Project acronym: CRISP
Project title: Evaluation and Certification Schemes for Security Products

Grant number: 607941
Programme: Seventh Framework Programme for Security
Objective: Topic SEC-2013.5.4-1 Evaluation and certification schemes for security products
Contract type: Capability project
Start date of project: 01 April 2014
Duration: 36 months
Website: www.crispproject.eu

D.4.1.
Legal Analysis of Existing Schemes

Authors: Irene Kamara, Paul de Hert, Alessia Tanas, Ioulia Konstantinou, Rosamunde van Brakel (Vrije Universiteit Brussel- LSTS), Cristina Pauner, Jorge Viguri, Artemi Rallo, Rosario García (Universitat Jaume I-UJI), Florian Fritz, Roger von Laufenberg (Vienna Centre for Societal Security- VICESSE), Eva Kalan, Jelena Burnik (Information Commissioner - Republic of Slovenia-IP-RS)

Dissemination level: Public
Deliverable type: Final
Version: 1
Submission date: 30 April 2015
Table of Contents

Table of Contents ........................................................................................................... 2
Tables and Figures ........................................................................................................... 6
Abbreviations .................................................................................................................. 7
EXECUTIVE SUMMARY ................................................................................................. 8
1 INTRODUCTION .......................................................................................................... 10
  1.1 Methodology .......................................................................................................... 11
    1.1.1 General Overview of Research and Analysis Methods ..................................... 11
    1.1.2 STEFi Dimensions ............................................................................................ 13
    1.1.3 Limitations and challenges .............................................................................. 14
  1.2 Brief Overview of Security Standardisation Landscape ....................................... 15
    1.2.1 CRISP Reports .................................................................................................. 15
    1.2.2 Mandate 487 .................................................................................................... 16
2 LEGAL ASPECTS OF CERTIFICATION AND EVALUATION SCHEMES ............ 18
  2.1 Introduction .......................................................................................................... 18
  2.2 Overview of Relevant Legislation to Accreditation and Certification .................. 18
    2.2.1 The New Approach ......................................................................................... 18
    2.2.2 The New Legislative Framework .................................................................... 19
  2.3 Soft Law .............................................................................................................. 20
    2.3.1 The ISO/IEC 17000 standard ......................................................................... 20
    2.3.2 The ISO/IEC 17067 standard ......................................................................... 21
    2.3.3 CEN, CENELEC and ETSI guidance ............................................................... 22
  2.4 Conclusions .......................................................................................................... 23
3 LEGAL STUDY ON SECURITY ASPECT OF SECURITY PRODUCTS, SYSTEMS AND SERVICES: MAPPING LEGISLATION AND LEGAL DEMANDS FOR SECURITY PRODUCTS, SYSTEMS, SERVICES IN THE EU ......................................................... 24
  3.1 Introduction .......................................................................................................... 24
  3.2 Security of Citizens .............................................................................................. 25
    3.2.1 Terrorism ......................................................................................................... 25
    3.2.2 Common Crime ............................................................................................... 26
    3.2.3 Civil Aviation Security .................................................................................... 26
3.2.4 Safety of Equipment ................................................................. 28
3.3 Security of Critical Infrastructures ............................................. 30
  3.3.1 European Critical Infrastructures ........................................... 31
  3.3.2 Aviation Security ................................................................. 32
  3.3.3 Maritime Security ................................................................. 36
  3.3.4 Port Security ....................................................................... 38
  3.3.5 Rail Security ....................................................................... 39
  3.3.6 Information Security ............................................................. 40
3.4 Border Security ........................................................................ 43
  3.4.1 Schengen Area ................................................................... 43
3.5 Crisis Management .................................................................... 45
3.6 Conclusion ................................................................................ 45
4 LEGAL STUDY ON TRUST ON SECURITY PRODUCTS, SYSTEMS AND SERVICES ................................................................. 47
  4.1 Legislation Related to the Concept of Trust .................................. 47
  4.2 Trust Issues connected to security products and services ............ 53
  4.3 Citizens’s Voice on Trust Issues of Security Products .................. 55
  4.4 The Role of Evaluation and Certification schemes in Addressing the trust issues of Security Measures ............................................. 57
  4.5 Conclusion ................................................................................ 61
5 LEGAL STUDY ON EFFICIENCY ASPECT OF SECURITY PRODUCTS, SYSTEMS AND SERVICES ................................................................. 63
  5.1 Efficiency from a Legal Perspective ............................................ 63
  5.2 Efficiency and Drones, CCTV, Alarm systems ............................. 65
  5.3 Conclusion ................................................................................ 68
6 LEGAL STUDY ON FREEDOM INFRINGEMENT IN THE CONTEXT OF SECURITY PRODUCTS, SYSTEMS AND SERVICES ................................................................. 69
  6.1 Privacy and Personal Data Protection ......................................... 69
    6.1.1 The right to private life and the core legal requirements for security products, systems, services ............................................. 69
    6.1.2 The right to the protection of personal data ............................. 75
    6.1.2.1 The Data Protection Directive in the context of Security Products, Systems and Services ............................................. 75
6.1.2.2 Core Requirements applicable to Security PSS from the General Data Protection Regulation ..........................................................81
6.1.2.3 ePrivacy Directive and Security Products, Systems and Services .............. 84
6.1.3 Impact of Security Employed Technologies on Privacy and Data Protection ... 84
6.1.3.1 Impact of CCTV systems on the right to privacy and data protection ........ 84
6.1.3.2 Impact of drones on the right to privacy and data protection .................. 88
6.1.3.3 Impact of biometrics of alarm systems on the right to personal data protection 93

6.2 Bodily Integrity ........................................................................................................... 96
6.3 Equal Treatment and Non-discrimination .................................................................. 100
6.3.1 Direct and indirect discrimination ........................................................................ 101
6.3.2 Differential Treatment .......................................................................................... 102
6.3.3 Protected grounds of non-discrimination and Security PSS ............................ 102
6.4 Freedom of Movement and Freedom from Unlawful Detention ................................ 104
6.5 Presumption of Innocence .......................................................................................... 109
6.6 Fair Trial and Due Process ......................................................................................... 114
6.6.1 The right to a fair trial ......................................................................................... 114
6.6.2 “Due Process” Rights ......................................................................................... 116
6.7 Conclusion .................................................................................................................. 117

7 LEGAL ANALYSIS OF SCHEMES ............................................................................ 120
7.1 Criteria for General Analysis of Schemes Operating in the EU ............................ 121
7.2 Presentation of analysed schemes operating in the EU ........................................ 122
7.2.1 Alarm systems ....................................................................................................... 122
7.2.1.1 VdS Guidelines for Alarm Systems – Biometric recognition procedures: Requirements and Test Methods ......................................................... 122
7.2.1.2 PSA Licensing Requirements for Door Supervision and Security Guarding 122
7.2.1.3 Code of Practice for Scaffold Alarm Systems (SAS) ....................................... 124
7.2.2 CCTV Systems ........................................................................................................ 124
7.2.2.1 Code of Practice for the Cambridge City Council’s Public CCTV Scheme 124
7.2.2.2 Warwick District Council Code of Practice for CCTV Scheme ................. 125
7.2.2.3 Community-Based CCTV Scheme of the Irish Department of Justice, Equality and Law Reform .......................................................... 126
7.2.2.4 NSAI Technical Annex TA-50132 for CCTV Installers ............................... 127
D4.1: Legal Analysis of Existing Schemes

7.2.2.5 EQA Scheme Regulations.................................................................128
7.2.3 Unmanned Aerial Vehicles (drones).....................................................128
7.2.3.1 JARUS Certification Specification for Light Unmanned Rotorcraft Systems 128

7.3 Criteria for Legal Analysis of Schemes Operating in the EU ......................129
7.3.1 Criteria for Security Aspect ...............................................................129
7.3.2 Criteria for Trust Aspect .................................................................131
7.3.3 Criteria for Efficiency Aspect ............................................................135
7.3.4 Criteria for Freedom Infringement Aspect ..........................................137

7.4 Analysis of Existing Schemes on The Basis of STEFi aspects .....................141
7.5 Security Assessment of Existing EU Schemes .........................................142
7.6 Trust Assessment of Existing EU Schemes ............................................143
7.7 Efficiency Assessment of Existing EU Schemes ......................................146
7.8 Freedom Infringement Assessment of Existing EU Schemes ....................148
7.9 Key Findings of Legal Analysis of Schemes operating in the EU ..............154

8 CONCLUSIONS ............................................................................................158
9 REFERENCES ..............................................................................................161
Tables and Figures

Table 1: Counter-Terrorism Legislation in the European Union
Table 2: Requirements for equipment and protective systems – new ATEX Directive
Table 3: European Critical Infrastructure sectors
Table 4: Requirements for Security Equipment for Civil Aviation Security according to Commission Regulation (EU) No 185/2010
Table 5: Normative on legal obligations related to trust
Table 6: Normative on the right to private life
Table 7: Responsiveness of the existing schemes to the core legal requirements of the STEFi dimensions based on type of scheme
Table 8: Responsiveness of the existing schemes to the core legal requirements of the STEFi dimensions based on type of security measure
Table 9: Responsiveness of the existing schemes to the core legal requirements of the STEFi dimensions based on issuing body
Table 10: Overview of WP4 case studies and related freedom infringements

Figure 1: Process of certification - ISO/IEC: 17000:2014
Figure 2: Operationalisation of Civil Aviation Security core legal requirements
Figure 3: Operationalisation of Safety Equipment core legal requirements
Figure 4: Operationalisation of Aviation Security core legal requirements
Figure 5: Operationalisation of Maritime Security core legal requirements
Figure 6: Operationalisation of Information Security core legal requirements
Figure 7: Security measures of SIS II
Figure 8: Consumer Trust Assessment Framework
ABBREVIATIONS

CCTV: Closed Circuit Television System
CJEU: Court of Justice of the European Union
DEL: Project Deliverable
DPA: Data Protection Authority
DPD: Data Protection Directive 95/46/EC
DoW: CRISP Description of Work
ECHR: European Convention of Human Rights
ECtHR: European Court of Human Rights
ECI: European Critical Infrastructure
EDPS: European Data Protection Supervisor
EN: European Standard
ESOs: European Standardisation Organisations
GDPR: (draft) General Data Protection Regulation
ISO: International Organisation for Standardisation
NLF: New Legislative Framework of 9th July 2008
OJ: Official Journal of the European Union
PSS: Product, system, service
RPA: Remotely Piloted Aircraft
SIS: Schengen Information System
STEFi: Security, trust, efficiency, freedom infringements
TFEU: Treaty on the Functioning of the European Union
UAV: Unmanned Aerial Vehicle
VIS: Visa Information System
WP: Work Package
WP29: Article 29 Data Protection Working Party
EXECUTIVE SUMMARY

This Report is one of the deliverables for Work Package 4 (WP4) “Analysis of core dimensions, security, trust, efficiency and freedom infringements (STEFi)” of security products, systems and services (PSS). The Legal Analysis of Existing Schemes Report aims to analyse the core issues of each of the STEFi dimensions and determine special requirements and legal demands for the security PSS.

The study on the legal framework on evaluation and certification schemes identifies the legislation applicable and soft law setting the best practices for certification in the EU. The lack of EU legislation for certification schemes is to a certain extent covered by the international and European standards and the guidance from standardisation bodies.

With regard to the security legal study, the EU and the Member States share competence in the area of security. The security legislation in the EU is sector-specific and provides useful insight as to requirements for security products and services. Demands relate to physical controls and training of personnel, as well as the performance and the functioning of the security equipment. The multi-layered risks of physical and digital nature urge for accountability, security and risk assessments. Access to information systems and prevention from illegal interception and interference to the data and systems are also significant requirements incorporated to the EU legislation.

In terms of standardisation and certification, trust means that the security PSS, among others, respects the legislation and fundamental rights, is technically reliable, efficient and transparent, and responds in a predictable and acceptable manner. The role of evaluation and certification schemes in enhancing the needs of the citizens can be crucial when it involves stakeholders, is reviewed regularly, is operated by an independent body and includes requirements that address the main concerns of the scrutinised in the auditing or evaluation procedure.

Looking at efficiency from a legal perspective, the case studies of this WP reveal significant challenges as to how the security PSS should operate and perform in order to balance investments and achieve the objective of security. Procedural economy, collective redress mechanisms, energy efficiency and adaptability to new technologies with the minimum cost possible are efficiency requirements for security PSS.

 Freedoms and fundamental rights of individuals are potentially at risk from the establishment and/or operation of security PSS in different environments by different entities such as public authorities, private legal persons or individuals. The impact of drones and CCTV systems in public spaces for crime prevention and detention to the right to privacy and data protection may include extended surveillance, panoptic effect, profiling, excessive collection of personal data, lack of notification to data subjects, lack of possibility to exercise data subject rights and others. Accordingly, biometric alarm systems pose risks to the rights to data protection and privacy, as well as others. Equal treatment and prohibition of discrimination, bodily integrity, presumption of innocence, due process and fair trial might be infringed by the security measures, either from the functionalities of the equipment itself or the use/abuse of
the security product. Similarly, security service providers might also infringe the above rights, when the safeguards for their protection are not respected. The study identifies core requirements for security PSS to respect the rights and freedoms and be in line with the protective framework.

Further, the Report examines to what extent the existing evaluation and certification schemes respond to the requirements identified in the legal studies of the previous chapters. Drawing lessons from the analysis of existing schemes, the type of entity operating the scheme and the type of the scheme (certification scheme, certification system, code of practice, technical specification) play a crucial role into determining the quantitative and qualitative integration of the STEFi requirements identified in the legal studies. Public authorities tend to prioritise trust and freedom infringement requirements, while certification and standardisation bodies, as well as the industry focus on security and safety requirements.

The impact of the STEFi dimensions to the function and performance, user acceptability and legal compliance of the security PSS and the difficulty to locate a scheme with a comprehensive approach to the core aspects of all the four dimensions, highlight the importance of the CRISP objective to develop an innovative evaluation methodology that integrates the security, trust, efficiency and freedom infringement assessment dimensions.

WP4 integrated the results from the previous Work Packages and in particular WP1 (Categorising security equipment, systems and services), WP2 (Review of standards, certification and accreditation for security products) and WP3 (Security certification stakeholder analysis). The findings from WP4 will be integrated in the WP5 (Developing and testing of the certification methodology), WP6 (Developing a Roadmap) and WP7 (Enhancing confidence in the new certification measures).
1 INTRODUCTION

This report is part of the Work Package 4, which focuses on the analysis of the core dimensions, security, trust, efficiency and freedom infringement (STEFi), with regard to security products, systems and services. The Work Package aims to analyse existing schemes and standards to identify evaluation criteria based on the four core dimensions and come up with requirements for further development, enhancement, adaptation and integration of evaluation and certification schemes of products used for security purposes. The Work Package also aims to identify and analyse core issues associated with certification.

The legal analysis report aims to analyse the core issues of each of the STEFi dimensions and determine special requirements and legal demands. The document consists of two main parts. The first part (Chapters 3-6) is the legal study conducted for each one of the four aspects defining the core requirements of the STEFi dimensions. The second part (Chapter 7), the legal analysis of schemes, assesses to what extent the existing evaluation and certification schemes respond to the core requirements.

