the use of technology without revealing one's name[22]. Anonymity, in the context of this discussion, should not only shield individuals while speaking or reading, but also when physically or electronically roaming about, interacting, and transacting through networks[23]. As electronic communications leave "digital traces," communications surveillance also has a disturbing effect on the right to anonymity[24].

Surveillance potential expands exponentially through data collection, storage and mining as communication technologies become more interconnected and are used more extensively and intensively. The convergence of communications and information technologies over the past few decades has led to more diverse and sophisticated technologies being used for personal communications, while governments and law-enforcement agencies an unprecedented ability to engage in powerful surveillance.

The legal apparatus reflects new powers, investigative methods, and procedures, all supported by a new technological environment. The far-reaching impacts of communications surveillance on rights and liberties cannot be assessed without considering the technological mechanisms that enable the monitoring of systems, as well as the deep changes in communicational exchanges that these mechanisms support or initiate. Another aspect that has to be taken into account is the potential impact on trust and social acceptance of technologies. The risks of unlawful or arbitrary surveillance and interception of the digital communication technologies can discourage innovation and undermine the opportunities presented by the digital economy, as the protection of privacy is seen as critical for trust that is a particularly important tool in the global online environment for reducing uncertainty and enabling reliance on others.[25]

According to the ECHR, communications surveillance is unacceptable, unless it fulfills three fundamental criteria set in Art. 8 (2):

(1) a legal basis;
(2) the need/necessity of the measure in a democratic society; and
(3) the conformity of the measure with the legitimate interests of national security, public safety, or the economic well-being of a country, prevention or disorder of crime, protection of health or morals, or protection of the rights and freedoms of the others.

The provision reflects the tension between individual and community and the need to take into account the interests of society, without infringing upon the intrinsic value of privacy in a democratic

[22] Mitrou, L. "A Pandora's box for rights and liberties." In Digital Privacy: Theory, Technologies and Practices, edited by A. Acquisti, S. De Capitani di Vimercati, S. Gritzalis and C. Lambrinoudakis, Auerbach Publications 2008.pp. 409 – 432.

[23] Zarsky, T.Z. "Thinking outside the box: Considering transparency, anonymity and pseudonimity as overall solutions to the problems of information privacy in the Internet Society." University of Miami Law Review 58 (2004) :991–1041.

[24] Mitrou L. –The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive, in Haggerty D. and Samatas M., Surveillance and Democracy, 2010, pp. 127ff

[25] OECD Digital Economy Outlook 2015, pp. 30, 209.

society. The Court of Justice of the European Union (CJEU), in its Tele 2 and Watson judgment[26] decided that national legislation, such as that relating to the retention of data for the purpose of combating crime, falls within the scope of European law.

2.3 Restrictions and balancing of rights and interests

Both the right to privacy and communication secrecy and the right to data protection are not absolute. In Art. 8 (2) ECHR, reasons of justification for interferences with Art. 8 (1) ECHR are stipulated. According to this provision, interferences with Art. 8 (1) by a public authority are only allowed if they are in accordance with the law and necessary in a democratic society, for instance, in the interest of national security. In conjunction with the requirement of 'necessary in a democratic society', further vital interests of States are listed such as public safety or the economic well-being of a country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of other. The derogation provided in Art 52 (1) of the EU Charter of Fundamental Rights and Freedoms allows limitations on the exercise of the rights and freedoms recognised [by this Charter] only if "provided for by law and [they] respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

The early case law on balancing of national security with privacy can be found mostly in the jurisprudence of the ECtHR. The ECtHR expressly puts forward the possibility of balancing between privacy and national security or public safety. The ECtHR in its case law has specified the requirements to be met. The three criteria that must be satisfied to ensure that any interference with privacy is in compliance with Article 8(2) are that the interference must be:

a) in accordance with the law;

b) in pursuit of one of the legitimate aims in 8(2); and

c) necessary in a democratic society.

The law authorizing the interference in the above analysed rights has to meet the standards of accessibility and foreseeability inherent in the concept of the rule of law, so that persons can regulate their conduct according to the law (Court of Human Rights, Malone v. U.K., Kruslin v. France). Conditions, safeguards for the individuals, and implementation modalities must be sufficiently summarized, in order to succeed the "quality of law" test[27].

Proportionality, a key principle in European constitutional law, requires a further assessment of the necessity of the measure and its suitability to achieve its aims. Even if necessary is not synonymous

[26] CJEU (Grand Chamber), Judgement of 21 December 2016, Joined Cases C-203/15 (Tele2 Sverige AB) and C-698/15 (Watson), ECLI:EU:C:2016:970, para. 73.
[27] Coemans, C. and Dumortier, J., Enforcement issues—Mandatory retention of traffic data in the EU: Possible impact on privacy and on-line anonymity, in Digital Anonymity and the Law, Nicoll, C. Prince J.E.J., and van Dellen, J.M., Eds., TMC Asser Press, The Hague, the Netherlands, 2003, p. 161.

with indispensable... it implies a pressing social need" (European Court of Human Rights, Handyside v. U.K.)[28]. As "pressing social need" the jurisprudence points to the following considerations:
a) Is the measure seeking to address an issue which, if left unaddressed, may result in harm to or have some detrimental effect on society or section of society?
b) Is there any evidence that such a measure may mitigate such harm?
c) What are the broader views of society on the issue in question?
d) Have any specific views/opposition to a measure or issue expressed by society been sufficiently taken into account?

The CJEU has equally dealt with the issue of conflicts and balances between public security in and data protection in its early case law. One of the most obvious cases in this regard is the case Parliament v. Council and Commission, also known as the Passenger Name Record (PNR) case (2006), which led to the annulment of decisions relating to the PNR agreement.[29] The grounds on which the adequacy decision were annulled was due to the fact that the processing of personal data, transferred on the basis of PNR agreement, did not fall within the scope of the Data Protection Directive (DPD) because it constituted "processing operations concerning public security".

The main characteristic of the jurisprudence in the earlier phase was that the European Courts did not lean towards a preference for protecting privacy, in its multifold nature (informational, communicational) but instead balanced the two values, privacy and security in a rather neutral manner, which allowed to rely on the concrete a factual background of the cases, leading to the result that, in the majority of cases, public security still prevailed over privacy. It was exactly in the context of the gradual awareness of the existence of mass surveillance measures and their gradual escalation in order to meet the challenges of new "asymmetric" terrorist threats that the European courts, notably the CJEU, increasingly began to tilt the balance towards the protection of privacy rather than security. That was the case in the judgment Digital Rights Ireland (2014) that annulled the Directive 2006/24/EC on the retention of data. Although the CJEU underlined that the "objective of that directive is […] to contribute to the fight against serious crime and thus to public security" it regarded the interference with the fundamental rights to privacy and data protection as disproportionate. The CJEU reaffirmed its strict stance towards data retention measures in Tele2 Sverige (2016)[30], where it found incompatibility of the national data retention measures with the EU privacy legislation. In these seminal the CJEU acted as a catalyst of policy change by striking a different balance between data protection and public security as the EU legislator.

In any case, the objective pursued must be balanced against the seriousness if the interference, which is to be judged taking into account, inter alia, the number and nature of persons affected and the intensiveness of the negative effects. Restrictions must be limited to a strict minimum. The necessity and proportionality have to be clearly demonstrated by considering that privacy is not only an

[28] European Court of Human Rights (Plenary), Handyside v. the United Kingdom, Application no. 5493/72), Judgment of 7 December 1976.
[29] *Following the grounds for annulment action, brought by the EP, the CJEU annulled the decision on which the PNR agreement was concluded, as well as the adequacy decision on the transfer of PNR to the USA, as it did not fall within the scope of application of the Data Protection Directive 95/46/EC.*
[30] European Court of Justice, - Tele2 Sverige (C-203/15), Judgment of the Court (Grand Chamber) of 21 December 2016

individual right of control over one's information, but moreover a key element of a democratic constitutional order (German Federal Constitutional Court, Census Decision 1985). In principle, the more intrusive the interference into privacy is, the more significant and necessary the legitimate objective of the measure should be.[31] These restrictions persist even where incursions into privacy rights have been justified by states on grounds of national security or prevention or detection of crime as evidenced by a number of prominent ECtHR cases [ECtHR Weber v. Germany (2006) and Klass v. Germany (1978)].

In case of crowd disasters prevention and management, as in EVAGUIDE, these purposes could be considered as "legitimate aim". With regard to the criterion of the existence of a legal provision set by the conventional and constitutional framework and the jurisprudence, we should note that there must be a legal basis for adopting proactive measures or react to natural or manmade disasters/crisis. Concerning the democracy test, it has to be underlined that before privacy-invasive measures are introduced (e.g. tracking through smartphone applications), it must be examined whether these measures are likely to indeed contribute to the effective management of crowds and whether they are the least intrusive ones. It has to be considered 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.

[31] See Hielke Hijmans Data Protection and Surveillance: The Perspective of EU Law. Draft (October 2018) of Paper Written for: Proceedings from 2018 ECLAN Conference, Hart Studies, European Criminal Law Series, Hart. This is the reasoning of the CJEU in Ministerio Fiscal, where it accepts the access to identification data – so, not metadata of communications - for non-serious crime.

3. DATA PROTECTION LEGAL FRAMEWORK

The European Data Protection Directive (Directive 95/46/EC)[32], adopted in 1995, has been a milestone in the history of personal data protection with worldwide impact and influence. Directive 95/46/EC has been credited with creating one of the world's leading paradigms for privacy protection.[33]However, despite the substantially positive track record and general acceptance of the Directive, its efficiency, if not the applicability itself, (has been) contested. The Directive 95/46/EC was conceived (in 1990), discussed and adopted before the explosion of the Internet and its impacts on economy, society, governance, communication and life. The convergence of the network around a single interoperable platform, the emergence of the "semantic web" and Web 2.0 as well as the changes in identification and authentication techniques, identity management and profiling have created a new environment. Technological and social phenomena like social networks, cloud computing, Radio Frequency Identification (RFID) and geo-location devices and applications, the new possibilities of data mining, machine learning and big data analytics have profoundly changed the way, and the extent to which, data are processed and pose crucial challenges for data protection[34].

In 2016, the General Data Protection Regulation has opened a new chapter for the protection of informational privacy in Europe. More than a simple revision of the Data Protection Directive (1995) and less than a regulatory paradigm shift, the Regulation attempts to keep path with technological and socio-economic changes while guaranteeing the persons' fundamental rights and enabling the control over their data. The GDPR Regulation is is directly applicable to all member states and took effect on 25 May 2018.

The GDPR refrains from technology-specific terminology and provisions and adopts the "technological neutrality approach".[35] Emphasis is put not on the technology used for data processing but on the effects to be regulated, on the risks and impacts on fundamental rights that are to be faced. Although the difficulties and complexities of digital environments have been taken into account by the designing of the data protection regulatory strategy, the regulatory choice of the GDPR consists more of what is perceived as technology – independent legislation. Technology independent rules are regarded as a means to stand firm with technological turbulences.[36] Technology, obviously, develops more quickly that the law. Even within the five-year period between the Commission's Proposal and the adoption

[32] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281/31). In this text we refer to this Directive as Directive 95/46/EC in order to avoid the confusion with "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA" (Directive).

[33] Robinson, Graux, Botterman, Valeri. (2009), pp. 6 f., 22 f.

[34] See L. Mitrou, The General Data Protection Regulation: A Law for the Digital Age? in T. Synodinou et al. (Eds), EU Internet Law, Regulation and Enforcement, Springer 2017, pp. 19-57

[35] With the GDPR the European legislator adheres explicitly to the technological neutrality approach as Recital 15 cites that the protection of natural persons should be technologically neutral and should not depend on the techniques used.

[36] Koops B J Should ICT regulation be technology-neutral? In Koops B-J, Lips M, Prins C., Schellekens M.(eds), Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-liners, It & Law Series, The Hague: T.M.C. Asser Press (2006) pp 77-108, 21.

of the GDPR, technology, or at least the spectrum and the extent of its uses, has changed substantially: mobile apps, Internet of Things or Internet of Everything, cyber-physical systems. etc. Therefore the provisions of GDPR have to be interpreted and implemented in an open and dynamic way.

In the following paragraphs a detailed presentation of the GDPR regulations and how will be implemented under the EVAGUIDE project is provided, giving valuable insights on the main aspects of the Regulation, concerning the collection, storage, processing and sharing of individual's personal data.

3.1. Main notions and definitions/ the concept of personal data

3.1.1 Key terms

The following key terms (Article 4) are defined in the GDPR and are particularly important. They are referred below for the better understanding of the regulation and for completeness reasons.

"'**personal data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'**processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'**controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

'**processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

'**profiling**' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

'**pseudonymisation**' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;Personal data and identified/ identifiable data subject

The data protection legal framework is to be considered and applied only in case that personal data is processed. Both the General Data Protection Regulation (GDPR) (Article 4 (1)) and Directive 2016/680/EU (3 (1)) define as "personal data" any information relating to an identified or identifiable natural person ('data subject')[37]. That means that the identification of data as personal and thus the

[37] Definition of Council of Europe Modernised Convention (108) for the Protection of Individuals with Regard to the Processing of Personal Data. Adopted on 18 May 2018

scope of the respective legislation is strictly related to the notion of identified / identifiable natural person. An individual is 'identified' or 'identifiable' if it can be distinguished from other individuals.

If it is possible to identify an individual directly from the information processed, then that information may be personal data. If an individual cannot be directly identified, it has to be considered whether the individual is still identifiable[38]. As mentioned in the Information Commissioners' Office (ICO)Guide on GDPR[39], a name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context. The GDPR provides in Article 4 (1) and in Recital 30[40] a non-exhaustive list of identifiers, including an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Some characteristics are so unique that someone can be identified with no effort, but a combination of details on categorical level (age category, regional origin, etc) may also be pretty conclusive in some circumstances, particularly if one has access to additional information of some sort. A person remains identifiable, even if the data controller/ processor needs additional information to identify her/him. As stated in Recital 26, to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.
Identifiability within the meaning of the GDPR may also result from matching the data with information held by third parties, or else from a smartphone application, in the individual case, of specific techniques and/or devices[41].

Information must 'relate to' the identifiable individual to be personal data. This means that it must concern the individual in some way. To decide whether or not data relates to an individual, the following has to be considered: a) the content of the data; b) the purpose of processing and the results of or effects on the person from processing the data. From the point of view of the content of the information, the concept of personal data includes data providing any sort of information.

Identification numbers, image and sound data or location data, to the extent that they allow the identification of individuals, are to be considered and treated as personal data and their processing shall be subject to the provisions of the GDPR.

[38] See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data. Also Information Commissioners Office, Guide to the General Data Protection Regulation (version of 22 May 2019).
[39] Https://ico.org.uk/ for-organisations/ guide-to-data-protection/
[40] As Recital 30 states natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them
[41] DPWP, Opinion 4/2007 on the concept of personal data

This is the case with the MAC address[42]. If an individual can be identified from that MAC address[43], or other information in the possession of the network operator, then the data will be personal data. The probe request and response will contain an identifier that will be specific to that user's device .The reason that WiFi access points can be used as a source of geolocation information, is because they continuously announce their existence.

Concering sound and image data, they may qualify as personal data from this point of view, insofar as they may represent information on an individual.

According to Article 29 DPWP, image and sound data that relate to identified or identifiable natural persons is personal data: a) even if the images are used within the framework of a closed circuit system, even if they are not associated with a person's particulars, b) even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers, c) irrespective of the media used for the processing (e.g., fixed and/or mobile video systems such as portable video receivers, colour and/or BW images), the technique used (cabled or fibre optic devices), the type of equipment (stationary, rotating, mobile), the features applying to image acquisition (i.e. continuous as opposed to discontinuous), and the communication tools used (e.g. the connection with a "centre" and/or the circulation of images to remote terminals).[44]

Images of individuals captured by a video surveillance system can be personal data to the extent that the individuals are recognizable. This is the case even if the individuals are not known to or not identified by the operators of the system. Less clearly visible images of an individual may also constitute personal data provided that the individuals are directly or indirectly (combined with other pieces of information) identifiable. Whether an individual can be considered indirectly identifiable depends on the circumstances of the case, including the purpose of the video-surveillance and the likelihood that the Institution (or other potential recipients) will be able to make all the efforts that are necessary to identify the persons captured on camera[45]. If it is possible to *single out/distinguish certain individuals via the analysis of video streams, they should be treated as personal data even when it is not the intention to identify individuals when detecting and interpreting the motion and behavior of crowds.*

---

[42] The unique ID for each WiFi access point is its MAC address (Medium Access Control). A MAC address is a unique identifier attributed to a network interface and usually recorded in hardware such as memory chips and/or network cards in computers, telephones, laptops or access points. See about Article 29 DPWP, Opinion 13/2011 on Geolocation services on smart mobile devices

[43] This identifier is known as the media access control (MAC)addressand is intended to be unique to the device (although it can be modified or spoofed using software). The first part of the MAC address is also unique to the manufacturer of the Wi-Fi interface controller. See ICO, Wi-Fi location analytics 1 1.0 16/02/2016.

[44] See Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance.

[45] See The EDPS Video-Surveillance Guidelines, Brussels 2010. The EDPS mentions as example Cameras are installed on the rooftop of a building with limited resolution to monitor the overall situation in the surrounding area for security purposes during special events. Although the camera footage may not always yield recognisable facial images, police, investigating a serious criminal offence, may be able to indirectly identify the persons captured on the cameras using information derived from the camera footage (for example, clothing, body type, objects carried) in combination with other information detected during the investigation (for example, with the help of witnesses or using other image recordings). In such situations, the Guidelines apply.

Identifiability in the meaning of the GDPR may also result from matching the data with information held by third parties, or else from a smarthphone application, in the individual case, of specific techniques and/or devices.

Images generated by "counting cameras" that capture individuals from a distance and an angle that does not allow the identification of persons, as in EVAGUIDE, are not likely to qualify as personal data. In certain circumstances the applicability of the GDPR may be ruled out for air survey images that cannot be usefully magnified or else do not include information related to natural persons.

The principles and in general the rules of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. The GDPR does not concern the processing of such anonymous information, including for statistical or research purposes (Recital 26 of GDPR).

3.1.2 (Geo)Location data

The term of "location data" is initially related to the legislation concerning the processing of traffic and location data by providers of e-communication services. In this context location data is defined as "any data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to the:

- latitude, longitude or altitude of the terminal equipment;
- direction of travel of the user
- identification of the network cell in which the terminal equipment is located at a certain point in time; and
- time the location information was recorded"[46].

In the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)[47], location data is a category of "metadata"[48].

In the above mentioned context the concept of "location data" does not generally include GPS-based location information from smartphones, tablets, sat-navs or other devices, as this data is created and collected independently of the network or service provider. Neither does it include location information collected at a purely local level (eg by wi-fi equipment installed by businesses offering wi-

[46] See Article 2 c and Recital 14 of DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), currently under revision

[47] Version adopted by the Council of the European Union Brussels, 12 July 2019 (OR. en) 11001/19

[48] Article 4 par. 3 c of the draft e-Privacy Regulation states as metadata any data processed in an by means of electronic communications network services for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication;

fi on their premises).[49] According to the draft e-privacy Regulation (Recital 17) "... location data that is generated other than in the context of providing electronic communications services should not be considered as metadata..." However, the term "location data" used in GDPR is not identical with the term used in e-Privacy Directive.[50]

Smart mobile devices are inextricably linked to natural persons. There is usually direct and indirect identifiability. Beyond the unique identifier, the MAC address, that is common in every smart device, the device may have other unique identification numbers, added by the developer of the operating system, which may be transmitted and further processed in the context of geolocation services. It is a fact that the location of a particular device can be calculated in a very precise way, especially when the different geolocation infrastructures are combined. This indirect identiability applies to WiFi access points as well. The MAC address of a WiFi access point, in combination with its calculated location, is inextricably linked to the location of the owner of the access point enabling a "reasonably equipped controller" to calculate an increasingly precise location of a WiFi-access point based on the signal strength and of the ongoing updates of the location through the users of its geolocation service[51].