In more detail, the report is developed as follows:

**Chapter 1** introduces the reader to the aims, background, methodology and scope of the research.

**Chapter 2** examines legal aspects of certification in terms of normative documents and soft law.

**Chapter 3** presents the legal study on security. It outlines the core legislation of several areas of security in the EU, in principle focusing on identifying the legal demands and special requirements for security products, systems and services.

**Chapter 4** includes the legal study on trust. The chapter focuses on identifying the trust issues connected to security products and services and suggests how they can be addressed by security evaluation and certification schemes.

**Chapter 5** develops the legal study on efficiency. The chapter examines three security measures, drones, alarm systems and CCTV systems for crime prevention and detention in public spaces from the efficiency perspective.

**Chapter 6** incorporates the legal study on freedom infringements. In particular it analyses how and under which circumstances the security products, systems and services might violate the bodily integrity, equal treatment and non-discrimination, freedom of movement and freedom from unlawful detention, presumption of innocence, fair trial and due process, privacy and data protection.

**Chapter 7** presents the results from the analysis of evaluation and certification schemes from a legal perspective. It examines to which extent the selected schemes correspond to the results of the legal study (recommendations, requirements and demands) and identifies good practices in existing schemes.
1.1 METHODOLOGY

1.1.1 General Overview of Research and Analysis Methods

The research in this report is based on the following methods:

**Literature review**

Desktop research of studies, papers, books, reports at international, European and national level. The review takes into account the important work of other research projects, such as IRISS, SIAM, PIAF, PRESCIENT, SAPIENT, DESSI etc. Also, the Mandate 487 and other key documents for security standardisation and certification form the fundamentals of the analysis.

**Legislation and jurisprudence**

The focus is mainly on the EU law and jurisprudence of the Court of Justice of the European Union. The rationale is that the aim of this report is to identify legal requirements and special demands in relation to security products, systems and services in the EU. Since the objective of CRISP is to develop a certification manual for the internal market, the EU legislation is the most relevant and applicable. With regard to freedom infringements study, case law and the legal texts (conventions, treaties) of the Council of Europe are also discussed and analysed. In limited cases, eg. Drones or CCTV, national legislation is analysed, due to the lack of such legislation at EU level.

**Interviews and communication with experts**

We conducted interviews and communicated with selected experts in the field in order to identify key topics and actual challenges of the issues related to security products, systems and services and their certification. The interviews provided us with substantial insight for several aspects of the analysis, especially in relation to the trust aspect.

**Analysis of standards and evaluation and certification schemes**

The analysis of existing schemes is substantial for the aim of CRISP. Analysing the existing schemes provides valuable knowledge on what are the core issues of current schemes, to

---


2 The personal and other data from the interviews and communication followed the CRISP guidelines on collection and processing of personal data and confidential information as in section 4.1. “Privacy/Confidentiality and data protection issues” (p. 76) of the Description of Work. In brief, the participants were informed on the research goals of the project in the form of a research brief and were given information about the contact details of the researcher (data controller), the purposes of the processing of their data and others. The participants provided informed consent prior to the processing operation as requested by the DoW. The researchers preserve the anonymity of the participants and stored securely and separately the personal data from the research data. Researchers comply with the principles of the Data Protection Directive 95/46/EC.
what extent they embrace the socio-legal aspects that CRISP promotes and what are the good practices that can be implemented by other schemes. The analysis of schemes, as it is explained in detail in the relevant section of this report, is based on general criteria and legal criteria. The general (minimum) criteria first introduce the scheme, its scope and objectives and examine what procedures the certification process employs (audit, issuance of certificate, renewal, etc.). The purpose is to identify core issues related to evaluation and certification schemes. The legal criteria on the other hand, are the result of the legal study in each one of the STEFi dimensions (see 1.1.2). The legal criteria operationalise the core requirements identified in the legal study in order to examine how the current schemes react to core minimum requirements. To a lesser extent, we analysed standards, where this could bring added value to the aim of the report.

Case studies

We selected three types of security measures for the evaluation and certification schemes: CCTV systems in public spaces for crime prevention and detention; unmanned aerial vehicles (drones); intrusion detection and access control alarm systems for private spaces. The criteria for the selection of the specific cases were mainly the following: 1) Coherence with the previous reports of CRISP, especially the Stakeholder Analysis report and the Reports of WP2- Review of standards, certification and accreditation for security products. 2) Stakeholders of CRISP identified the above three areas as of main interest during the CRISP Stakeholder workshop in December 2014. 3) Each case study has unique characteristics, but also overlapping ones. The focus is on the unique aspects. For example drones is a relatively new area for certification and it is interesting to see how the certification bodies approach the requirements for certification of drones. Drones, as CCTV systems, employ cameras. Since we examine the cameras in the context of the CCTV systems, this is not the focus in the case of drones (even though the impact on the rights, such as surveillance possibilities is discussed also for drones, since the surveillance capabilities are more enhanced in comparison to CCTV systems). The application of CCTV systems for crime prevention purposes on the other hand is a common security measure. In this case, the evaluation schemes are expected to be more advanced, accumulating the experience of years of practice. It was interesting therefore to see whether the existing evaluation and certification schemes implement the requirements of the STEFi aspects, i.e. to what extent they implement socio-economical and legal aspects. With regard to alarm systems, we examine the intruder prevention and access control alarm systems installed in private premises. The alarm systems, as the CCTV systems, are not new in the internal market. In this case it is also interesting to see the implementation of the STEFi aspects and requirements, but in a different context than the CCTV case study: in private spaces for intruder prevention. With regard to the freedom infringement aspect of the alarm systems, the focus is on the biometric recognition that many alarm systems employ, such as facial detection and recognition and fingerprints. Certainly, the security products, systems and services area is very broad and includes different technologies in different environments used for different purposes. The aim is not to be exhaustive, but to learn from the use cases and add to the general legal study.
1.1.2 STEFi Dimensions

As requested by the Description of Work of this Work Package, the analysis is based on four aspects: security, trust, efficiency and freedom infringement (STEFi)\(^3\). The STEFi methodology was first developed in the framework of the SIAM project in order to analyse the impact of security technologies in relation to these four aspects. Following the STEFi methodology as implemented in the SIAM project, in CRISP we aim to examine the four dimensions in relation to security products, systems and services, but an additional factor is added: the evaluation and certification of security products, systems and services. In that respect, the analysis of the STEFi dimensions in the legal analysis report, aims to examine the four dimensions of the security products, systems and services from a legal perspective in order to come up with requirements to enhance the existing schemes. For example, the legal analysis of freedom infringement aspect of STEFi reveals personal data processing operations by several security measures and the possibility of violation of the right to protection of personal data if the proper safeguards are not in place (by the manufacturer or the operator). The aim of the analysis here is to identify what are the safeguards that should be in place (data minimisation, purpose specification and purpose limitation etc.) and suggest that these requirements should be included in the evaluation and certification schemes.

In the context of CRISP, the STEFi dimensions shall be interpreted as follows:

**Security Dimension**

This dimension involves different aspects of security and safety. Security describes the functionality of a product in countering threats and reducing risks. It covers the questions of whether the product fulfils promises and expectations regarding its performance. Evaluation criteria, amongst others, are the detection rate, the false alarm rate and the impact of intended interference or environmental interference.

**Trust Dimension**

Trust encompasses the experience of the product provider as well as of the scrutinized in using the product. Beside the experience, the subjective perception defines the way in which a product achieves an appropriate acceptance level. Evaluation criteria for the Trust dimension include, for example, the degree of discrimination regarding the use of product and the potential physiological and psychological invasiveness of the product. For instance, health risks such as DNA damage associated with the ionising radiation used in body scanners or other effects such as claustrophobia and anxiety attacks.

**Efficiency Dimension**

Efficiency implies the economical dimension of the product in a broad sense. Product costs are not being considered as a suitable basis for security certification or standardisation, because they do not impact on the functionality of the product but are a criteria for buyers. But large investments in security technologies do have an indirect (derivative) impact on economic aspects of a company. The integration into existing systems for example is essential for companies investing in security products. The inclusion of the ability of

---

\(^3\) SIAM project (Security Impact Assessment Measures). SIAM was an EU-funded research project running between February 2011 and April 2013.
integration as a set of criteria for the assessment of such products also promotes the attempts of the EU in harmonising technological compatibility. A related field that should also be taken into account is the upgrade-ability and update-ability. Compatible systems will ensure that future technological developments will be following the set standards and can also be integrated in the existing system. Hence a continuous investment cycle will be established and security technologies can be up-to-date without the establishment of a complete new system, increasing their serviceable life.

**Freedom Infringement Dimension**

The freedom infringement dimension of security product evaluation depicts the impact of a product on the freedoms and rights of persons. One of the main impacts of security products and services is enhanced personal data collection, processing, sharing and retention. This affects the rights to privacy and data protection. Additionally, security and safety products have a tendency to affect other rights such as the right to self-determination, right to freedom of movement, right of association; these must all be taken into account in the evaluation of security products.

1.1.3 **Limitations and challenges**

This section describes the limitations of the analysis that follows in this report and highlights the main challenges the research team had to overcome during the research for the legal analysis report.

**Access to schemes**

The evaluation and certification schemes are copyright protected and quite often they cannot be accessed as they are a commercial “product” of the body that offers them. Limited information is usually available on the website of the body, but not the scheme itself. In certain cases, schemes were accessible for a small fee, but in most cases they were not available at all. In some other cases, only parts of the scheme were available, such as the rules of the scheme (normative part), but not the technical part. The research team has sent information requests to selected bodies in order to access to the documentation of the schemes. In many occasions, the contacted person was reluctant to grant access, for reasons of intellectual property rights, commercial secrets, confidential information, etc. Additionally, it is common that the certification scheme operator differs from the certification scheme owner, which adds to the complexity of the access to the documentation of schemes issue.

**Transparency of information**

With regard to the information relating to evaluation and certification schemes, the main source of information was the website of the certification body and relevant studies, reports and papers. The websites are not always up-to-date and differ substantially in the quantity and quality of information they provide.

**Applicability of legislation**

The legal analysis of schemes is a challenging task in terms of selecting the relevant legislation. The scope of the “security products, systems and services” operating in the internal market is broad and given the fragmentation of legislation, the research team decided to 1) focus on the EU legislation, since, as mentioned above, CRISP aims at facilitating a harmonised playing field for the European security industry 2) select key legislation that sets the framework of protection in the areas of security (e.g. civil aviation security, critical
infrastructures security, etc.) and has impact on the way the security PSS should operate or be used (e.g. data protection legislation, consumer protection legislation).

**Focus on core issues and requirements**
We identify the key requirements and demands in each of the STEFi dimensions. Instead of being exhaustive in analysing every possible legislative act, being selective based on what is relevant to CRISP objective and to security standardisation and certification, is the best approach since it gives instruments to the following Work Packages of CRISP to work with specific requirements. Additionally, an exhaustive list of requirements for the evaluation and certification schemes of security products, systems and services would not be possible to be implemented by a scheme. Being selective serves the aim of enhancing and further developing the schemes.

**Lack of harmonisation of evaluation and certification schemes**
Consequent to the lack of a common regulatory framework for certifications schemes, there is lack of harmonisation when it comes to certification schemes. The lack of harmonisation in structure and objective on the one hand is justified due to the free nature of the market. On the other hand, the lack of minimum requirements for the schemes in the EU leaves a quite considerable part of the market, unregulated and considerably open to abuse.

**Diverse terminology of schemes**
The research team also had to deal with diverse terminology in the evaluation and certification schemes. Not all schemes examined lead to certification. Quite often the interesting information for CRISP can be found in evaluation schemes, codes of practice or other documents. The common element of the examined documents is that prescribe requirements that should be accomplished by the security products, systems and services.

**Focal groups**
The main focus of this report is the individual that undergoes the security control. The “scrutinised” is the individual mostly affected by security measures, especially in relation to the societal aspects of STEFi that CRISP examines. A second group is the operator of the security measure, who is also affected for instance by how safe is the security PSS is, and a third the product or system manufacturer, particularly for the security and efficiency aspects.

**1.2 Brief Overview of Security Standardisation Landscape**

**1.2.1 CRISP Reports**
In this section, we briefly outline the work of the previous work packages of the CRISP project, as it a significant basis for the current report\(^4\),\(^5\),\(^6\),\(^7\). Starting with a glossary of security


\(^6\) Wurster Simone, Pohlmann Tim, Murphy Patrick, Fritz Florian, Von Laufenberg Roger, Kreissl Reinhard, Van Zetten Jolien, Garcia Mahamut Rosario, Pauner Christina, Rallo Artemi, Tanas Alessia, Van Brakel Rosamunde,
products, systems and services the D.1.1. of the CRISP project aimed at leading to a better understanding of PSS, their application areas and the core functionalities, as well as assisting with the development of criteria for that make the security PSS comparable. The glossary provides that a “security-related products, systems and services are all those PSS which serve a security function, or which in other words, give operators the capability to perform such functions”. According to the Glossary, it is the context that provides the characterisation of a PSS as security-related, and not other factors as for instance the technology as such of the PSS. Additionally, the deliverable proceeds into examining the functions of the security PSS, which are further divided into primitive (e.g. locate, track, etc.), connective (e.g. assess, identify, etc.) and performative functions (e.g. authorise, control, etc.).

The objective of the CRISP taxonomy was to produce a needs-based taxonomy for security products, systems and services on the market with the aim to categorise the security PSS. The deliverable placed particular stress on the classification through application areas, highlighting in parallel that an evaluation and certification scheme of products and systems will need to work across all security sectors. The taxonomy also showed that there are many services which serve more than one security functionalities, and as a result the context within which the security is seen, changes the meaning and the boundaries of the concept of “security”.

The CRISP Report on security standards and certification in Europe provides a comprehensive overview of the standardisation and certification landscape from a historical/evolutionary perspective. Starting from the state of the art in conformity assessment, standardisation and accreditation, the report further examines the general framework conditions in Europe at a general level (EU policies, key documents and reports) and at sector level within the work of the European and international standardisation organisations.

The CRISP Stakeholder analysis report, identified the primary and secondary stakeholders of security standardisation and certification in Europe and describes and analyzes the different needs of each group of stakeholders. The report also discusses the requirements of a harmonised approach for a European certification approach for security products, systems and services.

1.2.2 Mandate 487

The Commission programming mandate addressed to CEN, CENELEC and ETSI to establish security standards (Mandate M/487 of 17 February 2011) concerns the development of a work programme for the definition of European Standards and other standardisation
deliverables in the area of security\(^8\). The Mandate has an exclusively civil application and focuses on assisting the EU to ensure that security is better and consistently addressed in different security landscapes. The main objective of the Mandate is to increase the harmonisation of the European security market and reduce fragmentation with the establishment of a set of comprehensive European standards.

The Mandate highlights the importance of involving different stakeholders and operators, particularly end-users of security systems and SMEs. It emphasizes the need to take into account security measures in line with the security levels determined by public authorities and their underlying risk assessments, identifying security needs and secure interoperability schemes between the various nodes and centres for civil security in Europe dealing with law enforcement and crisis management. Similar needs from private perspectives should also be included.

As to the specific role of the standardisation activities related to security, the Mandate refers to the following sources: the ESRIF Report and its highlighted importance of an integrated approach to security; the Commission’s Communication on reaction to ESRIF pointing out the need for a prompt investing in an ambitious industrial policy for the security sector; the ECORYS Study on Competitiveness of the EU Security Industry recommending the development of new European and common international standards for security as a mean to reduce the security market fragmentation, which is leading to a lack of competitiveness of the Security European Industry; the Commission’s Communication Towards an increased contribution from standardisation to innovation in Europe underlining the contribution that standards could and should make to innovation (policy) and the Stockholm Programme inviting the Council and Commission to develop internal security strategy tailored to the real needs of users and focused on improving interoperability.