3.1.3 The notion of processing

The GDPR, as the repealed Data Protection Directive, defines "processing" in an apparently and consiously broad way: Article 4 (2) states that processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. This open definition aims at ensuring the technological neutrality of the provisions and the forms of processing they regulate.

In this respect since the MAC address of a WiFi access point, in combination with its calculated location, is treated as personal data, the collection of these data also results in the processing of personal data. Using a MAC address or other unique identifier to track a device with the purpose to single them outor treat them differently involves the processing of personal data. This could mean that the data controller can monitor the location of the device and track the behaviour of a particular

[49] See ICO, Guide to PECR accessible at https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/location-data/

[50] As interpreted by Article 29 DPWP, the e-Privacy directive (under revision) does not apply to the processing of location data by information society services, even when such processing is performed via a public electronic communication network. According to Article 29 DPWP, a user may choose to transmit GPS data over the Internet, for example when accessing navigational services on the Internet. In that case, the GPS signal is transmitted in the application level of internet communication, independently of the GSM network. The telecommunication service provider acts as mere conduit. It cannot gain access to GPS and/ or WiFi and/or base station data communicated to and from a smart mobile device between a user/subscriber and an information society service without very intrusive means such as deep packet inspection. See Opinion 13/2011 on Geolocation services on smart mobile devices.

[51] Article 29 DPWP, Opinion 13/2011 on Geolocation services on smart mobile devices

device over time[52]. In general smart phones transmit Wi-Fi signals which are captured at the Wi-Fi access points. The captured signals contain information about the measured received signal strength (RSS) and potentially personal data.

Personal data processing takes place also when image data are captured through the use of video surveillance. The GDPR applies even if the cameras are only used on an ad hoc basis. The video-surveillance comes under the scope of the Regulation despite its temporary and ad hoc character. We have to underline that privacy and security risks may be present, even if no footage is recorded and the footage is only transferred live to the intended recipients via an internal network[53].

3.2 The legal grounds of processing

In the European constitutional and legal order the processing of personal data and other interferences with the right to (informational) privacy should have a legal basis, as required by Article 8 ECHR and Articles 7 and 8j 52 CFREU. Any data processing activity must fulfill at least one of the criteria for making the processing legitimate. Similar to the situation under the 1995 Data Protection Directive, under the GDPR a data controller may process personal data only if there is a "lawful basis" for such processing.

Article 5 of GDPR decrees that personal data shall be "processed lawfully," and Article 6 lays out six legal bases that satisfy the lawfulness requirement:

a) The data subject has given consent to the processing of his or her personal data for one or more specific purposes.
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.
c) Processing is necessary for compliance with a legal obligation to which the controller is subject.
d) Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
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.
f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular where the data subject is a child.

Many of the lawful bases for processing depend on the processing being "necessary". As mentioned in ICO's Guide, this does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose[54].

Although Article 6 limits the legality of processing to situations where "at least one" of the bases applies, organizations should be cautious about relying on multiple lawful bases for any single

[52] See S. Georgievska1, P. Rutten, J. Amoraal, E. Ranguelova, R. Bakhshi1, Ben L. de Vries1, M. Lees and S. Klous, Detecting high indoor crowd density with Wi Fi localization: a statistical mechanics approach
[53] EDPS, Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines, 2019
[54] ICO, Guide to the General Data Protection Regulation

processing purpose. The Article 29 Working Party's guidance on consent suggests that "[a]s a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases." The legal for processing has to be identified at the time of collection, before processing occurs, and per Article 13(1)(3), must furnish the data subject with both the purpose of the processing and its legal basis at the time data is collected.[55]

Any personal data processing operation in EVAGUIDE 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 9 of GDPR that refers to the following categories of (sensitive) data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

As a general principle it is forbidden (Article 9 (1) of GDPR) to process sensitive personal data unless one of the grounds in Article 9 (2) of GDPR is met. These grounds are stricter than the ones under Article 6 of GDPR.

Beyond the research scope, aim and phase data controllers that will make deploy EVAGUIDE or similar systems, must bear in mind that they have to identify the legal basis that is most suitable to be applied in emergency cases, taking into consideration also the nature, the role, the obligations and the activities of the data controller. The correct legal basis will depend on the particular emergency situation, as well as on the scope of rights and obligations of the persons (natural or legal persons) and/ or the authorities which are involved in the emergency response. In the case of mobile apps, the Article 29 Working Party recommends data controllers to consider having two separate legal bases – one for installing an app and the other one for the processing of personal data during the usage of this app[56].

3.2.1. Consent

There are two main issues/ requirements that are to be dealt with regard to consent. The preliminary question relates to the acceptability of consent as legal basis. The second one refers to the conditions of consent with focus on information about the data processing which has to be provided to the data subjects. The Article 29 Working Party recommends consent as a principal legal ground when installing apps.

In general consent has to fill the requirements and conditions set up both in the definition of consent (Article 4 (11)) and Article 7 of GDPR, e.g. it has to meet certain criteria to be valid. Article 4(11) of the GDPR stipulates that consent of the data subject means any:

- freely given;
- specific;
- informed; and
- unambiguous indication

[55] See Article 29 Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 as last Revised and Adopted on 10 April 2018.
[56] Article 29 DPWP, Opinion 13/2011 on Geolocation services on smart mobile devices

of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

As a general rule, the GDPR prescribes that if the data subject feels compelled to consent or will endure negative consequences, then consent will not be valid[57]. In general terms, any element of inappropriate pressure or influence upon the data subject (which may be manifested in many different ways) which prevents a data subject from exercising their free will, shall render the consent invalid[58]. Furthermore, compulsion to agree with the use of personal data additional to what is strictly necessary "stands in the way of free consent"[59].

Consent could be a legitimate and suitable ground in the case of the EVAGUIDE mobile application, where the individuals are informed of the usage of their data through the app (e.g. location data) in advance and give their consent for this future operation. GDPR prescribes that if the data subject's consent is given in the context of a written declaration which also concerns other matters (for example in the case that the consenting person has to accept the terms and conditions of season tickets), the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

3.2.2. Consent as basis for processing in the research context

Consent of volunteers/ participants would be the most likely legal ground during the validation demonstrations when volunteers are invited to participate and let the EVAGUIDE project process their data. As emphasized by the European Commission[60], informed consent is the cornerstone of research ethics. Consent has to be given by a clear affirmative act, establishing a freely given, specific and informed and unambiguous indication of the subject's agreement to the processing of their personal data. Research participants must be informed about the object and aim of research, what their participation in your project will entail and any risks that may be involved.

For consent to data processing to be 'informed', the participant must be provided with detailed information about the envisaged data processing in an intelligible and easily accessible form, using clear and plain language. Information should at minimum include:

- the identity of the data controller and, where applicable, the contact details of the DPO;
- the specific purpose(s) of the processing for which the personal data will be used;

[57] Opinion 15/2011 on the definition of consent (WP187).
[58] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018. Article 29 DPWP refers to the example of mobile app or photo editing asks its users to have their GPS localisation activated for the use of its services. The app also tells its users it will use the collected data for behavioural advertising purposes. Neither geolocalisation or online behavioural advertising are necessary for the provision of the photo editing service and go beyond the delivery of the core service provided. Since users cannot use the app without consenting to these purposes, the consent cannot be considered as being freely given.
[59] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, p.8
[60] European Commission, Ethics and Data Protection, November 2018.

- the subject's rights as guaranteed by the GDPR and the EU Charter of Fundamental Rights, in particular the right to withdraw consent[61] or access their data, the procedures to follow should they wish to do so, and the right to lodge a complaint with a supervisory authority;
- information as to whether data will be shared with or transferred to third parties and for what purposes;
- information about how long the data will be retained before they are destroyed; and
- information about the further use of data for any other purposes, the sharing with research partners and/or the transfer of data to organisations outside the EU (see article 13 GDPR).

The consent process(es) and the information to be given to the participants should cover all the data-processing activities related to their participation in the research/demos. Consent may take the form of a written statement, which may be collected by electronic means, or an oral statement. As in all cases, where processing is based on consent, the controller must able to demonstrate that the data subject has consented to processing of his or her personal data. The informed consent procedure has to be documented, including the information sheets and consent forms provided to research participants, and the acquisition of their consent to data processing. Documentation may be requested by data subjects, funding agencies or data protection supervisory authorities. In the Deliverable 6.1 of EVAGUIDE a detailed description of the consent forms that will be provided to volunteers during pilot tests are described. Also at the Deliverables 6.2 & 6.3 a description of the data that will be gathered by the EVAGUIDE system are highlighted, along with the technical/ organizational and security measures that will be used to safeguard the rights of data subjects and to prevent an unauthorized access to them.

Informing participants / data subjects is necessary to comply also with the principle of transparency (Article 5 a). Transparency contributes to fairness and raises individuals' awareness about the uses of their personal data and thus enables them to keep control over their data, which is a main element of the right to data protection (right to informational self-determination). The fairness and transparency principles could be satisfied when the data controller (research partners or end-users) ensures that information about the collected personal data, its uses and rights of data subjects is made accessible to the users at any time when running the apps[62].

In the context and for the research purposes of EVAGUIDE, volunteers participating at the pilot demonstrations must be informed about each separate purpose of the system is and related to that - which categories of data will be processed for each purpose (e.g. mobile app, video streams). This includes what information might be stored on the platform or what information already stored will be accessed via the applications. In addition, the information notice should inform the users of how their data will be processed through the system, e.g. that their location might be tracked during evacuation, search and rescue operations.

[61] The GDPR requires that data controllers inform the data subject about their right to withdraw prior to giving consent. It is important to note that the GDPR requires that it must be as easy to withdraw as to give consent According to Article 7 par. 3 of GDPR, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

[62] Lina Jasmontaite and Diana Dimitrova, Online Disaster Management: Applicability of the European Data Protection Framework and Its Key Principles, Journal of Contingencies and Crisis Management Volume 25 Number 1 March 2017

Particularly for the smartphone application, mechanisms for withdrawing consent for the download of the whole app or only from its individual elements, e.g. the location tracking function during evacuation or entertainment information provision, should be available to the users all the time. In addition, there should be mechanisms for deactivating the app once the users have exited the end-user venues or while they are on the venue, if the wish to deactivate the app.

3.2.3 Legal obligation

Article 6c provides a legal ground in situations where "processing is necessary for compliance with a legal obligation to which the controller is subject". It may be an obligation to which a public authority or a private (natural or legal) person is subject. This legal ground may be used in case that the data controller, e.g. for example the authority, the stadium owner or the event organizer, is bound by a legal obligation that requires to take specific measures for ensuring safety of persons participating to an event and will use the EVAGUIDE platform/ system in real life situations. Data controller in this case could be a state authority, a department.

For Article 6(c) to apply, the obligation must be imposed by law, which must fulfil all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirement of necessity, proportionality and purpose limitation. The controller must have neither a choice whether or not to fulfil the obligation nor an undue degree of discretion on how to comply with the legal obligation.[63]

The (natural and/or legal) persons involved in the emergency response and management may be subject also to specific regulation that provides for emergency management. In this case these provisions may serve as legal ground for the processing of personal data in case that it is deemed necessary for fulfilling the said obligations.

3.2.4 Performance of a task in the public interest or exercise of official authority

Article 6(e) provides a legal ground in situations where 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). There is no requirement for the controller to act under a legal obligation, but the data processing must be "necessary for the performance of a task carried out in the public interest".

Article 6(e) has potentially a very broad scope of application. Article 29 Data Protection Working Party, favors a strict interpretation and a clear identification, on a case by case basis, of the public interest at stake and the official authority justifying the processing. As accepted by the Article 29 Data Protection Working Party, video surveillance for security and safety reasons is an example that may come under this broadly interpreted provision of "tasks carried out in the public interest".

[63] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC

3.2.5 Vital interests

Article 6(d) provides for a legal basis in situations where "processing is necessary in order to protect the vital interests of the data subject or of another natural person". This wording is different to the language used in Article 9(2)(c) which is more specific and refers to situations where "processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent".

This provision could be relied on as a legal basis if it is accepted that the protection of vital interests includes saving one's life, i.e. it is question of life and death or serious injuries, although the GDPR seems to be less restrictive, as Recital 112 refers to "vital interests, including physical integrity or life".

Although Article 6(d) does not specifically limit the use of this ground to situations when consent cannot be used as a legal ground it is reasonable to assume that in situations where there is a possibility and need to request a valid consent, consent should indeed be sought whenever practicable.

While this provision reads like a good candidate for a legal basis, it may be used only in emergency cases, e.g. that disaster has actually happened or there is immediate threat to the life or integrity/ health of the data subject. The use of this legal ground has to be assessed and decided on a case by case analysis and cannot normally be used to legitimize any massive collection or processing of personal data.[64]

3.2.6 Legitimate interest of data controller / third person

According to Article 6 pa. r1f, processing is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data. In addition to purpose and necessity test this provision requires a careful balancing between the interests of the controller and the fundamental rights of data subjects, such as privacy and data protection.[65] To this end, the interest of the controller should be clearly articulated to allow assessing and balancing. The balancing has to ensure that the processing of data on this legal ground pursues a legitimate aim and that for the achievement of this aim, the measures taken do not go beyond what is necessary to achieve the purpose and thus the disadvantage caused to individuals is only the minimum necessary.

A wide range of interests may be regarded as "legitimate", including "wider social benefits". In addition, this provision does not give a blanket permission to re-use and further process publicly available data, such as location information that individuals post on their social network profiles. A data controller can rely on legitimate interests as appropriate basis where he processes data in a way that have a minimal privacy impact or - where there is an impact on data subjects- it may still apply if

[64] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Jasmomaite and Dimitrova regard this legal basis as applicable only in such situations, when other search and rescue actions have been fruitless. L. Jasmontaite and D. Dimitrova, Online Disaster Management: Applicability of the European Data Protection Framework and Its Key Principles.

[65] ICO, Guide to the General Data Protection Regulation, 2018.

it can been demonstrated that there is an even more compelling benefit to the processing and the impact is justified. If individuals would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override the legitimate interests of data controllers or third parties. Performing activities of video surveillance that aims at ensuring the security and safety of persons and goods is often regarded as grounded on legitimate interest of the data controller.

Public authorities can principally not rely on legitimate interests in the performance of their tasks, with the exception of restrictive cases, e.g. if they are processing for a legitimate reason other than performing their tasks as a public authority.

Following the accountability requirement, it is advisable to perform a systematic legitimate interests assessment (LIA) before the processing and keep documentation about the legitimate interests pursued by the processing.

3.2.7. Processing employees' data

For the purposes of the pilots and demos, as well as in case of emergency responses, specific applications may be designed for the employees, acting also as a category of first responders (stewards) in case of emergency/ disaster. In case that employees are provided with applications, such as EVAGUIDE mobile app for spectators and stewards their data is also be collected, thus resulting also in the so called employee monitoring only during the pilots/ demos. This is also the case with respect to the use of video surveillance for the purposes of emergency/ disaster management.

As to the legal basis, in principle consent is not a suitable legal basis in the employment context. According to Recital 42, consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment. Although consent remains a potential legal ground also in the employment field, data protection authorities consider this basis principally as not acceptable as "employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer"[66].

A first possible legal basis would be the performance of the employment contract (Article 6 par. 1 b of GDPR) to be applicable in cases that it is provided that such applications or tools will be provided to employees to perform or assist their duties according to the contract. Another possible legal ground that can be invoked refers to the purposes of the legitimate interests of the controller (Article 6 par. 1 (f) GDPR), but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity and it outweighs the general privacy rights that employees also have in the workplace and what measures must be taken to ensure that infringements on the right to private life and the right to secrecy of communications are limited to the minimum necessary.

More specifically and particularly for the EVAGUIDE mobile application it has to be demonstrated that the app is the least harmful means for the employer to ensure that an emergency demo or a response is efficiently carried out. In any case employees must be clearly informed of the functionality of the

[66] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work.

app and the processing of their data. Additionally specific safeguards must be designed and provided to avoid the use of the app as a constant tracking tool.

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 5 of GDPR. These principles entail:

a) lawfulness, fairness and transparency (dealt mainly under 3.3);
b) 'purpose limitation';
c) data minimization (proportionality);
d) accuracy;
e) storage limitation;
f) integrity and confidentiality.

By understanding and following these key principles, interested parties set the basis to ensure their compliance with the new data protection framework.

3.4.1. Purpose definition – purpose limitation

According to the so-called purpose specification[67]/limitation principle, personal data have to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (5 par. 1b). With compliance to this principle, the data controller(s) should define the purposes for which they need to process the personal data, before personal data are processed (i.e. even before the data are collected), by the project partners. Defining the purpose is essential for determining what the boundaries of the legitimate use of the data are, which data and what storage period are relevant for that particular data processing. The concrete definition of the purpose is of outmost importance also for assessing compliance with the other principles relating to processing of personal data.

According to the data limitation principle it is not allowed to use the data collected for another purpose that is not compatible with the initial one. 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 transmitting to or sharing of information between different organisations, authorities etc. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia:

- any link between those purposes and the purposes of the intended further processing;

[67] The 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".
The Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle and Use Limitation P rinciple – were set out in Article 5 of the 1981 Convention (without those terms being used: the Convention li sts these principles together under the heading "Quality of data".

- the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use;
- the nature of the personal data;
- the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations (see Recital 50).

However, the GDPR considers as compatible further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

In general, in these cases the data subjects still need to be informed about the data processing[68]. However, if the provision of such information would involve a disproportionate effort or would be impossible, especially where the data are re-used for historical or scientific research, such as in EVAGUIDE, then this provision could be derogated from. However, appropriate measures still need to be taken to protect the data subject's rights and freedoms and legitimate interests (Article 14 par. 5 GDPR).

While it is evident most of the times that the data will be needed for research purposes, it is advisable to specify more narrowly these purposes. Such narrower definition is recommendable for every separate research activity where personal data are processed. However, the GDPR recognizes (Recital 33), it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. According to the abovementioned Recital, data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

In the context of use of the EVAGUIDE platform the exchange of collected data between system operators and other responders, including competent public authorities, for the purpose of emergency/ crisis management could be considered as compatible. As compatible can be regarded also the re-use for research purposes, for example when one of the end-users in EVAGUIDE platform wants to reuse the data lawfully collected by them or allow the other partners to use this data for other purposes. A safeguard that should be taken is the anonymization of data/ images captured permanently and irreversibly in such a way that they do not constitute personal data any longer and cannot be reversed, in which case the data protection framework would not apply if there is no risk of identifiability of the individuals recorded. Without prejudice to statistical/ scientific research purposes, if data are not anonymized, then a new legal basis for the processing needs to be established as there would be a change of the original purpose of processing and disclosure to further parties.