The Mandate strongly emphasizes the need to take into account the human factor issues, privacy concerns and identification of operator requirements for enhancing systems effectiveness. These should duly be taken into account, not forgetting transversal areas either. European Standardisation bodies are directly invited to ensure that the deliverables developed meet European legislative and other requirements, in particular as regards privacy and Intellectual Property Rights (IPR).

---

\(^8\) European Commission, Programming Mandate Addressed to CEN, CENELEC and the European Telecommunications Standards, M/487, Brussels, 17.02.2011.  
2 LEGAL ASPECTS OF CERTIFICATION AND EVALUATION SCHEMES

2.1 INTRODUCTION

Certification means guarantee of quality. In general, the supplier can assess and declare the conformity of its product to requirements of a normative document, such as a standard, by herself. Certification however is performed by third parties, independent certification bodies which after performing an audit, they issue a certification for compliance of a product, service or person with specific requirements. In that case, the impartiality and independence of the third party are crucial for the credibility of the certificate, which will be issued. It is the certification scheme, which sets the rules, requirements and methodology on how the process will take place and what the end result will be. The certification scheme may seek to provide the product with a certificate of compliance with a standard. It might be the case instead, that a scheme is based on other normative documents or legal provisions, or both.

There is a plethora of schemes certifying products, systems and persons. In 2009 the certification market worldwide was growing at around 25% per annum, with a worldwide cumulative total of 10 to 11 million. The market of security industry is not an exception, even though for certain areas of security the differentiation among the schemes is low due to the mandatory compliance with legislation and small margin for deviation.

There is not a formal procedure set by legislation for developing a scheme. The certification bodies determine their own processes, rules and schemes within the general legal frameworks and any contractual obligations. A factor which influences the content of the scheme is the content and the requirements of the standard or the other normative document, against which the scheme will assess the conformity of the product or service.

2.2 OVERVIEW OF RELEVANT LEGISLATION TO ACCREDITATION AND CERTIFICATION

2.2.1 The New Approach

Even though the New Approach does not contain specific provisions on certification schemes, it is an important legislative step, which changed the landscape of standardisation and indirectly certification in Europe. It is worth briefly mentioning therefore what the New Approach encompasses and what it means for the current state of play in the certification field.

The New Approach established the notion of harmonised standards. The essential safety requirements are prescribed in specific Directives, with which the products put on the market need to conform. The task of developing the technical specifications for the production and placing in the market of the products conforming to the Directives, is entrusted to the European Standardisation Organisations (ESOs). Quite substantial for the free market is the voluntary nature of the standards. The manufacturer can prove the conformity to the

requirements of the Directive in other ways, not necessarily being obliged to follow the practice suggested by the harmonised standard.

That possibility opened the way for the development of various certification schemes, seeking alternative ways to comply with the legislation. It also created a market for certification schemes that follow the requirements of the harmonised standards.

2.2.2 The New Legislative Framework

The New Legislative Framework (NLF) was adopted in Council on 9 July 2008 and published in the Official Journal on 13 August 2008. The NLF foresees measures to help the internal market for goods work better and to strengthen and modernise the conditions for placing a wide range of industrial products on the EU market.  

The NLF consists of three legal instruments of horizontal legislation:

- The Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to be incorporated whenever product legislation is revised.
- The Regulation (EC) No 764/2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC.

Among the main goals of the texts is to establish a policy for accreditation in order to evaluate the competence of testing laboratories, certification and inspection bodies. The value of accreditation lies in the fact that it provides an authoritative statement of the technical competence of bodies whose task is to ensure conformity with the applicable requirements.  

The European Commission suggested that the “accredited body” in the context of the Regulation 765/2008 is an organisation with a legal personality, and consequently natural

---

14 Recital 9 of Regulation (EC) 765/2008
persons are excluded from being accredited, as the latter would fail to meet the requirements laid down in the harmonised standards due to their lack of organisational structure\textsuperscript{15}.

2.3 SOFT LAW

As soft law in this context, we consider the normative documents and guidance of the stakeholders involved in the standardisation and certification process\textsuperscript{16}. The expertise of the bodies and the wide applicability have created a de facto status of acceptance in a worldwide level from both the industry and the users.

2.3.1 The ISO/IEC 17000 standard

The ISO/IEC 17000:2004 standard \textit{“Conformity assessment - Vocabulary and general principles”} provides the basic terminology for the conformity assessment framework and related activities\textsuperscript{17}. According to the standard, \textit{“certification is a third-party attestation related to products, processes, systems or persons”}, where attestation is \textit{“the issue of a statement, based on a decision following review, that fulfilment of specified requirements has been demonstrated”}. From the definitions of certification and attestation, five main elements can be extracted: review, fulfilment of requirement and demonstration, decision and issue of a statement.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{process_of_certification}
\caption{Process of certification - ISO/IEC: 17000:2014}
\end{figure}

Source: Own graph

Necessary for the certification process is the third party review. The party reviewing should be independent and impartial. The entity initiating the certification process by request to the

\textsuperscript{15} European Commission, DG Enterprise and Industry, CERTIF 2012-04 REV4 – The legal personality of accredited bodies – the case of natural persons, April 2014


\textsuperscript{17} ISO/IEC: 2004 standard \textit{“Conformity assessment - Vocabulary and general principles”}, 2004, \url{http://www.iso.org/iso/catalogue_detail.htm?csnumber=29316}
certification body needs to demonstrate the compliance of a product, service or person (in terms of proper training) with a normative document or requirements. The certification body then applies the certification scheme rules and procedures to review by auditing, testing or otherwise check whether the entity fulfils the requirements. In case the assessment result is that it conforms, then the certification body issues a statement in a form of a certificate which attests the conformity to the specific requirements.

The standard also proposes a functional model for conformity assessment systems. The proposed system has four stages, the selection, the determination and the review and attestation\(^ \text{18} \).

- The selection stage involves the selection of the object for conformity assessment.
- The determination stage involves activities such as testing, inspection, audit and peer assessment to determine whether the object of the assessment conforms to the requirements.
- The review involves the last check for the fulfilment of the requirements

Accordingly, in section A.4.3. of the ISO/IEC 17000:2004, the certification system or scheme is defined as “a conformity assessment system that includes selection, determination, review and finally certification as the attestation activity”.

\subsection{2.3.2 The ISO/IEC 17067 standard}

The ISO/IEC 17067:2013 standard on “Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes” uses the vocabulary of the ISO/IEC 17000\(^ \text{19} \). The standard further provides guidance on how schemes for product certification can be structured and managed. It identifies techniques for assessment that are used as a basis for product certification, such as product testing, inspection and auditing. The ISO/IEC 17067 replaced the Guide ISO/IEC 67 updating the conformity assessment framework and including product certification in its scope.

According to the standard (3.2.), a certification scheme is:

“A certification system related to specified products, to which the same specified requirements, specific rules and procedures apply”.

The standard presents six types of schemes, in which the selection, determination, review, decision and attestation stages differentiate according to the objectives of each scheme type. The scheme owner can be either a certification body that develops and operates the scheme or an organisation. In the latter case, one or more certification bodies participate in the scheme. In any of the cases, the certification scheme owner is a legal entity.

\begin{footnotesize}
18 CEN/CENELEC/PT, “Guidance for the application of conformity assessment to accessibility requirements for public procurement of ICT products and services in Europe,” August 2012

\end{footnotesize}
The ISO/IEC 17067:2013 sets minimum requirements for the content of the scheme, such as the scope, requirements against which the products are evaluated, methods and procedures, complaint mechanisms etc.

### 2.3.3 CEN, CENELEC and ETSI guidance

Even though certification is not part of the activities of CEN and CENELEC, the European Standardisation Organisations own and operate the Keymark certification scheme. The Internal Regulations on Certification provides substantial information on basic aspects of certification\(^ {20} \). The Regulations cover the CEN and CENELEC Keymark, which is a voluntary third-party certification mark, demonstrating compliance with the relevant European Standards\(^ {21} \). The minimum scheme requirements are that: a) the certification body should be located in one of the members of CEN and CENELEC b) The evidence of conformity of the product(s) with the requirements of the appropriate European standard(s) shall be based on type testing performed by a third-party testing laboratory c) the client should operate a quality management system at least covering the quality levels of the ISO 9001 d) the certification body should conduct periodic surveillance to the client.

ETSI has two important technical specifications relevant to the topic with regard to electronic signatures and infrastructures the Policy requirements for certification authorities issuing qualified certificates and Policy requirements for certification authorities issuing public key certificates\(^ {22} \). According to the general concepts of the ETSI TS 102 042 V2.3.1 document, the certification authority, which is identified in the certificate as the “issuer”, has the overall responsibility for the provision of certification services and ensures that the policy requirements are met\(^ {23} \). The services of a certification authority are the following\(^ {24} \):

- **Registration service**: verifies the identity and any specific attributes of a subject.
  - **Certificate generation service**: creates and signs certificates based on the identity and other attributes verified by the registration service.
- **Dissemination service**: disseminates certificates to subjects. This service also makes available the CA’s terms and conditions, and any published policy and practice information, to subscribers and relying parties.
- **Revocation management service**: processes requests and reports relating to revocation to determine the necessary action to be taken.

---


\(^ {21} \) The Keymark scheme is a “**set of specific product-related requirements and procedures to support the implementation of the Keymark system for the certification of products which are in conformity with specific European standards and labelled with the Keymark**”p.6 of the Internal Regulation part 4 op.cit.

\(^ {22} \) ETSI TS 101 456 (v1.4.3) technical specification “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates” and ETSI TS 102 042 (v2.3.1) technical specification “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”.

\(^ {23} \) Clause 4.1. ETSI TS 102 042 V2.3.1, op.cit.

\(^ {24} \) Clause 4.2. ETSI TS 102 042 V2.3.1, op.cit.
• **Revocation status service:** provides certificate revocation status information to relying parties. This may be based upon certificate revocation lists or a real time service which provides status information on an individual basis.

The ETSI TS 101 456 V1.4.3 document among others refers to compliance with the legal requirements. The certification authority is obliged to ensure that it meets all the applicable statutory requirements (including requirements of the Data Protection Directive) for protecting records from loss, destruction and falsification.

### 2.4 CONCLUSIONS

The aim of the chapter was to identify the key legislation and documents that set requirements or are best practices for evaluation and certification schemes. With regard to the relevant legislation, there is no specific regulation for evaluation and certification schemes at EU level. The Regulations and Directives of the New Approach and the New Legislative Framework refer mainly to standardisation. International standards of the ISO adopted by the European Standardisation Organisations and guidance documents by such organisations and bodies form the framework of best practices and “soft law” for certification in the EU. Quite importantly these documents, refer both to core issues, such as the content and management of a certification scheme, and the actual best practices or the issues that stakeholders encounter and suggest solutions, based on the accumulated experience of the experts involved. The gap of the specific legislation on the hand offers the opportunity to a free market to develop schemes according to actual needs. On the other hand, a minimum set of legal rules in the form of legal obligations could provide the market, and mainly the consumers of the certified products, with the legal certainty and boost the trust and confidence for the certified products.

---

25 Since the specification is based on the electronic signatures Directive, it does not deviate from its provisions. It is interesting however to see the concept of accountability, in this case through the obligation of the certification body to comply with the legal requirements, in a broader context for certification bodies in general.
3 LEGAL STUDY ON SECURITY ASPECT OF SECURITY PRODUCTS, SYSTEMS AND SERVICES: MAPPING LEGISLATION AND LEGAL DEMANDS FOR SECURITY PRODUCTS, SYSTEMS, SERVICES IN THE EU

3.1 INTRODUCTION

Security as a concept has different uses and meanings. It is not a static concept. It adapts and develops according to several variables such as the societal needs, the needs of citizens and the market practices. As highlighted in the CRISP Taxonomy of security products, systems and services, any attempt to pin down a final definition of “security” will “run up against boundaries created by the problem that security-conceptually- is determined by context”\(^26\). In the Treaty on the Functioning of the European Union (TFEU)\(^27\), “security” is an area of shared competence between the European Union and the Members-States in the context of foreign and security policy, where a high level of security requires measures against crime, racism and xenophobia\(^28\). According to the Programming Mandate 487 of the European Commission to the ESOs the concept of security includes: protection against threats by terrorism, severe and organised crime, natural disasters, pandemics and major technical accidents\(^29\). As a result, we often encounter the notions of physical security, political security, information security and socio-economic security\(^30\).

Following the plurality of notions of security, the EU legislation uses the term in several contexts. Not every legal text relating to security however is of use for this analysis. The analysis below will present the main legal texts at EU level that are related to security. The presentation will follow the areas of security as in CRISP glossary (D.1.1.), which are\(^31\):

- Security of citizens
- Security of infrastructures
- Border Security
- Crisis Management

The mapping of the legislation is not intended to be exhaustive. In this part, the focus is on legislation, which is relevant to security standardisation and certification schemes. The selected legislation also corresponds to the needs of the case studies of this Work Package and aims at orientating the reader with regard to the existing legislation and determining special requirements and legal demands in the several fields of security, mainly related to products.

\(^{26}\) Sveinsdottir Thordis et. al., Taxonomy of Security Products, Systems and Services, Deliverable 1.2 of the CRISP project, op.cit., p. 93
\(^{28}\) TFEU art. 63 para. 3
\(^{29}\) M/487 Programming mandate addressed to CEN, CENELEC and ETSI to establish security standards, op.cit, read further section 1.2.2., p.14 of current report.
\(^{30}\) Fritz Florian et. al., Glossary of security products and systems, Deliverable 1.1 of the CRISP Project, op.cit.
\(^{31}\) The categorization of the legislation under the specific categories of security is indicative. It might be the case that a law might be categorized under several areas of security. An example is the civil aviation security which is relevant to the security of citizens, the security of critical infrastructures and the crisis management.
It should also be noted that freedom, security and justice is an area of shared competence between the EU and the Member States according to the art. 4 (j) of the Treaty on the Functioning of the European Union. The area is therefore regulated both at national level and EU level, with the latter mainly regulating on the basis of the principle of subsidiarity and proportionality. With regard to the common and foreign security policy, the EU is exclusively competent to legislate and adopt legally binding acts art. 2 (1) TFEU).

### 3.2 Security of Citizens

Security of the citizens in the context of CRISP includes counter terrorism, crime prevention and organized crime, and public order as necessary subareas. In general it covers all possible threat aiming at European citizens as a result of an intended/deliberate attack or a natural hazard, by trying to create a peaceful environment, including the prevention of radicalisation.

#### 3.2.1 Terrorism


<table>
<thead>
<tr>
<th>Date</th>
<th>Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/12/2011</td>
<td>Council Decision 2011/872/CFSP of 22 December 2011 updating the list of persons, groups and entities subject to Articles 2, 3 and 4 of Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and repealing Decision 2011/430/CFSP</td>
</tr>
</tbody>
</table>

---


33 See Deliverable D.1.2 of the CRISP project, Fritz Florian et. al., Glossary of security products and systems, Deliverable 1.1 of the CRIS Project, op.cit.