[68] According to Article 13 par. 3 of GDPR where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information. Similar is the provision of Article 14 par. 4

3.4.2. Principle of Data minimization (proportionality)

Once the lawfulness of the processing has been validated and its purpose articulated, the principle of data minimisation requires careful assessment of the proportionality of the arrangements applying to the data processing. Protecting human life through proper evacuation management is undoubtly a legitimate aim but it has to be pursued under consideration of the proportionality/ data minimisation princile, in order to ensure that rights and freedoms of individuals are not affecte in a disproportionate way.

The principle of data minimization is a core principle of data protection and implies that data (to be) processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'). Article 5 of GDPR clarifies the application of the principle of proportionality to underline that it should apply throughout the entire processing, and in particular in respect of the means and methods used in the processing. It is furthermore reinforced by the principle of data minimization.[69] The proportionality principle is of particular importance. It serves as an instrument for balancing conflicting interests in a way that does not give precedence to any of them. In order not to unnecessarily restrict the rights of the individuals in return for societal benefits, a -often- delicate balance must be struck between the employed means and the pursued purpose.

The proportionality principle as such, has not been explicitly mentioned in the European Convention of Human Rights, but according to the European Court of Human Rights rulings it is a central feature of human rights. The principle is also used in the jurisprudence of the Court for establishing a balance between the right to a 'protected private life of the individuals' and 'the interest for a safer society and protection of national interests".[70]

At European Union level, the proportionality principle is contained in Article 52(1) of the Charter of Fundamental Rights, which constitutes a condition to be fulfilled when a necessity (according to the pressing social need of the jurisprudence of the Strasburger Court) requires the limitation of non-absolute rights. The European Court of Justice (ECJ) has developed this principle using a "test" for assessing the proportionality of a measure. This test is composed of three steps:

(i) appropriateness;
(ii) necessity; and
(iii) proportionality stricto sensu.

The measure must be first of all appropriate or suitable to protect the interests that require protection. It must be necessary, meaning that no measure less restrictive must be available to attain the objective pursued. And it must be proportionate stricto sensu, meaning that the restriction that it causes must not be disproportionate to the intended objective or result to be achieved.

[69] Douwe Korff and Marie Georges, The DPO Handbook Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, T4Data, 2019

[70] See J. Milaj (2015): Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance, International Review of Law, Computers & Technology

According to Article 29 Working Party, one factor in assessing whether a proposed (i.e. new) intrusive measure is strictly necessary and proportionate is by reviewing the effectiveness of the already existing measures" over and above the proposed measure."[71] Furthermore it has to be demonstrated that the proposed technology (app, platform etc.) is likely to address the legitimate aim and the respective pressing social need.

The proportionality test requires both a) the researchers/ developers to design applications/ systems and carry out demonstrations and tests while restricting the data processing to what is strictly necessary for achieving the research purpose and b) the decision makers that want to use such apps/systems to consider the usefulness, necessity and stricto sensu proportionality of a technology to be introduced in their premises and make the respective choices. Therefore, the controller(s) in the research/ deployment phase must assess and justify the necessity and relevance of all categories of personal data in advance of each processing.

A first issue relates to the extent of use of the apps, e.g. if the activation of the system is (designed to be) dependent on the identification of the risk/ emergency case. Principally the activation has to be avoided until a situation necessitates it. Furthermore, another requirement refers to the nature, categories and amount of data collected and processed. They have to be defined in the light of compliance with the data minimization principle, e.g. they have to be relevant and restricted to the minimum necessary. What is considered necessary depends on what data the individual apps/ platforms process, on the particular situations and on the potential/ art of processing, as some platforms may per se be more intrusive than others. The purpose is to ensure that the chosen means and measures do not go beyond what is necessary in order to respond to the event and they are the least intrusive ones.

Proportionality refers also to the extent of accessibility of information collected. The need-to-know principle is applicable firstly with regard to the (minimum) amount of data considered as necessary for the purposes of application. For example the use of apps should not result to retrieve/ access more data than necessary or for longer time than necessary. A possible solution could be to store not all the location data produced. In this respect it is not regarded as necessary and stricto sensu proportionate to track via mobile apps individuals at all times. Proportionality and minimization principles refers also to the categories and number of bodies/ persons that are entitled to access this data: the personal data processed through the system should not be accessed by partners/employees/officials not involved in the emergency response. In this context it has the storage possibilities and media have also to be examined and assessed.

The requirements deriving from data minimization principle are applicable also to the use of video surveillance apparatus. If researchers and /or end-users are persuaded that there is a clear need to use video surveillance tools and there are no other less intrusive methods available, they should only use this technology if the detrimental effects of video-surveillance are outweighed by the benefits of the video-surveillance.

[71] Article 29 Working Party, Opinion 1/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector

Therefore, it has to be underlined that for the purposes of gaining density information (or unusual) crowd behavior no facial recognition would be necessary. When identification is not necessary, the camera resolution and other modifiable factors should be chosen to ensure that no recognisable facial images are captured.

Compliance with the data minimization principle relates both to camera locations, the viewing angles and the zooming features/capabilities. The visual angle should be designed/deployed in a way that does not allow visualising details and/or somatic traits that are irrelevant to the purposes pursued. In this regard image quality and resolution have to be oriented and adapted to the intended legitimate purposes in order to be considered as proportionate. In the case of EVAGUIDE cameras will be installed overhead the crowd and only for people-counting purposes, minimizing this way the possibility of capturing people's faces.

The EVAGUIDE solution has to be designed and deployed in a way to ensure - to the extent that such is possible - that it (and the data collected) will not be used for incompatible purposes that are not provided by law, thus exposing the rights and freedoms of individuals to high infringement risks. Pseudonymisation or anonymization of data is not only a preferable security measure but also a way to ensure the proper balance between safety and privacy, unless that pseudymisation or anonymization jeopardizes the achievement of the legitimate purpose of evacuation management. It can be recommended to use blurring mechanisms/tools as form of anonymization of image data captured, unless they would be deemed necessary to identify a certain individual for rescue purposes.

However, we should keep in mind that while the principle of "data minimization" obliges data controllers to collect and process only the personal data that is necessary for the purposes of the processing, the implementation of the principle is difficult in practice as response to different types of emergencies may require to process different types of personal data.[72]

3.4.3 Data accuracy

One of the "data quality" principles relates to the accuracy of personal data. According to Article 5 par. 1d personal data must be accurate and, where necessary, kept up to date. Beyond the data protection requirements we should note that is of a significant importance in emergency situations, for example, when determining the location of an affected individual or a first responder/ steward. The GDPR does not explicitly distinguish between personal data that is created/ collected by the data controller and personal data that someone else has provided to the data controller.

What is new with regard to the provision of Directive 95/46/EC is that includes a clearer proactive obligation to take reasonable steps to delete or correct without delay inaccurate personal data. In this context the data controller has to ensure that the source and status of personal data is clear and carefully consider whether it is necessary to periodically update the information. What is regarded as 'reasonable step' depends on the circumstances and, in particular, the nature of the personal data

[72] Workshop on Mobile, Networked and Collaborative Public Protection and Disaster Relief 2016 _Report by Lina Jasmontaite - 14 June 2016

and the purpose for which they are used for. As noted by ICO, the more important it is that the personal data is accurate, the greater the effort you should put into ensuring its accuracy.[73]

Concerning the obligation to keep the data up to date, its scope depends on the purpose, for which data are collected for. Updating personal data may under certain circumstances also defeat the purpose of processing.

Under this provision and in combination with Article.19 GDPR, individuals have a stronger right to have inaccurate personal data corrected under the right to rectification.

3.4.4. The storage limitation principle

The GDPR confirms the storage limitation principle as established already in Directive 95/46/EC. Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. They may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (Article 5 par. 1 e). It is noteworthy that ICO recommends to comply with this principle also to reduce the risk of use of this data "for error-to the detriment of all concerned"[74]

Neither the GDPR nor – in principle – the national laws set specific time limits for different types of data. The retention period with regard to personal data collected through apps, video surveillance or other means has to be specified in line with the specific purposes and features of each case. However, both researchers and end-users under the EVAGUIDE project have to consider that several national laws set specific retention period for data captured through the use of CCTV systems.

In absence of a specific retention provision images may be kept in form that they allow the identification of data subjects for a few days. According to the Guidelines issued by the EDPS, when cameras are installed for purposes of security and access control, one week should in most cases be more than sufficient for the data controller to make an informed decision whether to retain any footage for longer in order to further investigate a security incident or use it as evidence[75].

With respect to the reasonable retention period for data collected through the applications, it has to be defined, taking into consideration, whether there has been an emergency or not. In the context of the project, the EVAGUIDE partners that retain personal data are required to delete it as soon as it is not necessary any more for the purposes of the research. A reasonable storage time would be until the end of the project, unless the partners can demonstrate why the data should be stored longer and the data subjects are informed of this when they provide their consent.

In any case a retention policy has to be elaborated and adopted by the (joint) data controllers to list the types of record or information they hold, what they use it for, and how long they intend to keep

[73] ICO, Guide to the General Data Protection Regulation, 2018
[74] ICO, Guide to the General Data Protection Legislation.
[75] See THE EDPS VIDEO-SURVEILLANCE GUIDELINES (2010/2018) . See also Article 29 DPWP Opinion 4/2004 of the Article 29 Data Protection Working Party on the Processing of Personal Data by means of Video-Surveillance, part 7(E),

it and if possible to establish and document standard retention periods for different categories of personal data. In case that data is to be retained beyond the normal retention period, it is advisable to keep a register indicating at least the reason why the footage needs to be retained and the expected date of the review of the necessity to retain the footage any longer. To note is also the clear links to the new right to erasure (right to be forgotten) as laid down in Article 17 GDPR that provides that an individual may require the deletion of data, if they are no longer necessary for the fulfilment of the purpose it has been initially collected for.

3.4.5. The data security principle

The principle of data security (Article 5 par. 1 f) requires that appropriate technical or organisational measures are implemented when processing personal data to protect the data against accidental, unauthorised or unlawful access, use, modification, disclosure, loss, destruction or damage[76]. The GDPR states that the controller and the processor should take into account "the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" when implementing such measures.

When putting specific security measures in place, the controller – or, where applicable, the processor – should take into account several elements, such as the nature and volume of the personal data processed, potential adverse consequences for data subjects, and the need for restricted data access. The current state of the art of data security methods and techniques for data processing must be considered when implementing appropriate security measures. The cost of such measures must be proportionate to the seriousness and probability of potential risks. A regular review of the security measures is required so that they may be updated as necessary.
Depending on the specific circumstances of each case, appropriate technical and organisational measures could include, for example, pseudonymising and encrypting personal data and/or regularly testing and evaluating the effectiveness of the measures to ensure the data processing is secure. [77]

Pseudonymisation is not to be confused with anonymization. While anonymization means that all links to identifying the person are broken, pseudonymising data means replacing the attributes in personal data – which make it possible to identify the data subject – with a pseudonym, and keeping those attributes separate, under technical or organisational measures. This is especially important in the research context, as the data controllers need to ensure that they are dealing with the same data subjects but do not require, or ought not to have, the data subjects' real identities. Pseudonymisation is therefore strongly to recommend as it can function as an important element when implementing privacy by design.
In Deliverable D.6.2 we have outlined the technical and organizational measures for the protection of personal data than will be collected/processed under the EVAGUIDE project. The analyses has been conducted taking into account the GDPR regulation, aiming to assess the nature, scope, context and purposes of the data collection/ processing and the technical/ organizational mitigation measures for their protection.

[76] See also General Data Protection Regulation, Recital 39 and Art. 5 (1) (f)
[77] In this context see also the Explanatory Reportyt of Council's of Europe Modernised Convention 108, para. 56

3.5. THE RIGHTS OF THE INDIVIDUALS

Under the EVAGUIDE project when partners and end-users (stadium operators/ owners) process personal data both for the research purposes and for the crisis management, they need to fully respect the rights of the data subjects, as laid down in Articles 12-22 of GDPR.

3.5.1. The transparency principle and the information of data subjects

The GDPR reinforces the position of data subjects by introducing more and more clear requirements with regard to the information of data subjects. Transparency places a triple obligation upon data controllers insofar as the rights of data subjects under the GDPR are concerned. Under EU law, the transparency principle requires that any personal data processing should generally be transparent to individuals. Individuals have the right to know how and which personal data are collected, used or otherwise processed, as well as to be made aware of the risks, safeguards and their rights regarding processing

They must, not only provide information to data subjects on their rights and facilitate the exercise of those rights, but there is also the requirement to comply with the principle of transparency (i.e. relating to the quality of the communications). According to the WP29, the GDPR requirements in relation to the exercise of a data subject's rights and the nature of the information required are designed to meaningfully position data subjects so that they can hold data controllers accountable for the processing of their personal data.

The provisions of Articles 12-14 GDPR define specifically the transparency obligations of data controllers. According to the Guidelines issued by the Article 29 Data Protection Working Party[78], the information or communication made available to data subjects must comply with the following rules:
a) it must be concise, transparent, intelligible and easily accessible;
b) clear and plain language must be used (particularly when providing information to children); and
c) it generally must be provided free of charge.

Article 13 and Article 14 of the GDPR deal with the right of data subjects to be informed, either in situations where personal data were collected directly from them, or in situations where the data were not obtained from them, respectively.

The information must be provided in writing, including by electronic means and when requested by the data subject, it may also be provided orally if the identity of the data subject is proven by other means. The WP29 has explained that "intelligible" means that the information should be understood by an average member of the intended audience. A data controller will have knowledge about the people it collects information from and it can use this knowledge to determine what that audience would likely understand; for example, working professionals will have higher level of understanding than children. The fair processing principle requires that information be easily understandable to data subjects. Language must be used which is appropriate for the addressees. The level and type of language used would need to be different depending on whether the intended audience is, for example, an adult or a child, the general public or an academic expert. The question of how to balance

[78] Article 29 Data Protection Working Party,

this aspect of understandable information is considered in the Article 29 Working Party Opinion on More Harmonised Information Provisions[79]. This promotes the idea of so-called layered notices, allowing the data subject to decide which level of detail they prefer. However, this way of presenting information does not relieve the controller from its obligation under Article 13 and Article 14 of the GDPR. The controller must still provide all information to the data subject.

The data controller has to provide the information on actions taken on requests for exercising the data subjects' rights to the data subjects within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. In the case where the personal data have not been obtained from the data subject, the controller must provide the information (1) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed or (2) at the latest at the time of the first communication to that data subject (if the personal data are to be used for communication with the data subject) or (3) at the latest when the personal data are disclosed (if a disclosure to another recipient is envisaged).

3.5.2. Rights to access and right to rectification

Under the GDPR, the right to access one's own data is explicitly acknowledged in Article 15 of the GDPR. The right to access is a central element of the fundamental right to the protection of personal data in Article 8 (2) of the EU Charter of Fundamental Rights.

The GDPR provides that every data subject has the right to access their personal data and certain information about the processing, which the controllers must provide. In particular, every data subject has a right to obtain (from the controller) confirmation as to whether or not data relating to them are being processed, and information about at least the following:

- processing purposes;
- categories of data concerned;
- recipients or categories of recipients to whom the data are disclosed;
- period for which the data is intended to be stored, or, if not possible, the criteria used to determine that period;
- existence of rights to rectify or to erase personal data, or to restrict personal data processing;
- right to lodge a complaint with the supervisory authority;
- any available information about the source of the data undergoing processing if the data are not collected from the data subject; and
- in the case of automated decisions, the logic involved in any automated processing of data.

The data controller must provide the data subject with a copy of the personal data being processed. Any information communicated to the data subject must be provided in an intelligible form, which means that the controller must make sure the data subject can understand the information provided.

Under Article 16 GDPR data subjects have the right to have their personal data rectified. According to EU law and Council of Europe (CoE) law, inaccurate personal data must be rectified without undue or excessive delay.

[79] Article 29 Data Protection Working Party), Opinion 10/2004 on More Harmonised Information Provisions,

3.5.3. Rights to erasure, Rights to restriction and to objection

Providing data subjects with a right to have their own data erased is particularly important for the effective application of data protection principles and notably the principle of proportionality (data minimization), as well as the storage limitation principle.

Under EU law, Article 17 of the GDPR gives effect to data subjects' requests to have data erased or deleted. The right to have one's personal data erased without undue delay applies where:

- the personal data are no longer necessary regarding the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; and
- the personal data have been collected concerning the offer of information society services to children pursuant to Article 8 of the GDPR.

There are five exceptions where the controller may refuse to comply with the data subject's request for exercising the right to erasure (Article 17 (3) GDPR). These exceptions are applicable where the processing is necessary for:

- exercising the right of freedom of expression and information;
- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- or the establishment, exercise or defense of legal claims.

The burden of proof that the data processing is legitimate will fall on the data controllers (in EVAGUIDE's case the researchers (partners)/ end-users (stadium operators/owners)), as they are responsible for the lawfulness of the processing. According to the principle of accountability, the controller must at any time be able to demonstrate that there is a sound legal basis to its data processing and that the data protection principles are respected.

Article 18 of the GDPR gives data subjects the right to seek the temporary restriction of processing. Data subjects can request the data controller to restrict processing where:

- the accuracy of the personal data is contested;

- the processing is unlawful and the data subject requests that the use of the personal data be restricted instead of erased;
- the data must be kept for the exercise or defense of legal claims; or
- a decision is pending on the legitimate interests of the data controller prevailing over the interests of the data subject.

The methods in which a data controller can restrict personal data processing can include, for example, temporary movement of the selected data to another processing system, making the data unavailable to users or the removal of personal data on a temporary basis[80].

Furthermore, data subjects can exercise the right to object to personal data processing on grounds relating to their particular situation. As clarified in Recital 69, data subjects do not have a general right to object to the processing of their data. Article 21 (1) of the GDPR empowers them to raise objections on grounds relating to their particular situation where the legal basis for the processing is the controller's performance of a task carried out in the public interest, or where the processing is based on the controller's legitimate interests.

In the context of EVAGUIDE, it is reasonable to assume that in some cases end-users (stadium operators/ owners) in their capacity as data controllers might be required by national law to process the data or it may be necessary for the performance of a task carried out in the public interest or exercise of official authority vested in the controller. The notion of public interest is also a very broad one and will have to be interpreted in the context of the specific processing activity.

Finally, it has to be noted that the GDPR tries to balance the rights of data subjects with the requirements of scientific, statistical or historical research with specific safeguards and derogations in Article 89. The European Union or Member State law may provide derogations of the right to object insofar as such right is likely to render impossible or seriously impair the achievement of the research purposes, and if such derogations are necessary for the fulfilment of those purposes.

[80] See GDPR, Recital 67.

4 ELEMENTS OF COMPLIANCE

4.1. Data Protection Impact Assessment

As a historical descendant to environmental and technology impact assessments and sharing similarities with Security Risks Assessments and Privacy Impact Assessments, which progressively developed from the 1990s, the Data Protection Impact Assessment[81] is expected to form another tool for better monitoring and ensuring compliance with the GDPR. In this perspective the introduction of Data Protection Impact Assessments as requirement is one on the innovative elements of the Regulation that may serve to respond also proactively to unforeseen technological challenges and anticipate and/or mitigate the respective risks.