3.2.2 Common Crime

Common crime is mainly regulated at national level in the European Union. The Union adopts legislation on three areas: a. Minimum rules on Euro-crimes such as terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime (art. 83 (1) TFEU), b. Criminal law for enforcement of EU policies (art. 83 (2) TFEU) c. Criminal sanctions against market abuse (art. 83 (2) TFEU) and d. Protection of EU public money (arts. 310 (6), 325, 85 and 86 TFEU). With this legal basis, the Directive 2012/29/EC on the rights, support and protection of victims of crime ensures that victims of crime receive appropriate information, support and protection and are able to participate in criminal proceedings. Similarly, other Directives and Council Framework Decisions support the national legislation of the Member States on the area of criminal justice and security.

3.2.3 Civil Aviation Security

Civil aviation security is an important field for the security of citizens. Aviation security means “the combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference that jeopardize the security of civil aviation”\textsuperscript{36}. The Regulation (EC) 300/2008 on common rules in the field of aviation


D4.1: Legal Analysis of Existing Schemes

security lays down principles of what has to be done in order to safeguard civil aviation against acts of unlawful interference without going into the technical and procedural details of how they are to be implemented. The goal of the Regulation is the “one stop security” for all flights within the EU. The achievement of this goal is aimed among others with the setting of common standards and common rules for the protection of civil aviation. An obligation for the Member States to draw up, apply and maintain a national civil security aviation program, national quality control program, an airport security program, an air carrier security program and an entity security program is established in the articles 10-14 of the Regulation. A common set of minimum basic standards regarding airport security is also provided in the Annex of the Regulation. Among others it addresses issues regarding location, access control, screening of persons and items, examination of vehicles, surveillance – patrols and other physical controls), aircraft security, passengers and cabin baggage, hold baggage, cargo and mail, supplies, in-flight security measures, staff recruitment and training. Security equipment which is used for screening, access control and other security controls shall comply with the defined specifications and be capable of performing the security controls concerned. First, performance as a criterion here is not further defined; however from the context it shall be accepted that it means “performance as intended”. Second, the term “defined specifications” refers to technical specifications and procedures for approval and use of security equipment [art. 4 (3)].

Figure 2: Operationalisation of Civil Aviation Security core legal requirements
Source: Own source

3.2.4 Safety of Equipment

The ATEX Directive is the most important in this field as it sets safety requirements for equipment and protective systems intended for use in potentially explosive atmospheres. The safety of equipment is important not only in terms of security, but also for the trust of the end users to the security products, systems and services.

In 2014, the new ATEX Directive was voted, which will enter into force on 20th April 2016. The following analysis is based on the new ATEX Directive. The scope of the Directive covers all the products which are new to the Union market, both new or second hand, manufactured in the EU or imported from a third country.

In the context of the Directive,

“equipment” means:

“machines, apparatus, fixed or mobile devices, control components and instrumentation thereof and detection or prevention systems which, separately or jointly, are intended for the generation, transfer, storage, measurement, control and conversion of energy and/or the processing of material and which are capable of causing an explosion through their own potential sources of ignition.”

And “protective systems” means:

“devices other than components of equipment which are intended to halt incipient explosions immediately and/or to limit the effective range of an explosion and which are separately made available on the market for use as autonomous systems.”

Article 6 provides a list with obligations for the manufacturers of the products. Among others, manufacturers are obliged to ensure that the design and manufacture of the products is in accordance with the essential health and safety requirements, draw up technical documentation and carry out relevant conformity assessments. Also, importers and distributors have obligations according to articles 8 and 9, mainly related to the verification
that a conformity assessment procedure for the product has been undertaken or the product bears the CE marking and that they should act with due care in handling the product.

The conformity of the product is an important issue. Presumption of conformity of the product with the essential health and safety requirements of the Directive is established when the product is in conformity with the harmonised standards (art.12).

<table>
<thead>
<tr>
<th>Type of requirement</th>
<th>Categories of issues to be addressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>General requirements</td>
<td>• Principles of integrated explosion safety</td>
</tr>
<tr>
<td></td>
<td>• Special checking and maintenance conditions</td>
</tr>
<tr>
<td></td>
<td>• Surrounding area conditions</td>
</tr>
<tr>
<td></td>
<td>• Marking</td>
</tr>
<tr>
<td></td>
<td>• Instructions</td>
</tr>
<tr>
<td>Selection of materials</td>
<td>-</td>
</tr>
<tr>
<td>Design and construction</td>
<td>• Enclosed structures and prevention of leaks</td>
</tr>
<tr>
<td></td>
<td>• Dust deposits</td>
</tr>
<tr>
<td></td>
<td>• Additional means of protection</td>
</tr>
<tr>
<td></td>
<td>• Safe opening</td>
</tr>
<tr>
<td></td>
<td>• Protection against other hazards</td>
</tr>
<tr>
<td></td>
<td>• Overloading of equipment</td>
</tr>
<tr>
<td></td>
<td>• Flameproof enclosure systems</td>
</tr>
<tr>
<td>Potential ignition sources</td>
<td>• Hazards arising from different ignition sources</td>
</tr>
<tr>
<td></td>
<td>• Hazards arising from static electricity</td>
</tr>
<tr>
<td></td>
<td>• Hazards arising from stray electric and leakage currents</td>
</tr>
<tr>
<td></td>
<td>• Hazards arising from overheating</td>
</tr>
<tr>
<td></td>
<td>• Hazards arising from pressure compensation operations</td>
</tr>
<tr>
<td>Requirements for Safety-related devices</td>
<td>• Control and display units</td>
</tr>
<tr>
<td></td>
<td>• Requirements in respect of devices with a measuring function for explosion protection</td>
</tr>
<tr>
<td></td>
<td>• Risks arising from software</td>
</tr>
<tr>
<td>Integration of safety requirements relating to the system</td>
<td>• Hazards arising from power failure</td>
</tr>
<tr>
<td></td>
<td>• Hazards arising from connections</td>
</tr>
<tr>
<td></td>
<td>• Placing of warning devices as parts of equipment</td>
</tr>
<tr>
<td>Hazards arising from external effects</td>
<td>-</td>
</tr>
</tbody>
</table>

Table 2: Requirements for equipment and protective systems – new ATEX Directive
Source: Annex II- new ATEX Directive

In particular, in relation to safety-related devices, Annex II provides a set of requirements:

- Safety devices must function independently of any measurement and/or control devices required for operation.
As far as possible, failure of a safety device must be detected sufficiently rapidly by appropriate technical means to ensure that there is only very little likelihood that dangerous situations will occur.

The fail-safe principle is to be applied in general.

Safety-related switching must in general directly actuate the relevant control devices without intermediate software command.

In the event of a safety device failure, equipment and/or protective systems shall, wherever possible, be secured.

Emergency stop controls of safety devices must, as far as possible, be fitted with restart lockouts. A new start command may take effect on normal operation only after the restart lockouts have been intentionally reset.

Figure 3: Operationalisation of Safety Equipment core legal requirements
Source: Own source

### 3.3 Security of Critical Infrastructures

Critical infrastructures include the security of energy, transportation and telecommunication, supply chains, health infrastructure, and also control systems – general infrastructures which are of high importance of the functioning of a vital society and thus a protection against threats aiming at the disruption or destruction of the like plays an important role in the European policy making and the security industry.
3.3.1 European Critical Infrastructures

The Council Directive 2008/114/EC sets the framework for the identification and designation of the European critical infrastructures\(^{45}\). Since the disruption or destruction of the European critical infrastructures would have significant cross-border impacts, the European legislator requires that the critical infrastructures are assessed based on common minimum criteria. Before analysing the criteria provided in the Council Directive 2008/114/EC, we provide with the definition of the term “critical infrastructure” as in the article 2 (a) of the Directive.

Critical infrastructure is:

> “An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions”.

The Directive establishes three criteria for the identification and designation of critical infrastructures:

- The casualties criterion
- The economic effects criterion
- The public effects criterion

First, the casualties criterion is assessed with regard to the potential number of fatalities or injuries. The second criterion addresses the economic loss and the degradation of products or services. It also takes into account any potential environmental effects. The criterion of public effects refers to the impact on public confidence, the physical suffering and the disruption of daily life. The three cross-cutting criteria, as indicated in the Directive\(^{46}\), are based on the severity of the impact of disruption or the destruction of a particular infrastructure. The specific thresholds for the above criteria are determined on a case-by-case basis by the Member States. In addition to the cross-cutting criteria, specific criteria corresponding to the characteristics of the individual European Critical Infrastructure Sector shall be established by the Member States.


European Critical Infrastructure sectors

<table>
<thead>
<tr>
<th>Sector</th>
<th>Subsector</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Energy</td>
<td>1. Electricity Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity</td>
</tr>
<tr>
<td></td>
<td>2. Oil Oil production, refining, treatment, storage and transmission by pipelines</td>
</tr>
<tr>
<td></td>
<td>3. Gas Gas production, refining, treatment, storage and transmission by pipelines LNG terminals</td>
</tr>
<tr>
<td>II Transport</td>
<td>4. Road transport</td>
</tr>
<tr>
<td></td>
<td>5. Rail transport</td>
</tr>
<tr>
<td></td>
<td>6. Air transport</td>
</tr>
<tr>
<td></td>
<td>7. Inland waterways transport</td>
</tr>
<tr>
<td></td>
<td>8. Ocean and short-sea shipping and ports</td>
</tr>
</tbody>
</table>

Table 3: European Critical Infrastructure sectors

The European Commission in its Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, highlighted the intention to upgrade the current framework. The new approach builds on the existing regime as set in the Critical Infrastructures Directive (described above) and emphasizes the interdependencies between critical infrastructures, industry, and state actors. The focus is also on the interdependencies within sectors, which are spanning a number of European countries. An example of such an interdependency across Member States is the European high-voltage electricity grid, composed of the interconnected national high-voltage electricity grids.

3.3.2 Aviation Security

The Commission Regulation (EU) No 185/2010 of 4 March 2010 lays down detailed measures for the implementation of the common basic standards on aviation security. The Annex provides detailed requirements for security equipment. It follows the harmonisation of security measures in:

---


48 Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security
- Walk Through Metal Detection Equipment (WTMD)
- Hand-Held Metal Detection Equipment (HHMD)
- X-Ray Equipment
- Explosive Detection Systems (EDS) Equipment
- Threat Image Projection (TIP)
- Explosive Trace Detection (ETD) Equipment
- Equipment For Screening Liquids, Aerosols and Gels (LAGs)\(^{49}\)
- Methods Of Screening Using New Technologies

The following table presents the main requirements for each type of security equipment.

---

\(^{49}\) Detailed measures on Equipment for Screening Liquids, Aerosols and Gels are provided in the Commission Implementing Regulation (EU) No 246/2013 of 19 March 2013 amending Regulation (EU) No 185/2010 as regards the screening of liquids, aerosols and gels at EU airports.
<table>
<thead>
<tr>
<th>Type of Security Equipment</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| **Walk Through Metal Detection (WTMD)** | • Shall be able to detect and to indicate by means of an alarm at least specified metallic items, both individually and in combination.  
• Shall be independent of the position and orientation of the metallic item  
• Shall be firmly fixed to a solid base  
• Shall have a visual indicator to show that the equipment is in operation  
• The means for adjusting the detection settings of WTMD shall be protected and accessible only to authorised persons.  
• Shall give both a visual alarm and an audible alarm when it detects metallic items  
• Shall be positioned so as to ensure it is not affected by sources of interference.  
• Shall generate an audible and/or visual signal on a percentage of persons passing through the WTMD who did not cause an alarm  
• Shall count the number of persons screened, excluding any person that passes through the WTMD in the opposite direction;  
• Shall count the number of alarms  
• Shall calculate the number of alarms as a percentage of the number of screened persons. |
| **Hand-Held Metal Detection (HHMD)** | • Shall be able to detect ferrous and non-ferrous metallic items.  
• Detection and identification of the position of the detected metal shall be indicated by means of an alarm.  
• The means for adjusting the sensitivity settings of HHMD shall be protected and accessible only to authorised persons.  
• HHMD shall give an audible alarm when it detects metallic items. The alarm shall be noticeable at a range of 1 metre.  
• The performance of HHMD shall not be affected by sources of interference.  
• HHMD shall have a visual indicator to show that the equipment is in operation. |
| **Explosive Detection Systems (EDS)** | • Shall be able to detect and to indicate by means of an alarm specified and higher individual quantities of explosive material contained in baggage or other consignments.  
• Image quality requirements for EDS laid down in shall comply with the detailed requirements laid down in a separate Commission Decision. |
| **Threat Image Projection (TIP)** | • Shall be able to project virtual images of threat articles within the x-ray image of bags or other consignments being screened.  
• The virtual images shall be placed within the x-ray image of bags and consignments being screened in an evenly distributed manner and not in a fixed position.  
• It shall be possible to set the percentage of virtual images to be projected.  
• TIP shall not impair the performance and normal functioning of x-ray equipment.  
• No indication shall be given to the screener that a virtual image of a threat article is about to be projected or has been projected until a message is presented  
• The means for managing TIP shall be protected and accessible only to authorised persons.  
• Access to equipment with TIP installed and deployed shall require that the screener uses a unique identifier.  
• TIP shall be able to store the results of the responses of individual screeners for a minimum of 12 months and in a format to allow the provision of reports. |

---

50 X-Ray security equipment is regulated with Separate Decision Commission
**Explosive Trace Detection**

Shall be able to collect and analyse particles on, or vapour from, contaminated surfaces or contents of baggage or consignments, and to indicate by means of an alarm the presence of traces of explosives.

**Equipment For Screening Liquids, Aerosols And Gels**

- Shall be able to detect and to indicate by means of an alarm specified and higher individual quantities of threat materials in LAGs.
- The detection shall be independent of the shape or material of the LAG container.
- Shall be used in a manner that ensures that the container is positioned and orientated so as to ensure that the detection capabilities are met in full.
- The equipment shall give an alarm in each of the following circumstances:
  a. when it detects threat material;
  b. when it detects the presence of an item that prevents threat material from being detected;
  c. when it cannot assess whether the LAG is benign or not; and
  d. when the contents of the screened bag are too dense to be analysed.

<table>
<thead>
<tr>
<th>Table 4: Requirements for Security Equipment for Civil Aviation Security according to Commission Regulation (EU) No 185/2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: Own Table</td>
</tr>
</tbody>
</table>

The Commission Regulation also takes into account that screening methods using new technologies, might be employed. In order to cover the new technologies, the Commission Regulation requires the new screening methods to fulfil three minimum criteria in relation to:

a. the purpose of the new technologies to evaluate a new method of screening,

b. the guarantee that it does not affect the overall level of security and

c. the provision of information regarding the trial of the new technology to those affected, including the passengers.

In the field of Aviation Security there is a number of published Regulations in the Official Journal of the EU, the substantial content of which is in a confidential and thus unpublished Annex. Such Regulations are the Commission Regulation (EC) No 622/2003, the Commission Regulation No 781/2005 of 24 May 2005 and the Commission Regulation (EC) No 857/2005.

---

51 Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security.


3.3.3 Maritime Security

Maritime security is extensively regulated in the EU. The Regulation (EC) No 725/2004 on enhancing ship and port facility security\textsuperscript{54, 55}. The main objective of the Regulation is to introduce and implement measures aimed at enhancing the security of ships used in international trade and domestic shipping and associated port facilities in the face of threats of intentional unlawful acts. Article 3 of the Regulation foresees a mandatory risk assessment for the Member States in order to determine the extent to which they apply, the provisions of this Regulation to different categories of ships operating domestic services, their companies and the port facilities serving them. We see that the concept of risk assessment becomes an official part of the legislation and a mandatory method to decide upon appropriate measures.