Anyone who processes personal data has a duty, deriving at least from the data minimization principle, to assess purposes, means and risks involved. This assessment becomes mandatory when the planned processing is likely to pose "a high risk" to individual's fundamental rights and freedoms. As indicated in the Article 29 Data Protection Working Party (WP29) Statement (14/EN WP 218), the reference to "the rights and freedoms" of the data subjects primarily concerns the right to privacy, but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion[82]. This approach has been reinforced by the Declaration of the 40th International Data Protection Authorities (DPAs) Conference that acknowledges the need for data protection and privacy authorities to think about human rights more broadly[83].

The text of the Regulation does not define what is understood under "high risk". According to Recital 75 "*a risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where*

[81] As PIA is defined as "a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative which involves the processing of personal information and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts" . See D. Wright and P. De Hert (eds.), Privacy Impact Assessment 2012

[82] Article 29 DPWP Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

[83] See 40th International Conference of Data Protection and Privacy Commissioners, DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE, October 2018.

processing involves a large amount of personal data and affects a large number of data subjects". The Privacy and Data Protection Commissioners state that by assessing the risks one should take into consideration the collective impact that the use of Artificial Intelligence (AI) may have on groups and on society at large[84].

Recital 76 clarifies when a risk is assessed "the likelihood and severity of the risk … should be determined by reference to the nature, scope, context and purposes of the processing". In order to identify a risk as "high", it has to be evaluated "on the basis of an objective assessment". The cases that a "high risk" could occur are indicatively listed in the Regulation, which refers to the "use of new technologies" also "taking into account the nature, scope, context and purposes of the processing" (Article 35 par. 1). In this context Article 35 (par. 3) defines the cases that definitely fall under the category of "high risk" these pertain:
a) to profiling or to any "systematic and extensive evaluation of personal aspects" and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person[85];
b) the processing on a large scale of special categories of data[86] or data related to criminal convictions and offences (sensitive data); or
c) the large-scale monitoring of a public area (par. 2).

According to Article 29 Data Protection Working Party, a DPIA has to be carried out, in case of systematic monitoring, e.g. processing used to observe, monitor or control data subjects, including data collected through "a systematic monitoring of a publicly accessible area" (Article 35(3)(c)). This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).[87]

The GDPR does not specifically define the notions of 'systematic monitoring' or 'large scale'. According to the Recital 91, large-scale processing operations "aim to process a considerable amount of personal data at regional, national or supranational level … which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights". Particularly, a data protection impact assessment is necessary when monitoring

[84] See 40th International Conference of Data Protection and Privacy Commissioners, DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICAL INTELLIGENCE, October 2018.
[85] See Recital 71 that clarifies ""in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles".
[86] These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9 par.1).
[87] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (2017).

publicly accessible areas using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale

A DPIA seems to be mandatory also in cases of Innovative use or applying technological or organisational solutions. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown.

The GDPR provides that the supervisory authorities (and the EDPB) must adopt and publish a list of the kind of processing operations that need to be subject to impact assessments. They may also establish a list of processing operations exempted from this obligation. That means that data controllers have to take into consideration also these lists to decide if they are subject to a mandatory DPIA, e.g. the have to check compliance with decisions and other acts of the national supervisory authorities which might classify certain operations as posing 'high risks' per se. In cases where it is unclear whether a data protection impact assessment is required, the Article 29 Working Party recommends carrying out such an assessment because it is "a useful tool to help data controllers comply with data protection law".[88]

The GDPR provides a process-oriented approach to risk and high risk by enumerating the steps to be taken, including the necessary consultation. A data protection impact assessment should include the following as a minimum:

a) a systematic description of the process, its purpose and which justified interest it protects;
b) an assessment of whether the process is necessary and proportional, given its purpose;
c) an assessment of the risk that processing involves for people's rights, including the right to privacy; and
d) the measures selected for managing risk identified.

They have to identify the impact of the use of such systems for the rights and liberties of persons, with focus on right to privacy and data protection and where an impact assessment is required, controllers must assess the necessity and proportionality of the processing and the possible risks to the rights of individuals. The impact assessment must also contain the planned security measures to address the risks identified.

The Garante, the Italian Data Protection Authority, has proposed that it is useful to follow the approach adopted by ENISA (the EU Agency for Network and Information Security), which in turn builds on the widely accepted standard ISO 27005: "Threats abuse vulnerabilities of assets to generate harm for the organisation"; and to consider in more detailed terms risk as being composed

[88] Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679 (2017)

of the following elements: Asset (Vulnerabilities, Controls), Threat (Threat Agent Profile, Likelihood) and Impact[89].

As also outlined by the Garante, a proper risk assessment involves four steps:

1) Definition of the processing operation and its context;
2) Understanding and evaluation of impact;
3) Definition of possible threats and evaluation of their likelihood (threat occurrence probability);
4) Evaluation of risk (combining threat occurrence probability and impact).[90]

The DPO should keep full records of all these risk assessments, and of such advice. These records have to demonstrate that processing is performed in accordance with the GDPR and with national legislation, if there is such a specific provision (accountability principle).

Whether the system falls within the ambit of the any of the situations described in the indicative list in the GDPR, depends on the particular scenario. In the context of EVAGUIDE project, which is a two year research project, the DPIA is not mandatory as the EVAGUIDE system will be tested in a "closed" environment, with selected and limited number of volunteers that will explicitly give their consent in participating in the three (3) pilot demonstrations and evacuation scenarios (Deliverable 6.1 - H Requirement, No 3 - Templates of the Informed Consent/Assent Forms and Information Sheets).

The Informed Consent Form will be written in a language and terms that the volunteers can understand, and will describe the aims, methods and nature of the participation and any benefits, risks or discomfort that might ensue. Also, the consent form will explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time – without any consequences. An option for the volunteers will also be included in the consent form in order to agree whether the forms can be retained post project for a period, for any post follow up by the partners. It should be noted that under no circumstances will vulnerable data subjects be selected as an EVAGUIDE volunteer; this includes persons under the age of 18 and any other person unable to give the informed consent. The only reason to involve volunteers is the demonstrations is to provide valuable insights in the evaluation process and to test the system results and (e.g. reduce the evacuation time).

Furthermore in Deliverable 6.2 a thorough description of technical and organizational measures that will be implemented to safeguard the rights and freedoms of the data subjects/ research participants have been elaborated and also on Deliverable 6.3 a description of the security measures that will be implemented to prevent unauthorized access to personal data or equipment used for processing have

[89] See Douwe Korff & Marie Georges, The DPO Handbook - Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation, 2019 and also ENISA Threat Landscape Report 2016, Figure 4: The elements of risks and their relationships according to ISO 15408:2005, https://www.enisa.europa.eu/publications/enisa-threat-landscapereport-2016. See also its 2017 report, https://www.enisa.europa.eu/publications/enisa-threatlandscape-report-2017

[90] Giuseppe d'Acquisto, presentation to the first "T4DATA" training session on data security, June 2018

been submitted. The results of the above mentioned deliverables will be updated, if needed, during the project.

Nevertheless, when the EVAGUIDE system becomes commercially available, is installed and fully operational in the premises of a stadium or large facility, it is reasonable to assume that a DPIA will be required to be carried out by the facility owners/ operators, to identify risks that pose for rights and liberties of individuals entering the facility, both the video surveillance activities and the use of EVAGUIDE apps.

If the case of video-surveillance installed and used for purposes of safety and emergency management, the data controllers (researchers/ end-users) should carefully and concretely evaluate risks. In this respect they have to identify in detail the types of security incidents that are expected to occur in the area under surveillance and that they wish to deter, prevent, investigate or prosecute using the cameras. They should not simply identify any security risks that may potentially exist but must also justify, in a realistic and verifiable manner, the existence and extent of those risks (specific safety dangers). This risk analysis should be documented in writing and should identify and assess any existing risks.

According to the EDPS's Guidelines, introduction of "high-tech video-surveillance tools" or "intelligent video-surveillance systems" are permissible only subject to an impact assessment. One of the examples enumerated refers to the capability of such systems for the data in the images to allow automated searches and alerts (e.g. for tracking individuals) or a network of cameras installed, complete with a tracking software application that can track moving objects or people throughout the whole area.

The GDPR does not specify which DPIA process must be followed but instead allows for data controllers to introduce a framework which complements their existing working practices provided it takes account of the components described in Article 35(7). As noted by the Article 29 DPWP in its Guidance on DPIA, such a framework can be bespoke to the data controller or common across a particular industry (p.20). The Article 29 DPWP provides also examples of EU generic frameworks. Standards like the ISO/IEC 29134:2017 may provide helpful guidance. The ISO/IEC 29134:2017 "Guidelines for privacy impact assessment" standard aims to provide detailed directions for the privacy impact assessment process and the structure of its report.

At any event, the impact assessment ought to be drafted prior to undertaking such processing. However, it has to take into consideration that - as significant element of such assessments is the continuity of the evaluations, which follow the processing / application during their entire life-cycle - a DPIA has to be updated, when new features or modifications are introduced or new purposes are pursued.

Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)), carrying out a DPIA in an incorrect way (Article 35(par. 2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can each result in an

administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher[91].

4.2. DATA PROTECTION BY DESIGN

The GDPR recognizes the contribution of technology to the transformation of economy and social life and the need to facilitate the free flow of data, "while ensuring a high level of the protection of personal data" (Recital 6). Data protection by design falls between the responsibilities of controllers, referring mainly to the concept that information and communications technologies and systems should be designed and also operated as taking data protection by design into account, even from the outset, as a default setting[92]. The article 25 par. 1 requires the data controller to implement -both at the time of the determination of the means for processing and at the time of the processing itself- appropriate technical and organisational measures, which are designed to implement data-protection principles and to integrate the necessary safeguards into the processing in order to meet the requirements of the Regulation[93].