The Regulation also provides Requirements for companies and ships. The requirements are mainly a reference to the requirements provided in the International Ship and Port Facility Security Code (ISPS Code)\textsuperscript{56}.

With regard to the principle of accountability, there is an interesting provision in the same Annex of the Regulation, according to which the Companies, shall at all times keep information available on the following points:

\begin{itemize}
  \item Visual Indicators for equipment
  \item Access control
  \item Protection against interference
  \item Image quality requirements
\end{itemize}

\textit{Figure 4: Operationalisation of Aviation Security core legal requirements}

Source: Own source

\textsuperscript{54} ‘Maritime security’ means the combination of preventive measures intended to protect shipping and port facilities against threats of intentional unlawful acts (art. 2 Regulation (EC) 725/2004).


\textsuperscript{56} “The International Ship and Port Facility Security Code is a set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States. The ISPS Code is implemented through chapter XI-2 Special measures to enhance maritime security in the International Convention for the Safety of Life at Sea (SOLAS), 1974. The Code has two parts, one mandatory and one recommendatory”: International Maritime Organisation, ISPS Code, available: \url{http://www.imo.org/ourwork/security/instruments/pages/ispscode.aspx}
1. Who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship;
2. Who is responsible for deciding the employment of the ship; and
3. In cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party(ies).

The Regulation also foresees a mandatory ship security alert system. The ship security alert systems shall:

- Initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration, which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised;
- Not send the ship security alert to any other ships;
- Not raise any alarm on-board the ship;
- Continue the ship security alert until deactivated and/or reset.

Additionally, the ship security alert system activation points shall be designed so as to prevent the inadvertent initiation of the ship security alert.

Special reference is made to the Ship Security Certificate of the ISPS Code. In the case the Government of a contracting party to the ISPS Code wishes to apply control and compliance measures to a ship in its port, then the control is limited only to the verification that a valid International Ship Security Certificate or a valid Interim International Ship Security Certificate exists onboard. The significance of such a certificate here is substantial in terms of costs, time and manpower; the ship demonstrates the compliance to the international rules of the ISPS Code by providing a recognized certificate. The holding of such a certificate onboard provides a presumption of compliance to the ISPS Code principles and rules.

The guidance provided by IMO expressly states the following:\(^57\):

\textit{In simple terms, if a ship does not have a valid certificate that ship may be detained in port until it gets a certificate. Of course, the port State has various other options available at its disposal if a ship does not have a certificate. It may expel the ship from port, it may refuse the entry of the ship into port, it may curtail the operations of the ship...} [emphasis added]

With regard to core criteria for training of personnel, the Commission Regulation (EC) 884/2005, provides with criteria for training of inspectors\(^58\). Article 7 sets the following four qualification criteria for the training of the inspectors in the field of maritime security:

\(^57\) See IMO Q&A section, available at: \url{http://www.imo.org/blast/mainframe.asp?topic_id=897#whathappen}

1. Good understanding of maritime security and how it is applied to the operations being examined;
2. Good working knowledge of security technologies and techniques;
3. Knowledge of inspection principles, procedures and techniques;
4. Working knowledge of the operations being examined.

In addition, the inspectors shall be recurrent, accredited by the European Commission and ensure a standard of performance adequate for the purposes of controlling whether security measures are implemented in accordance with Regulation (EC) No 725/2004 and Directive 2005/65/EC.  

![Figure 5: Operationalisation of Maritime Security core legal requirements](source: Own source)

3.3.4 Port Security

The area of port security, as part of the area of security, also belongs to the areas of shared competence of the European Union and the Member States. The EU legislator introduces appropriate measures to enhance the port security only when necessary and the objectives cannot be achieved in a sufficient manner by the Member States.

The Directive 2005/65/EC provides a comprehensive framework of measures and obligations with the aim of enhancement of port security. The Recital 3 of the Directive specifies the relation of the Directive to the Regulation on maritime security as analysed above. The Regulation is limited in scope to security measures on board vessels and the immediate ship/port interface and as a result the security measures imposed by the Regulation constitute only part of the measures necessary to achieve an adequate level of security throughout maritime-linked transport chains. The Directive requires detailed security assessments for the

---

adoption of the appropriate measures to ensure port security. Clarity on the division of tasks is another requirement, a port security is required to be appointed and a port security plan employed in order to effectively implement preventive and remedial port security measures.

The Port Security Assessment needs to cover at least the identification and evaluation of the important assets and infrastructure, the identification of possible threats to the assets and infrastructure and the likelihood of their occurrence in order to prioritise the security measures, the identification, selection and prioritisation of the counter-measures and procedural changes and their level of effectiveness in reducing vulnerability and the identification of weaknesses, including human factors in the infrastructure, policies and procedures.

### 3.3.5 Rail Security

For the CRISP objectives, the certification of train drivers operating locomotives and trains on the railway system in the Community is interesting. It is established in the Directive 2007/59/EC. It is a “harmonised complementary certificate”, which is valid throughout the whole territory of the Community.

The certificate is issued by the railway undertaking or the infrastructure manager who employs or contracts the driver. The certificate is owned by the undertaking or manager issuing it. A set of minimum requirements is set in the Directive in order to obtain and reserve a valid certificate. The requirements are related to the age of the applicants, education and training, physical fitness, occupational psychological fitness and demonstration of general professional competence.

The license is valid for ten years (art. 14) and is subject to periodical checks as described in the Directive. With regard to the specific procedure for issuing and updating the certificates, each railway undertaking and infrastructure manager have the flexibility to set their own procedures, within the limitations and in accordance to the principles of the Directive. Quite important is also the provision for accreditation: Persons or bodies accredited under the Directive have to be accredited by the national accreditation body. The article also provides

---

60 Recital 6 and article 6 of the Directive 2005/65/EC Of The European Parliament And Of The Council of 26 October 2005 on enhancing port security

61 Recital 7, article 7 and 9 of Directive 2005/65/EC Of The European Parliament And Of The Council of 26 October 2005 on enhancing port security


63 Article 3(j) of the 2007/59/EC Directive provides: “certificate’ means the harmonised complementary certificate indicating the infrastructure on which the holder is authorised to drive and the rolling stock which the holder is authorised to drive”.

64 Article 6 of the 2007/59/EC Directive

65 See article 20 of the Directive 2007/59/EC
that the accreditation process shall be based on criteria of independence, competence and impartiality, such as the relevant EN 45000 series European standards.\(^{66}\)

### 3.3.6 Information Security

An area of fast evolving potential for criminal activity is the area of information systems.\(^{67}\) The digital world demands equal attention as the physical world in terms of security. The impact of interferences or attacks against the information systems can have serious effects on various fields of activity, political, social and economic.

Recently, the EU legislator voted the Directive 2013/40/EU on attacks against information systems.\(^{68}\) The Directive clearly states the increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and of the Union. The objective of this Directive is to establish minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. The Directive also aims to facilitate the prevention of such offences and to improve cooperation between judicial and other competent authorities.\(^{69}\)

The Directive regulates the protection of the information systems against the following types of threats:

- Illegal access to information systems
- Illegal system interference
- Illegal data interference
- Illegal interception

In detail, the illegal access to information systems is punishable when committed intentionally. It is sufficient for the commission of the crime that the individual infringes a security measure and accesses the whole or part of the information system without right. The illegal system interference requires that there is serious hindering or interrupting the


\(^{67}\) "'Information system' means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance" : article 2 of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 2013, OJ L 218, 14.8.2013, p. 8–14


\(^{69}\) Article 1of Directive 2013/40/EU
functioning of an information system by means of inputting computer data, transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right. Interfering without right and intentionally with the data of the information system by deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible is also punishable. Illegal interception is punishable in cases of interception, by technical means, of non-public transmissions of computer data to, from or within an information system. The case of electromagnetic emissions from an information system carrying such computer data is also covered. In each of the above crimes, the condition “at least for cases which are not minor” is added. The EU legislator gives the discretion to the Member States to also punish the “minor cases”. A definition of “minor case” is intentionally left to the Member States according to their national law and practice. The Recital 11 of the Directive provides an example of what can be considered as a minor case, that is a case where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition of a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary.

In the field of electronic communications, the Directive 2006/24/EC aims at harmonising the Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law”. The Directive required the retention of several types of data (not the content of communications however) by the providers of publicly available electronic communication services.

The Court of Justice of the European Union found invalid the Data Retention Directive on the grounds of interference to the right to private life and protection of personal data as protected in art. 7 and 8 of the Charter of Fundamental Rights of the EU. The Court found that:

“the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary.”

71 For the security breaches which fall under the scope 2002/58/EC Directive read the Freedom Infringement section of this report (chapter 6).
Data protection legislation might also applicable in case the protected and processed information is personal data. Obligations for the data controller – the person that defines the means and purposes of the processing – are established in the art. 17 of the Data Protection Directive. The data controller must take appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

In 2013, the European Commission submitted a proposal for a Network and Information Security Directive. While the legislative procedure is still ongoing, it is important to see the security requirements of the Directive. The Directive lays down measures to ensure a high common level of network and information security within the Union (art. 1). In particular, article 14 establishes the security and notification requirements for public administrators and market operators. Among the other proposed requirements, appropriate technical and organisational measures to manage risks are foreseen. The measures should guarantee a level of security, which is appropriate to the risk. Two are the main purposes of the measures: First, to prevent and minimize the impact of the incidents on the core services and second, to ensure continuity of the services. Public administrators and market operators need to notify to the competent authorities incidents that have a significant impact on their core services. The proposal does not require the notification of every incident regarding every service they provide, but only of those that have significant impact only on the core services.

On the scope of the Directive in the cases of processing operations for national security, intelligence services etc. see Chapter 6 of current report.


The explanatory report of the NIS Directive provides the relation between the NIS Directive with the Directive on attacks against Information Systems: “The co-legislators are currently discussing the Commission proposal for a Directive on attacks against information systems which aims to harmonise the criminalisation of specific types of conduct. It covers only the criminalisation of specific types of conduct and does not address the prevention of NIS risks and incidents, the response to NIS incidents and the mitigation of their impact. The present Directive should apply without prejudice to the Directive on attacks against information systems”.


According to art. 2 (8) a market operator is: (a) provider of information society services which enable the provision of other information society services, a non exhaustive list of which is set out in Annex II; (b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health, a non exhaustive list of which is set out in Annex II. In the first category the following are included: 1. e-commerce platforms 2. Internet payment gateways 3. Social networks 4. Search engines 5. Cloud computing services 6. Application stores (Annex II).

Article 14 (1) and (2) is applicable to market operators which provide services within the EU (art.14.3)
The Directive contains a provision explicitly supporting standardisation of security requirements. According to the Recital 32, standardisation of security requirements is a market-driven process. Article 16 provides:

1. To ensure convergent implementation of Article 14(1), Member States shall encourage the use of standards and/or specifications relevant to networks and information security.
2. The Commission shall draw up, by means of implementing acts a list of the standards referred to in paragraph 1. The list shall be published in the Official Journal of the European Union.

3.4 BORDER SECURITY

Border security includes the means for providing security of land, air and sea, but also of borders in embassies in order to prevent the illegitimate crossing of people. Further focus in border security aims also at the detection of illegal products, goods and substances within custom services.\(^{80}\)

3.4.1 Schengen Area

When it comes to borders, the European Union has additionally established the Schengen Area. The Schengen Borders Code provides EU Member States with a single set of common rules that govern external border checks on persons, entry requirements and duration of stays in the Schengen Area.\(^{81}\) According to article 21 of the Visa Code Regulation, in the case of an application for a uniform visa, the risk to the security of the Member States is assessed along with the risk of illegal immigration. In the framework of border security and the Schengen Area, mechanisms for exchange of information are established, with the aim of facilitating cooperation among the authorities of the Member States. The Visa Information

---

80 Legislation relevant to border security is also analysed under critical infrastructure and security of citizens.
System (VIS) was establishes with the Council Decision 2004/512/EC. The Schengen Information System (SIS) allows the Schengen States to exchange data on suspected criminals, on people who may not have the right to enter or stay in the EU, on missing persons and on stolen, misappropriated or lost property. Currently the SIS II is in progress. The SIS II should contribute to maintaining a “high level of security within the area of freedom, security and justice of the European Union by supporting the implementation of policies linked to the movement of persons that are part of the Schengen acquis”. Its objective is to ensure a high level of security within the area of freedom, security and justice of the European Union, maintain the public security and safeguard the security of the territories of the Member States.

Article 10 provides necessary security measures for the Member States, including the physical protection of data, facility access control, data access control etc. (see figure below).

Figure 7: Security measures of SIS II
Own figure, source: Regulation (EC) 1987/2006

---

83 European Commission website of DG Home Affairs
85 For the supervision of the VIS by the Data Protection Authorities: https://secure.edps.europa.eu/EDPSWEB/edps/Supervision/VIS
86 Recital 5of the Regulation (EC) 1987/2006
As of July 2015, the Regulation 603/2013 will be in force\textsuperscript{88}. The Regulation provides that the EURODAC database containing fingerprints and other personal data, which was previously used only for asylum purposes, will now be used also for law enforcement purposes\textsuperscript{89}. The procedure includes a reasoned electronic request from the authority for the transmission for comparison of fingerprint data to the Central System via the National Access Point.

In terms of border guards, FRONTEX is the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union\textsuperscript{90}.

### 3.5 Crisis Management

Crisis Management includes mainly the restoration of security in the aftermath of a crisis, which may result from a natural disaster, but also from deliberate attacks. Furthermore a focus within the European Union policy lies on the prevention and preparedness of crisis and disaster. The taxonomy of CRISP, identifies as key functions of crisis management, the disaster detection, data gathering and sharing, as well as communication around a network of centres around Europe\textsuperscript{91}. Many of the legislative acts mentioned earlier in the sections for other areas of security cover the area of crisis management\textsuperscript{92}.

### 3.6 Conclusion

The legislation in the EU relating to security is sector-specific, designed to address the specificities of each field of security. Notwithstanding the significance of such approach into highlighting the unique characteristics and demands of each area of security in the European Union, there are aspects of security that would benefit from a centralized approach. The shared competences of the EU with the Member States are a constraint in that respect towards a centralized holistic approach and to the extent the Commission can make legislative proposals to that end.

---

\textsuperscript{88} European Parliament and the Council, REGULATION (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180/1, 29.6.2013

\textsuperscript{89} Read further on the protection of privacy and data protection and the risks posed by security measures and collection and processing of biometric data in chapter 6.1. of this Report.

\textsuperscript{90} Fritz Florian, et.al, Glossary of security products and systems, Deliverable 1.1 of the CRISP Project, op.cit.


\textsuperscript{92} The bank recovery and financial crisis of the Eurozone are not in the scope of this research.
For the aim of CRISP, the analysis of the key legislation of the security areas at EU level, revealed important legal demands at high principle level, mainly demonstrating the direction that CRISP should focus in terms of security. Physical controls such as patrols, screening of persons and items, but also protection against digital threats such as unlawful interference in systems and databases, hold a central role in the priorities of the legislator.

Performance of the security equipment either relating to quality of images (captured by security cameras), detection of failure, independent functioning of the security PSS or others, also a requirement identified in the majority of the legal acts. The safety and security of the scrutinized and the operator of the security equipment is also a substantial requirement. In order to facilitate that requirement, risk and security assessments, proper training and certification of the operators is often required by the legislation.

A set of minimum demands for security equipment is established in the EU legal framework. An example is the Commission Regulation 185/2010, which includes a very detailed list of requirements for the different types of security equipment. Last but not least, key demand is the accountability; clear policies and codes, distribution of responsibilities, positive obligations and provision of the necessary information to the scrutinized individual and other affected parties play a critical role in promoting security.
4 LEGAL STUDY ON TRUST ON SECURITY PRODUCTS, SYSTEMS AND SERVICES

The aim of this chapter is to examine the trust aspect of security products, systems and services, i.e. to identify what are the core legal demands that facilitate the trust of the individuals to the security PSS, analyse the main concerns and trust issues and lack of confidence of the individuals relating to security PSS and examine what elements an evaluation or certification scheme should fulfil in order to help build trust and overcome the difficulties to that end.

4.1 LEGISLATION RELATED TO THE CONCEPT OF TRUST

The concept of trust can be explained in different ways, for example, as an individual feature, as a part of relationship and as a part of economic and social exchange. And it can be found a definition of trust in different disciplines. For example, the economists define it as trusting the institutions and their accounts while the psychologists explain it with the reliable and unreliable behavior of the individual. Sociologists use it as the reliable, fair and ethical behavior in interpersonal relations\(^93\). In all cases, many authors have emphasized the importance of trust for achieving organisational success\(^94\).

As described in the Stockholm Programme\(^95\), EU is facing new challenges to fight against criminality and security is one of the main goals of its policy\(^96\) including protecting citizens from the risks posed by crises and natural disasters. Any strategy must be based upon the full respect of fundamental rights and on solidarity between Member States. A common security strategy has to be built on trust among States, institutions and people. In this sense, trust and security are mutually reinforcing: trust increases the feeling of security and protection of Union's citizens and the more security citizens enjoy, the more trustful they live. And European legislation reflects this feature in specific provisions.


\(^96\) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Delivering an area of freedom, security and justice for Europe’s citizens: Action Plan Implementing the Stockholm Programme COM(2010) 171 final
Coming to our topic and as described in Deliverable 2.1 (Chapter 6.2)\(^97\), there is not a common European market for security products, as in other areas. The market is highly fragmented and suffers from time-consuming and costly national certifications.

In this sense, ECORYS\(^98\) identified the following issues in particular:

- Highly fragmented European market, challenges regarding future growth;
- No common (single) framework that applies to security products and the market for security products as a whole;
- Absence of common certification systems for security products;
- No mechanism of mutual recognition across countries of products certified at a national level; and
- Slow speed of response and adaptation of certification procedures, notably where new security threats require the implementation of new security solutions and technologies.

An effective response to security threats requires that new technologies and solutions “need not only to be validated; they should also be certified and where appropriate standardised”\(^99\). In connection with our study, a common European market on security products, services or systems will have a positive impact on trust of citizens as it could be assumed as a guarantee of the multiple aspects mentioned below.

Having the above in mind, a selection articles from the European legislation will be highlighted, as they reflect core issues related to trust in products, systems and services.

Before analyzing the impact of trust, the context of security products, systems, services the concept of “consumer” has to be clarified. In legal terms, “consumer” means any natural person who is acting for purposes which are outside his or her trade, business or profession\(^100\). Although the notion of consumer varies in the EU legislation and the Member States\(^101\), with Spain, Greece and Hungary for example establishing the notion of “final addressee” of the goods, i.e. the person which enjoys the goods without aiming at integrating them in production or commercialisation process\(^102\), what is common ground of every consumer protection law is the aim of protecting the party in a “weaker” position in the

---

\(^97\) CRISP Project, DEL 2.1 Report on security standards and certification in Europe. A historical/evolutionary perspective, Chapter 6.2.

\(^98\) ECORYS Final Report. Study on the Competitiveness of the EU security industry Within the Framework Contract for Sectoral Competitiveness Studies (ENTR/06/054), November, 2009.


transaction. The consumer protection legislation therefore can be seen as an instrument to enhance trust in the commerce and the market. In that sense, principles from the consumer protection legislation, give useful insight to our study on how to address trust issues to security products, systems and services also in the case of the scrutinized, even though the person undergoing the security measures may not be in the strict sense of the term considered as “consumer”.

In general terms, the protection of consumers in Union policies is recognized in Article 38 of the Charter of Fundamental Rights declares that “Union policies shall ensure a high level of consumer protection.” A high level of consumer protection is also granted on the Treaty on the Functioning of the European Union as Article 114 (3) states that proposals from the Commission regarding safety and consumer protection, among others, “will take as a base a high level of protection, taking account in particular of any new development based on scientific facts. Within their respective powers, the European Parliament and the Council will also seek to achieve this objective” or, even more demanding, Article 169 (1) of the Treaty on the Functioning of the European Union provides that “In order to promote the interests of consumers and to ensure a high level of consumer protection, the Union shall contribute to promoting the health, safety and economic interests of consumers, as well as to promoting their right to information, education and to organise themselves in order to safeguard their interests.”

The competence in the area of consumer protection is shared between the Union and the Member States (Article 4.2 f) of the Treaty on the Functioning of the European Union) and consumer protection requirements “shall be taken into account in defining and implementing other Union policies and activities” (Article 12 of the Treaty on the Functioning of the European Union).

Technologies employed in security measures may interfere to fundamental rights of individuals. In this sense, to result competitive or even legitimate on the European market, security PSS have not only to respond to general qualities of items (such as efficiency, security or trust) but also to be respectful with freedoms and rights of the “consumers” (such as privacy, equal treatment, freedom of movement or presumption of innocence, among others). As the definition shows, security of the PSS is a principal element to build trust of consumers. This security has to be translated not only into physical security (health or environmental consequences of the PSS performance) but also in confidence on its usefulness to comply with its finality. Accordingly, trust relates to both trustworthiness and the way people perceive and experience security PSS. This is specified in relation to what people trust: the technical reliability of a PSS, the actual safety it provides, the level of confidence

---

that end users have, and the belief end users have that such PSS respect their rights and freedoms.

As the Glossary of CRISP project indicates, physical security is one of the different dimensions of security. The Glossary accepts the definition incorporated in other projects and provided by the doctrine and defines physical security as an important aspect of producing secure measures in order to safeguard the physical characteristics and properties of citizens, infrastructure, objects, but also abstract/control systems. The physical security protection is one of the biggest security sectors regarding market size on a European and global level and examples of security-PSS include e.g. CCTV systems, fire alarm, intruder alarm systems, burglar alarm systems, communication systems, etc.

The obligation of placing safe products on the market is frequently underlined in European Directives, as for example, in Article 3 of the Directive 2001/95/EC. The safety of products should be assessed taking into account all the relevant aspects; especially the categories of the scrutinised which can be particularly vulnerable to the risks posed by the products under consideration, in particular children and the elderly (article 2.b iv). And consumers must be provided by producers with the relevant information to enable them to assess the risks inherent in a product throughout the normal or reasonably foreseeable period of its use, where such risks are not immediately obvious without adequate warnings, and to take precautions against those risks (Articles 5 and 8 of the Directive 2001/95/EC).

In parallel, trust in the security products, also relates to the presentation of the information. Article 6 of the Directive 2005/29/EC regulates misleading actions. In this sense, it understands by this a practice that contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise: the existence or nature of the product; the main characteristics of the product; the extent of the trader’s commitments, the motives for the commercial practice and the nature of the sales process, any statement or symbol in relation to direct or indirect sponsorship or approval of the trader or the product; the price or the manner in which the price is calculated, or the existence of a specific price advantage; the need for a service, part, replacement or repair; the nature, attributes and rights of the trader or his agent and the consumer’s rights.

Finally, in case of use of electronic communications by the security PSS (such as communication of information from a drone, transmission of data in digital format by IP

---


video cameras and webcam) the Directive 2000/31/EC on electronic commerce\textsuperscript{106} contains some obligations of providers related to the transmission or carrying of information that should be revised in an assessment of security PSS.

This directive states that the development of electronic commerce enhances the competitiveness of European industry, provided that everyone has access to the Internet (Recital 2). Nowadays, it is undisputed that most of European citizens have access to the Internet. However, the development of information society services within the Community is hampered by a number of legal obstacles to the proper functioning of the internal market which make less attractive the exercise of the freedom of establishment and the freedom to provide services.

These obstacles arise from divergences in legislation and from the legal uncertainty as to which national rules apply to such services; in the absence of coordination and adjustment of legislation in the relevant areas (Recital 5 Directive). Therefore, Recital 8 states that the objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States.

To that end and in accordance with the principle of proportionality, the measures provided for in the Directive are strictly limited to the minimum needed to achieve the objective of the proper functioning of the internal market; where action at Community level is necessary, and in order to guarantee an area which is truly without internal frontiers as far as electronic commerce is concerned, the Directive must ensure a high level of protection of objectives of general interest, in particular the protection of minors and human dignity, consumer protection and the protection of public health (Recital 10). The confidentiality of communications is guaranteed by Article 5 Directive 97/66/EC\textsuperscript{107}.

In order to achieve it, Article 10 of 2000/31/EC states that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service\textsuperscript{108}: (a) the different technical steps to follow to conclude the contract; (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible; (c) the technical means for relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.

The following table gives an overview of the key legislation on legal obligations and requirements related to the trust of the users and scrutinised to the security products, systems, services.

\\textsuperscript{107} Member States must prohibit any kind of interception or surveillance of such communications by others than the senders and receivers, except when legally authorised.

\textsuperscript{108} Except when otherwise agreed by parties who are not consumers.
### Source of legal obligation | Relevant article
---|---
Charter of Fundamental Rights of the European Union | Article 38
Treaty on the Functioning of the European Union | Article 12, Article 114, Article 153 (1) and (3), Article 169 (1)

Table 5: Normative on legal obligations related to trust

Source: own table

De Bruin discussed consumer trust aspects of electronic transactions and developed a consumer trust assessment framework based mainly on the EU legislation\(^\text{109}\). The following graphic provides the consumer trust aspects and their sub-criteria\(^\text{110}\).


\(^{110}\) The original consumer trust assessment framework as provided by Ronald de Bruin includes additionally the aspects of electronic contracts, electronic payment and applicable laws and jurisdiction, which however are not relevant to our study.
4.2 TRUST ISSUES CONNECTED TO SECURITY PRODUCTS AND SERVICES

This section aims to discuss the key factors that generate trust or mistrust to security PSS. The overview will then help identify the potential role of the evaluation and certification schemes in building confidence to security measures.

The CRISP Stakeholder Analysis Report offers valuable input on the trust levels of stakeholders, including end users and individuals, to security products, systems and services\textsuperscript{112,113}. Key needs of the individuals are the protection, privacy, non-discrimination, non-harm of health, transparency and provision of information. For end users, high level of security, product quality and efficiency are the needs to be addressed via security certification scheme.

The SIAM project identified key factors that drive people to trust or not a security measure. The “trust drivers” are logical criteria that take into account different trust issues of people

\textsuperscript{111} De Bruin Robert, op.cit. p. 46
\textsuperscript{112} See CRISP Deliverable 3.1., Sveinsdottir Thordis et. al., op.cit.
\textsuperscript{113} End users in WP3 (p.31 of the Report) are the procurers, strategic planners and operators working with security products, systems and services, such as the local authorities, emergency organisations, transport operators, law enforcement authorities, retail organisations, health organisations and educational organisations. The respondents of the end-user survey were civil society organisations, consumer rights organisations, procurers of security products, systems and services in the public and the private sector, operators of security products and systems.
towards the security measures. The project reached to the following clusters of trust
drivers:\(^\text{114}\):

- Reliability
- Health hazards
- Experience
- Communication
- Human Interaction
- Diffusion
- Appearance
- Privacy
- Cultural/historical/religious background
- Regulation gaps

Focusing on the issues that are relevant to the objectives of the CRISP project such as
reliability and health hazards and can be addressed by an evaluation or certification scheme,
it is apparent that those issues are relevant to both actual and perceived risks. Health hazard is
an example of an actual risk. It might also work as perceived risk, in the case of a security
measure which eradicates the impression of hazard to health. Body scanners with x-ray
radiation or electromagnetic pulse technology can generate mistrust due to the perception of
health hazard. Reliability is connected to the high or low rates of false negatives and false
positives of the security measure. In case the scrutinised or user is aware of high negatives for
example, the trust to the measure is possible to decrease.

The physical appearance of the security measure, eg. strong lights, high noise etc. might
influence the trust of the individual in a negative way. Also the potential of violation of the
right to privacy is a criterion capable of reducing the trust levels of the individuals to the
security measure. Moving one step further, one could say that the perception of freedom
infringement in general may lead to mistrust. The mere perception that a smart CCTV system
categorises people with ethnic criteria or by the criterion of surveilled bearing a religious
symbol, creates the perception to individuals that they might be also victims of such
differential treatment, and this has a negative impact to their trust towards the smart CCTV
system. Last but not least, a critical indicator is the possibilities of misuse and abuse of the
security measure\(^\text{115}\).

SAPIENT (Deliverable 1.1) on the state of the art in the area of smart surveillance mentions

Media Analysis of discourse about future security technologies, FP7 SIAM project, 21 June 2013,
http://www.tu-berlin.de/fileadmin/f27/PDFs/Forschung/SIAM/10.2_Media_Analysis_of_discourse_about_future_technologies_PDF

\(^\text{115}\)Rossnagel Alexander, Geminn Christian Ludwig, Deliverable 9.8. Evaluation of case study reports & further
the adverse effects on trust by overt unmitigated security measures: “the adverse effects of profiling, alienating and victimizing certain ethnic and religious groups, which engender a deep mistrust of the police”\textsuperscript{116}. This means that any scheme used to certify a product, system or service with the capability to profile should take into account that negative effects could arise also for the operators.

4.3 C\textsc{itizens}'\textsc{'} s \textsc{v}o\textsc{ice on Trust Issues of Security Products}

Inextricably related to trust is the end user. In order to obtain a better understanding on the identified trust issues, we contacted ANEC.

ANEC, the consumer voice in standardisation, represents the European consumer interests in the creation of technical standards, especially those developed to support the implementation of EU legislation and public policies\textsuperscript{117}.

The interview with ANEC revealed a series of concerns of the consumers relating to security products, systems and services. Surveillance of citizens by public and police authorities for national security purposes is an important concern that leads to lower levels of trust. The misuse or excessive and disproportionate use of the security measures that record and store information on citizens, calls for more open and transparent procedures. In the UK, the Information Commissioner has published several guidelines and codes of practices on the issue of surveillance by CCTV systems\textsuperscript{118}. As the ICO states:

“The UK is recognised as a leading user of CCTV and the public are used to seeing CCTV cameras on virtually every high street. Such systems continue to enjoy general public support but they do involve intrusion into the lives of ordinary people as they go about their day to day business and can raise wider privacy concerns. We know from our research that the public expect CCTV to be used responsibly with proper safeguards in place”\textsuperscript{119}.

Since 2012, the UK has a Surveillance Camera Commissioner, responsible to encourage compliance with the surveillance camera code of practice, review how the code is working and provide advice to ministers on whether or not the code needs amending\textsuperscript{120}.