Data Protection by Design, like its "ancestor" Privacy by Design, is not a new concept: it embraces a practical approach that orientates the entire life cycle activities pertinent to a technology or system- from research, design, development, implementation, use and disposal – towards the embedment of privacy and data protection into the design of the technology or system. Another concept, Privacy in Design is closely related with Privacy by Design. Privacy in Design emphasizes on raising awareness about the processes through which values and norms become embedded in the technological architecture[94].

Like the performance of data protection impact assessments, the requirement of data protection by design underlies that risk awareness and a precautionary approach are crucial for addressing the challenges of new technologies. If Data Protection Impact Assessments have been suggested as a useful tool for engineers and software developers to help them to consider potential negative consequences of particular elements of a technology design, data protection by design enables the adaptation of the data protection framework to technological developments and, vice versa, the embedment of data protection principles in technological products and apps.

[91] See Article 29 DPWP, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.
[92] Attila Kiss and Gergely László Szoke, Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation IN Reforming European Data Protection Law.
[93] Data protection by design has regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data.
[94] According to the European Group on Ethics, privacy in design refers to the Constructive Technology Assessment (CTA), which was developed in the Netherlands and Denmark. CTA focusses on broadening design, development, and implementation processes. This model emphasizes the early involvement of a broad array of actors to facilitate learning about technology and its potential impacts. See European Group on Ethics in Science and New Technologies to the European Commission, Ethics of security and surveillance technologies - Opinion no. 28, 2014.

A serious limitation of the obligations of Article 25 is that they apply only to impose an obligation on controllers and not to the developers of those products and technology used to process personal data. The obligation for products and technology providers is not included in the substantial provisions of the GDPR. However, Recital 78 of GDPR states that "*When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations...".* Thus, the application of Article 25 would require the provider to design their products in such a way as to enable the controller to put in place all the necessary measures needed to protect the individuals and their data, and configure them in a way that by default, without any user intervention, no personal data at all are collected or at least only those that are strictly necessary to carry out what can be expected from the basic utilisation of that product. This is especially important for EVAGUIDE project as partners act both as joint controllers and developers.

According to Article 29 Data Protection Working Party, the measures that have to be adopted to build in data protection requirements should be implemented both at the time of processing and when determining the means for processing. In implementing these measures, the controller needs to take into account the state of the art, the costs of implementation, the nature, scope and purposes of personal data processing and the risks and severity for the rights and freedoms of the data subject. [95] According to EDPS, the state of the art of available technology and the cost of implementation of the measures, must not beinterpreted in such a way that the measures chosen do not sufficiently mitigate existing risks and the resulting protection is not adequate.
Data protection by design must consider the whole life cycle of a service or a product, from initial planning to service/product disposal. Adequate governance and management structures and procedures in the organisationare then needed to enable the overall approach.

In the view of the EDPS[96], "data protection by design" has several dimensions;

- the first dimension is that personal data processing operations should always be the outcome of a design project, covering the whole project lifecycle, within which the data protection risks and requirements should be clearly identified;
- the second dimension is that the design project should be based on a risk management approach, within which the assets to be protected are the individuals whose data are to be processed and in particular their fundamental rights and freedoms;
- the third dimension is that the measures to be taken to protect those individuals and rights and freedoms must be appropriate and effective in relation to those risks, viewed in the light of the data protection principles set out in Article 5 GDPR, which can be seen as goals to achieve;

[95] See Article 29 Working Party (2017), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 4 October 2017.
[96] EDPS, Preliminary Opinion on privacy by design (Opinion 5/2018), issued on 31 May 2018

- the fourth dimension is the obligation to integrate the identified [necessary, appropriate and effective] safeguards into the processing.

The EDPS considers all four dimensions as equally important and an integral part of accountability and as such subject to supervision from the competent data protection supervisory authorities.

The EDPS suggests some methodologies for translating legal principles into actionable requirements. The main goals and elements of "privacy engineering" to identify safeguards for IT systems processing personal data consist of the classical IT security triad of confidentiality, integrity and availability, and "unlinkability"[97], "transparency"[98] and "intervenability"[99]. On top of the classical security objectives (confidentiality, integrity and availability) the US NIST[100] adds as engineering objectives the predictability[101], manageability[102] and disassociability[103].

Incorporating data protection by design and data protection by default principles in all of the controller's data processing operations, products and services, at each step, from their conception through to their actual operation reflects a general data protection culture and approach[104].

As already stated in D.6.2., of particular significance to the EVAGUIDE consortium is Article 32 of the GDPR, which requires data controllers to protect personal data against a variety of risks through the adoption of appropriate technical and organisational controls. Specifically, these controls must be incorporated into the design of the processing system and also the processing itself. This means that security cannot simply be added on to data systems but must be built in.

4.3. Accountability as element of compliance

The GDPR introduced among the principles relating to processing of personal data the principle of accountability that implies that data controllers are responsible and must be able to demonstrate compliance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and security (confidentiality and integrity). Accountability as laid down in Articles 5(2) and 24 GDPR is a key element to drive the effective implementation of data protection principles.

Accountability has two main aspects. On one hand, it serves as a tool which ensures that the data controller respects the provisions of data protection in the course of each and every data processing operation and that data subjects can exercise effectively their rights. On the other hand, pursuant to

[97] Unlinkability" relates to the ability of pieces of information to be related to each other and to an individual

[98] "Transparency" implies that all privacy-relevant data processingincluding the legal, technical, and organizational setting-can be understood and reconstructed at any time

[99] "Intervenability" enables the effective enforcement of changes and corrective measures

[100] NIST, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", Special Publication 800-122, April 2010.

[101] Predictability is about enabling reliable assumptions by individuals, owners and operators about PII and its processing by an information system.

[102] Manageability" means providing the capability for granular administration of PII including alteration, deletion, and selective disclosure, which are essential for proper personal data management

[103] "Disassociability" enables the processing of PII or events without association to individuals or devices beyond the operational requirements of the system. This privacy objective clearly focuses on minimisation of personal data and possible anonymisation.

[104] D. Korff and M. George, The DPO Handbook, 2019

the principle of accountability, the data controllers are obliged to demonstrate this compliance upon request by the relevant data protection authorities.

Accountability obligations are specified in a number of provisions, for instance on security, on a register of processing operations, on data protection by design and default, as well as on ex ante data protection impact assessments for processing operations with a high risk for the individual. A reflection of the principle of accountability could be seen in the conditions for consent established by Article 7 GDPR that requires, among others, that the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

As noted by Hijmans[105], a general feature of accountability is that data controllers are relatively free in the means they choose, but that they should consider the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Data controllers should put in place internal mechanisms and implement practical tools for more effective data protection from the outset. The mechanisms should be in place throughout the whole processing activity, thus implying that accountability should be "an ongoing activity".

As measures that take account of the principle of accountability can be considered, more specifically, identification of data processing operations, response to access requests, allocation of resources, designation of individuals responsible for the organisation of data protection compliance, such as data protection officers etc. It is also important to be able to demonstrate compliance with the data protection requirements, e.g., by maintaining sufficiently well documented records. Records should be maintained of personal data and processing activities in order for actions to be traceable and publicly liable. In addition, records should be maintained of the decision-making schemas and actions that lead to exceptional data processing actions.

Pursuant to the Article 29 Working Party opinion[106], 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. The Article 29 Working Party has recognised data protection impact assessment as an "important tool for accountability" and an enabler for data controllers to both comply with the regulation's requirements and demonstrate that appropriate measures have been taken[107].

[105] See Hielke Hijmans Data Protection and Surveillance: The Perspective of EU Law. Draft (October 2018) of Paper Written for: Proceedings from 2018 ECLAN Conference
[106] Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability.
[107] Article 29 Data Protection Working Party, Article 29 DPWP Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

5 Summary

The objective of this deliverable is to identify whether there are potential ethical and data protection issues that need to be addressed under the EVAGUIDE project. All data will be gathered on the relevance of ethical issues and the protection of citizens' rights, while engaging the end users of the system (facility owners/ operators) in a dynamic process of data handling, for the purposes of safe evacuation in their facilities.

The deliverable also examines to what extent the EVAGUIDE system will affect the ethical, privacy and data protection rights of data subjects, during the duration of the project and after its closure, as a commercial product. Special attention also paid to the new personal data protection EU Regulation - GDPR

Taking into consideration the data protection principles and the requirements as embedded in EU law and mainly in the GDPR, the app developers, the researchers and the end-users of crowd/ disaster management systems (facility owners/ operators), should proceed to the respective data collection / processing, while taking into account:

- The need to identify the **proper legal basis for the processing** – In this context it has to be considered that while for downloading of the app in the research phase, users' consent may be sufficient, for the subsequent processing of the personal data, a separate legal basis may be required. If consent is the applicable legal basis, then it must be freely given, specific and informed. Which legal basis will be regarded as appropriate depends on a context, such as the particular emergency situation and the end-users involved.
- The compliance/need to comply with the purpose **specification principle** thus defining clearly and narrowly the purpose(s) of each application and limit usage of personal data to the identified purpose (purpose limitation principle).
- The compliance/need to comply with the **principle of transparency** thus ensuring especially that operation of the app and the respective data processing should be transparent all the times.
- The compliance/need to comply with the **principles of accuracy and data minimization** to ensure the quality of data and to not interfere with rights and freedoms of affected individuals by processing data in such an extent that it is neither necessary nor proportionate. A data controller must justify the **necessity and proportionality** of each operation.
- The respect for data subjects' rights, in particular, the **right to information, rectification, erasure, blocking and objection**. There must be adequate, effective and transparent procedures, available to the end-users of apps at any moment.
- The **assessment of the level of risks** deriving from data processing for the rights and freedoms of individuals and the data protection impact assessments to identify and mitigate risks.
- The necessary technical and organization security measures to ensure the **confidentiality and integrity of data** and processing and adopt an internal security policy, which entails also procedures to handle data breach incidents.