\textsuperscript{117} We would like to thank ANEC, the European Association for the Co-ordination of Consumer Representation in Standardisation for the contribution to this chapter. More information on ANEC and its work: http://www.anec.eu/anec.asp

\textsuperscript{118} See ICO website

\textsuperscript{119} Abstract from ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

\textsuperscript{120} See in detail responsibilities of the Surveillance Camera Commissioner: https://www.gov.uk/government/organisations/surveillance-camera-commissioner/about
The domestic use of CCTV systems is also an issue that concerns the consumers and citizens. Recently, the Court of Justice of the European Union, issued a preliminary ruling relating to the applicability of the Personal Data protection legislation to the CCTV systems used for domestic purposes\(^\text{121}\). The Court provided that, the exception of the art. 3 (2) of the Directive 95/46/EC must be interpreted narrowly so that the processing of personal data falls within the exception only where it is carried out “in the purely personal or household setting of the person processing the data”. The ruling continues that video surveillance that covers even partially, a public space and is directed outwards from the private setting of the person processing the data, it cannot be regarded as an activity which is a purely ‘personal or household’ activity for the purposes of the second indent of Article 3(2) of Directive 95/46. Consequently, the CJEU ruled that:

“The second indent of Article 3(2) of 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 must be interpreted as meaning that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.”

[emphasis added]

Certainly, this ruling on the applicability under the conditions stated above of the data protection legislation on the CCTV systems installed on family houses comes to enhance the confidence of individuals, as there is no regulatory gap. However, this is only a step towards building trust with regard to the CCTV systems.

In general, privacy-related aspects of technologies, highly concern the individuals. ANEC draws attention to the access authorisation and the security of data, the transparency on data processing activities and the control of the users\(^\text{122}\). With regard to the digital environment, security and surveillance, EDRi stresses that measures such as filtering, blocking and untargeted surveillance are often easy to implement and extremely difficult to rectify\(^\text{123}\)\(^\text{124}\).

Another issue that affects the trust of consumers to the security products is the reliability and the technical complexity of the products. As identified also earlier, false negatives and false positives can pose a security risk and in turn lower the trust levels of the consumers. Low level of accuracy in technologies employed in security products and systems affects the


\(^{123}\) EDRi is an international non-profit association (AISBL) under Belgian law, promoting the protection of digital rights. Members of European Digital Rights have joined forces to defend civil rights in the information society. Currently, 33 privacy and civil rights organisations have a membership. They are based or have offices in 19 different countries in Europe. https://edri.org/about/

\(^{124}\) Read further on EDRi website: https://edri.org/theme/security-surveillance/
performance of the measure and the also the confidence of the citizen in relation to the individual security needs and its protection.

All the above issues stressed by the consumer association need to be taken into account not only in standardisation, but also in the certification of security PSS, as it will be further analysed below.

### 4.4 The Role of Evaluation and Certification schemes in Addressing the Trust Issues of Security Measures

In attempting to address the trust issue in security PSS, this section adds to the CRISP research objective a list of best practices and requirements that if addressed through an evaluation or certification scheme, they are capable of mitigating trust concerns discussed above. The evaluation and certification schemes are a means to address the mistrust of operators and citizens towards aspects and use of security products, systems and services. The evaluation and certification schemes need to fulfil the following conditions.

- **Actual Safety And Technical Reliability**

  The main factor cultivating trust to security products and systems is the actual safety it provides. An evaluation or certification scheme must look into the actual safety requirements of the security measure under evaluation and ensure that the security measure complies with the relevant safety of equipment legislation and the relevant technical standards.

- **Transparency**

  Transparency is crucial for the consumer and the scrutinised. Transparency should be met at least at two levels: in relation to the security measure and in relation to the evaluation or certification scheme itself. The evaluation scheme should be clear on what the scope of the evaluation, its evaluation procedures, the validity period of its evaluation, its rules, criteria and methodology. And this information should be easily accessible to any interested party, without additional burdens. This provides the consumer with the necessary capability to control and make a conscious choice on the product or systems he or she employs. Transparency is also substantial for building trust to the security measure; the scheme should impose transparency obligations to the security PSS under evaluation, such as open and accessible security and information policies, auditable processes and documentation. The transparency of the results of a certification – in this case through the STEFi model – should be made publicly available. This gives more accountability on what requirements were in the reality achieved, what is the exact level of compliance, instead of simply stating that certain criteria were met and thus the security PSS is certified.

- **Evaluation that takes into account freedoms and rights**
Users and scrutinised need to rely on evaluation that has specific requirements for protection of fundamental rights and freedoms. The perception of respect for human rights and freedoms by the security measure brings confidence to the affected persons. A certification scheme that takes into account the societal aspects of STEFi and in particular the freedoms and rights reinstates trust to the certified products. End users and scrutinised should be made aware what the certificate or the evaluation stands for; this entails that the scheme needs to have an appropriate reach to the market and a broadly recognised mark (trust-mark).

- **Certification That Supports Privacy And Data Protection By Design**

  Although freedoms and rights are equally important for the scrutinised to trust a security measure, privacy and personal data protection are in the spotlight the last years. This is partly the case due to the potential intrusive nature and impact that some of the security technologies might have to these two fundamental rights. In particular therefore, the need for protection of the two rights needs to be enshrined in the evaluation of the security measure. Privacy by Design requires the adoption and implementation of principles such as proactive instead of reactive protection of privacy, full lifecycle protection, visibility and transparency, privacy embedded into the design of the product or system. Data Protection by Design suggests taking into account protection of personal data in the whole lifecycle of the product, starting from the design process by building data protection safeguards in the product itself. The European Union Agency for Network and Information Security (ENISA) in a recent study recommended that standardisation bodies need to include privacy considerations in the standardisation process. According to the study, also privacy certification or privacy seals provide also a framework for privacy assessment. In line with this view, CRISP suggests the privacy and data protection requirements (as identified in the Freedom Infringement chapter) should be part of the evaluation of a security product.

- **Privacy Impact Assessment or Data Protection Impact Assessment**

  Another aspect to safeguard the protection of privacy of the individuals and accordingly their trust to the security PSS, is the Privacy Impact Assessment. PIA should be compulsory if there is a likelihood of risk to the protection of privacy and personal data, as the impact on privacy and freedoms of security PSS can be important. A PIA can grant that these rights are further protected and thus by instance also can improve the trust in a given security PSS.

---

125 Read further on the impact of the Work Package case studies on the right to privacy and data protection on sub-chapter 6.1.3. of this Report.

126 Burgess Peter, Kloza Dariusz, “Identification of practices and procedures of compliance for the use of video surveillance archives”, Deliverable D2.3. for the ADVISE project, v. 3.4., p. 9

127 Art. 23 of the draft General Data Protection Regulation introduces the concepts of Data Protection by Design and by Default

128 ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014
Since as mentioned before, trust can to a large extent be achieved through transparency, that’s why in the PIAF project, one of the main recommendations for the implementation of Privacy Impact Assessments on a European level is transparency on a threefold level:

- Stakeholder involvement throughout the PIA process
- Making the PIA reports publically available and easy accessible
- An easy accessible central registry of carried out PIAs.\(^{129}\)

But not only the accessibility of the PIA report is important for transparency and thus for trust, but also information about who did the PIA. It should be open, who undertook the PIA and how they can be contacted in order to obtain more information and advice about the PIA\(^{130,131}\).

- **Accountability**

According to the CRISP report on security standards and certification in Europe, which discussed the concept of accountability in European Standardisation, accountability in European standardisation entails “that the system is open and transparent, that the standard meets the consensus of all major interested parties and that it is applied in a uniform way throughout the territory of the Member States”\(^{132}\). The EU privacy Seals project identified accountability as one of the added values of correctly implemented privacy seal schemes\(^{133}\). An evaluation and certification scheme that requires clear distribution of responsibilities and liability issues, compliance with norms and regulations and capability of demonstration of the compliance offers a degree of confidence to the end user and scrutinised\(^{134}\). If not compliant with the accountability requirements, the certification should be subject to revocation.

---


\(^{130}\) ISO and IEC are under the process of developing a PIA methodology (ISO/IEC WD 29134), which will be published in 2016.


\(^{132}\) Wurster Simone, et. al., Report on security standards and certification in Europe - A historical/evolutionary perspective, Deliverable 2.1 of the CRISP project, 2014, p. 35


- Independence of Certification Body

Inextricably related to transparency, the independence of the Certification or Evaluation body in relation to the manufacturer or service provider is also an element substantial to increase the trust of the end users and scrutinised. EDRi, the European Digital Rights organisation, points out that “commercial trustmark schemes suffer from a tradeoff between being sufficiently thorough (which requires an often off-putting level of investment in terms of time and oversight) and being sufficiently lenient for companies to be willing to join (which can undermine the credibility of the system). EDRi urges for adequate oversight and legal underpinning. A third party evaluation therefore should provide increased warranties of impartiality and integrity; Certification bodies that are themselves accredited according to the ISO/IEC 17021 for management systems and relevant standards prove to be independent and to comply with internationally accepted requirements.

- Involvement of Stakeholders

As the CRISP Stakeholder report highlighted, the involvement of the stakeholders in standardisation and certification is of paramount importance for the quality, acceptability and trust in the end result. An evaluation or certification scheme that consults the needs of different stakeholder groups, especially the consumers, will be heard. Participation in such procedures that have an impact, boosts trust to the result, i.e. the scheme

- Regular Review of the Compliance and Updating Auditing Procedures

The after the evaluation or certification period is equally important. Recent cases of certification providers failing to meet their obligations emphasised the importance of monitoring not only the certified product after the first evaluation, but also the certification body itself for the obligations they undertake. The certification body needs to regularly review that the product, system or service continues to be compliant. Outdated certifications and control methods work in the opposite direction; they foster general public mistrust on certification and consequently to the certified security PSS.

The scheme also needs to follow the developments in technology, management, security and other fields and update its procedures and practices. The scheme can be improved by following the best practices in the field and tailoring and re-adjusting its procedures to correspond to the latest updates.


The above requirements deal with both scheme organisational aspects such as the review of compliance, the independence of the certification body, and the content in relation to the security PSS, when for instance the scheme should require reliability, transparency and accountability in the audit of security PSS.

4.5 CONCLUSION

Although the concept of trust and confidence is difficult to be captured and measured, the research based on interviews, surveys, legislation and project review showed that there are key trust issues when it comes to security products, systems and services, where the evaluation or certification scheme can have an active role in building trust.

In terms of standardisation and certification, “trust” means firm belief / confidence that the product or system:

- Respects legislation. When an organisation complies with the legislation, it conveys to consumers greater security and confidence.
- Respects fundamental rights (body integrity, equal treatment and non-discrimination, freedom of movement, freedom of unlawful detention, presumption of innocence and presumption of fair trial and due process privacy and data protection). Every individual is submitted to certain security barriers such as scanners at airports, recording cameras in closed or public spaces or surveillance by drones. In this sense, every security products, systems, services must be evaluated respecting fundamental rights so as not to infringe freedoms of people to assess the compliance with normative of freedoms.
- Respects rights and interests of consumers. Justice for growth policies aim at clear consumer and commercial rules and efficient dispute resolution both at national and EU level.
- Responds to reliability, honesty and benevolence granting security. Honesty or credibility indicates the certainty the consumer has in the business' sincerity and the fact that it keeps its promises. Benevolence is related to the consumer's belief that the company is interested in his welfare, that it does not intend to show opportunist behavior and that it is motivated by the quest for joint benefit.\(^{137}\)
- Responds to usefulness, efficiency, and efficacy to comply with its finality. Accordingly, efficiency means the resources used to achieve a particular result. However, it is sometimes confused with efficacy, which means the ability to achieve a particular result, or productivity, which is defined as the relationship between effectiveness and efficiency. To achieve it, clear consumer and

commercial rules and efficient dispute resolution both at national and EU level are important.

- Responds in a predictable and acceptable manner. The PSS provider must comply with good practices (e.g. updating the software or the information) and must act according to a manner widely recognized and used by its sector of industry.

- Has the desirable qualities for the purpose for which it is intended and involves no risk. This means that producers shall provide consumers with the relevant information to enable them to assess the risks inherent in a product throughout the normal or reasonably foreseeable period of its use, where such risks are not immediately obvious without adequate warnings, and to take precautions against those risks.

To conclude, trust on security PSS is a complex and multi-dimensional matter. Factors and variables have potential influence on the trust of the scrutinized and/ or the operators (end users) of the security measures. In this chapter, we examined the trust aspect from a legal perspective and also from a viewpoint of actual needs and perceived threats of consumers and scrutinized individuals.

The actual safety, reliability and maintenance of the security measure are distinct requirements influencing the confidence to the measure. A measure that might harm the health of the scrutinized, thus is not safe, will not be trustworthy, even though it might serve its purpose to satisfy the security needs. Together with other requirements, transparency of information and detectability of the security measure is also crucial. Covered surveillance performed with hidden CCTV systems stands among the factors that have negative impact on trust. Finally, respect for the legislation, implementation of standards, good practices and ethical codes also play a substantial role in building confidence to the security measure.

In the context of CRISP, we also examined the potential role of evaluation and certification measures in addressing the trust issues. The analysis showed that the schemes can have a significant role in addressing such issues; both with organisation and procedures of the evaluation itself and requirements relating to the security measures that are part of the audit.
5 LEGAL STUDY ON EFFICIENCY ASPECT OF SECURITY PRODUCTS, SYSTEMS AND SERVICES

This chapter examines the concept of efficiency from a legal perspective aiming to identify legal demands and special requirements for the security PSS. In order to achieve this objective, we examined the “legal” concept of efficiency in relation to the case studies of this Work Package: CCTV systems, alarm systems and drones.

5.1 EFFICIENCY FROM A LEGAL PERSPECTIVE

Efficiency is a key part in standardisation and certification but sometimes this term is confused with other terminologies\textsuperscript{138}. Despite the fact that this is an essential feature in the European market, there is no definition of efficiency in the EU legislation since it is not a legal term.

However, and as it has been mentioned above, this term is related to the fulfilment of the task to a minimum expenditure of resources, whether time, labor, materials or expenses. Therefore, based on this consideration, it can be considered actual expenditure against budgeted expenditure or it may be referred to the optimal method for accomplishing a task\textsuperscript{139}.

In public sector\textsuperscript{140}, it can be outlined efficiency of public expenditure via composite indicators. These attempts are of two broad types: macro-measurements, and micro-measurements. On the one hand, macro-measurements have as their aim an evaluation of public spending in its entirety. In other words they attempt to measure, or rather to get some ideas of, the benefits from higher public spending. On the other hand, micro-measurements attempt to determine the relationship between spending and benefits in a particular budgetary function or even sub-function (i.e. spending for industrial security control).

In private sector, productive efficiency can be defined as the capacity for a given firm to allocate its resources in such a way that makes it possible to reduce or eliminate the underutilisation of its production factors. In this area, productive efficiency is difficult to measure because it depends on various factors, some of them not being observable. In this respect, the following factors can be identified as a source of efficiency gains: intermediate

\textsuperscript{138} As it is mentioned above the term efficiency is related to the resources used to achieve a particular result. However, it is sometimes confused with efficacy, which is the ability to achieve a particular result, or productivity, which is defined as the relationship between effectiveness and efficiency, M. M. Rozenstein, “Productividad, eficacia y eficiencia en la empresa pública”, Revista de Administración Pública, pp. 59-60, 1984, pp. 76 f.


consumption (raw materials and subcontracting), labor force, productive assets, organisational gains and increase in competition\textsuperscript{141}.  

In this sense, the Court of Justice of the European Communities\textsuperscript{142} evidenced the low efficiency of private security companies due to the Spanish imposition of the following requirements:

1. The requirement of acquiring Spanish nationality. The Court of Justice observed:

"Member States must exercise their functions in the field of private security, ensuring the fundamental freedoms guaranteed by the Treaty".

2. To require the establishment of legal persons in the foreign registration scheme. Thus, the Court resolved, "The requirement of legal personality is not suitable for those reasons pursued".

3. Authorization is not recognized. It is issued by another Member State to staff of foreign companies although the requirements are similar to those required in Spain. The Court of Justice stated:

"The Spanish legislation does not provide the possibility of taking into consideration the requirements that have been accredited by the staff of enterprises in their home Member State."

Efficiency often comes to be not a means but an end in itself. This displacement of goals is a major problem in a rational society and varies according to the PSS\textsuperscript{143}.

In the EU legislation, "efficiency" does not appear often as a term. The most prominent example of use of the term in the legislation is the energy efficiency legislation. The energy efficiency Directive defines energy efficiency as “the ratio of output of performance, service, goods or energy, to input of energy”\textsuperscript{144}. The energy performance of buildings Directive establishes the requirement of cost-optimal levels of performance and of combination of improvements, which is interesting for a larger application to other products and systems, such as the security PSS\textsuperscript{145}. The aim of the requirement is to achieve a balance between the investments involved to achieve the desired performance levels and the costs saved by the investments throughout the lifecycle of the product. Another requirement that could be derived from the legislation and can be related to the concept of “efficiency” is the collective redress mechanisms requirement, which promotes procedural economy and efficiency of
enforcement. The collective redress mechanisms ensures that, in cases of mass harm to the public or a group of persons, compensation can be obtained. Apart from the individual redress, such as claiming compensation in court, collective redress may have important impact in saving time and litigation costs for both sides. The manufacturer or vendor of the security product or system should have mechanisms into place to facilitate collective redress.

5.2 Efficiency and Drones, CCTV, Alarm Systems

Technologies employed in CCTV, drones and alarm systems can be utilised in the following ways:

1. New resource efficiency technologies replace existing technologies or the state of the art in an existing application field in order to increase resource efficiency (competing technology / substitute technology).

2. Innovative functionalities of new technologies lead to new applications resulting in a higher resource efficiency (new technology field).

Regarding to Closed circuit television (CCTV), surveillance cameras serve many functions and are used in both public and private settings. CCTV has traditionally been implemented for the prevention of personal and property crime. UK is the most representative country in the usage of CCTV. Despite the use of these cameras, many authors posed the questions on whether CCTV systems for crime prevention are efficient.148

Welsh and Farrington undertook a meta-analysis of existing evaluations of CCTV pointing out their advantages and disadvantages. On the one hand, they may increase the true probability of detection, may increase pedestrian usage of places and hence further increase the probability of being subject to detection, may encourage potential victims to take security precautions, and may direct police and security personnel to intervene to prevent crime. Another possibility is that CCTV could signal improvements in the area and hence increase community pride, community cohesion, and informal social control.149 On the other hand, CCTV does not show any effect in crime prevention (with the exception of reducing crime in...
car parks) and could even cause crime to increase because they could give potential victims a false sense of security and make them more vulnerable or displace crimes to other locations, times, or victims. In terms of efficiency, a crime per year per thousand installed cameras in London is only solved (and crime reduction has resulted more effective than in other countries). In contrast, total expenditure amounted to 500 million pounds. Ultimately, CCTV cameras generate enormous costs for minimal effectiveness.

In Spain, Soto has studied the linkage between the effectiveness CCTV and crime prevention. It was evaluated 41 surveillance cameras installed in the historic centre of Malaga in April 2007. The research analysed 6,245 crimes. Violations were divided into two areas: the treatment area and control area in four areas: 10 blocks with cameras, 10 blocks near cameras, 10 blocks similar to the streets with cameras and 10 blocks with similar features to the streets near cameras. The study provides that a significant change among citizens interviewed have not seen before and after the installation of the cameras (in relation to the perception and fear of crime) although the feeling for traders who have establishments in the surveillance area of the historic centre was safer. The Cambridge Council publishes reports on efficiency against crime, including but not limited statistics referring to events referred to police, response to calls from police, pre-planned police operations, arrests, cautions/words of advice given, fixed penalty notices issued, number of images viewed, number of evidence media produced, quality of evidence, failure to establish contact with police, percentage of time CCTV operational, visitors to control room, missing persons searched for, complaints, complaints upheld, response to alarms, radio contact with retailers, radio contacts with pubs/clubs, contact with car parks/others, viewing of private areas, out of hours call service. In short, for this study it is an inefficient measure since there was not a significant reduction of crime and fear. In addition, some crimes were displaced to the adjacent streets in the area of intervention or towards streets similar to the streets with cameras. Thus, the simple inversion in CCTV is inefficient. These PSS would be much more efficient if they used with other prevention measures such as; street lighting improvement; higher technology capable of detecting facial recognition or patterns that reveal suspicious activities (foreign objects, movement patterns that may involve a fight) for early intervention or prevention thereof or other systems to enable a comprehensive efficiency (smart cities or Geographic Information Systems, GIS).

Efficiency is considered in a different way in drones. They have most often been associated with national security in terms of efficiency, as they were considered as an

---


152 They are more known as unmanned aerial vehicles (UAV), a flying robot remotely controlled or able to fly autonomously through software-controlled flight plans in their embedded systems working in conjunction with
efficient, effective way to gather intelligence and target suspected terrorists\textsuperscript{153}. When it comes to the civilian use of drones, one can find many applications such as search and rescue, surveillance, law enforcement, inspect electricity networks, carry out aerial mapping, among other things\textsuperscript{154}.

Regarding to the economic efficiency, Europe does not yield information about the savings that the use of drones would result. However, the US CBP's Office of Air and Marine has calculated the cost of operating a drone at $2,468 per hour and the inspector general's office put the actual hourly rate at $12,255 without including key expenses such as salaries for operators and equipment\textsuperscript{155}.

It is estimated that drones are products huge added value because its effectiveness is relatively higher compared to other current PSS\textsuperscript{156} and in a near future, it is likely that drones will increasingly include more and more automated and autonomous features to help them fly more efficiently and operate with a higher level of safety. This includes elements such as predefined flight-paths using GPS, “sense-and-avoid” systems, and safety mechanisms that are activated automatically in the event of pilot or communications failure\textsuperscript{157}.

Thus, the effectiveness of the solutions to be adopted to mitigate the risks associated with the use of drones for civilian purposes will depend on the ability of the EU and national legislation, commercial bodies and individuals to coordinate their operations although new technological developments in the future as well as decreased operating costs will likely boost the use of unmanned aircraft systems for commercial purposes such as industrial/agricultural monitoring, video surveillance and commercial deliveries\textsuperscript{158}.

Finally and regarding to alarm systems, European providers and users of security P/S/S are represented by major organisations, such as:

- The European Organisation for Security (EOS), representing providers of equipment and technology-based solutions and services

\footnotesize{GPS. For more information about this new technology, see monographic on drones in \textit{Computer Law & Security Review}, n° 30, 2014.}


\footnotesize{\textsuperscript{154}A remarkable use for drones can be appreciated in commercial area. Nowadays, Amazon and Dominos pizza have already placed advertisements on YouTube suggesting that deliveries will be affected more efficiently with the use of drones. So, equipped with a GPS, drones used in this context will be able to gather location data corresponding to the addresses of their customers increasing competitiveness of technology companies. (Finn, R. L., D. Wright and A. Donovan, \textit{"Privacy, data protection and ethical risks in civil RPAS operations"}, D3.3: Final report for the European Commission. Trilateral Research & Consulting, LLP, p. 35).}

\footnotesize{\textsuperscript{155}Office of Inspector General, Department of Homeland Security, \textit{Report on U.S Customs and Border Protections and Unmanned Aircraft System Program does not achieve intended results or recognised all cost of operations.}, December 2014.}

\footnotesize{\textsuperscript{156}Compared to human activities, their benefits include; reliability, accuracy, rapid operation, quick adjustment to take account of new data and less expensive than a human equivalent, particularly for work involving a modest amount of variability but within a general pattern.}

\footnotesize{\textsuperscript{157}Finn, R. L., D. Wright and A. Donovan, \textit{"Privacy, data protection and ethical risks in civil RPAS operations"}, op. cit., p. 348.}

\footnotesize{\textsuperscript{158}Pecoraro, Y., \textit{Can drones break into the commercial market?}, Portolano Cavallo Studio Legale, 3 April 2014}
The Confederation of European Security Services (CoESS), representing providers of skilled guarding services and security systems operators

The European Corporate Security Association (ECSA), representing corporate users of security solutions and services.

Although the main objective of each organisation is to represent the interests of the groups it represents, these three organisations share the common goal of reaching an adequate level of security, in line with the European ideals of freedom, security and justice. Through periodic consultations and where joint interests exist, they draft common position papers and voice-shared views.\(^{159}\)

The EU acknowledges that private security companies constitute a part of a state’s security system. However, no harmonisation of legislation concerning the private security industry at the European level has yet taken place despite the fact that the European Court of Justice has established its competence over matters related to the private security industry, considered an economic sector of the EU and therefore falls under the regulation of the internal market.\(^{160,161}\)

5.3 Conclusion

The chapter presented the legal study on the efficiency aspect of security products, systems and services. Although efficiency is not a legal term, the study revealed aspects of efficiency derived from the legislation or aspects that can be related to legal criteria and requirements such as the minimum performance requirements, the cost-optimal investments etc. The case studies of CCTV systems, alarm systems and drones provided useful insight on further demands in relation to efficiency. These requirements are useful to the work of CRISP, as they could be included in an evaluation or certification scheme, so that the security PSS is tested against them.

\(^{159}\) Confederation of European Security Services (CoESS) Website: [http://www.coess.org/](http://www.coess.org/).

\(^{160}\) It is appropriate to note that EU Directive for services in internal market does not apply to private security companies. CoESS justified this exception due to the specific nature of private security services – meaning its close links to public security – and the obligation of severe conditions to enter the market. These two reasons are sufficient to consider that the general provisions of the directive wouldn’t fit into the necessities of the sector. See Joint Declaration by CoESS and UNI-Europa, *Towards a European Model of Private Security*, Madrid, 14 & 15, October 2004, p. 3.

\(^{161}\) “For example, in 2003 it was argued in the European Court of Justice that Spanish legislation on private security did not comply with the principles of freedom of establishment and the free movement of services as set out in Articles 43 and 49 of the Treaty (Action brought on 8 December 2003 by the Commission of the European Communities against the Kingdom of Spain). In another case, the constraints that the Netherlands places on the private security companies that wish to provide services on its territory were considered unjustified by the Commission, and it was claimed that these constraints breached Directives 89/48/EEC and 92/51/EEC on a general system of professional recognition of qualifications (Action brought on 5 May 2003 by the Commission of the European Communities against the Kingdom of Netherlands). Therefore, in these rulings, the European Court of Justice has established its competence over matters related to the private security industry, as it is considered an economic sector of the EU and therefore falls under the regulation of the internal market.” SOURCE: Hans Born, Marina Caparini and Eden Cole, Regulating Private Security in Europe: Status and Prospects, Geneva Centre for the Democratic Control of Armed Forces (DCAF), Policy Paper n. 20, 2007, p. 7 [http://www.dcaf.ch/content/download/35400/526017/file/PP20_Born_Caparini_Cole_.pdf](http://www.dcaf.ch/content/download/35400/526017/file/PP20_Born_Caparini_Cole_.pdf)
6 LEGAL STUDY ON FREEDOM INFRINGEMENT IN THE CONTEXT OF SECURITY PRODUCTS, SYSTEMS AND SERVICES

Another core dimension of the security PSS evaluation is the analysis of the impact of technologies and security measures on the freedoms of people. These freedoms include: bodily integrity, equal treatment and non-discrimination, freedom of movement, freedom of unlawful detention, presumption of innocence, fair trial and due process, privacy and data protection. In this chapter, we analyse how and under which circumstances the security products, systems and services might violate the above rights and freedoms and we identify core requirements and legal demands for their protection.

6.1 PRIVACY AND PERSONAL DATA PROTECTION

6.1.1 The right to private life and the core legal requirements for security products, systems, services

Perhaps the most prominent issue in the security industries is balancing security versus privacy. The crux of the issue is about forfeiting privacy in the name of security. The issue has gained momentum especially after 9/11 and is often in the media spotlight. Security measures and practices that once seemed like science fiction are now common, with more acceptance by society as a whole. But is it really necessary to sacrifice privacy for security? Raab observes that advocates of civil liberties see the use of personal data in national security as a violation of privacy, whereas the supporters of those policies tend to see privacy as an obstacle. Arguments such as: “If you’ve got nothing to hide, you’ve got nothing to worry about” are flawed. The debate between privacy and security is not necessarily a zero-sum game in which you can only choose between one value and the other. Protecting privacy does not have a cost over security measures; it merely involves adequate oversight and regulation.

Privacy has many aspects; the PRESCIENT project suggests variations as to the types of privacy:

Privacy of the person

Privacy of the person means, that everyone has the right to keep his body functions and characteristics private (e.g. biometrics). So mainly all biometric technologies like

body scanners, facial recognition and the databases processing these biometric data have a potential of conflicting with this type of privacy.

**Privacy of thoughts and feelings**
This means essentially that individuals have the right to not have their thoughts and feelings shared or revealed without their consent. Here again biometrical technology, mainly facial recognition systems can not only identify persons based on their facial characters but also evaluate whether a person is happy, sad, anxious or stressed – which thus challenges the privacy of thoughts and feelings, as this is often not known to citizens.

**Privacy of location and space**
This type of privacy gives citizens not only the right to go wherever they want without being monitored, of course without interfering with other people’s privacy, but also the right to have privacy in one’s home, car or workplace. This privacy conception is in conflict with a wide range of technologies: CCTV systems in public spaces have the possibility to monitor the movement of citizens while CCTV systems in private places can risk the privacy of citizens in their home (if not installed correctly). RFID chips in travelling documents like passports can likewise monitor location-data.

**Privacy of data and image**
Similar to the privacy of thoughts and feelings, the privacy of data and image gives citizens the rights that their personal data and images are not processed, shared and revealed without their consent. There are again a lot of technologies challenging this type of privacy, as data is often processed without the data subject knowing about it. Examples are once again RFID chips, being able to communicate with readers without the person carrying the chip knowing it, or for example full body scanners which also have the potential of storing the captured image.

**Privacy of behaviour and action**
Personal behaviour and actions in public as well as in private spaces are also an important privacy feature. While behaviour can be casually observed, a systematic processing of behavioural data should be refrained – a person should be able to behave in public as he or she wishes within the legal boundaries without fearing to be monitored (similar to the privacy of location and space). Also here facial recognition or behavioural recognition in CCTV systems have a large potential of conflict with this type of privacy.

**Privacy of personal communication**
Privacy of personal communication should grant the citizens the right that their communication is not intercepted in any way, be it mail, e-mail or phone communication. Citizens should have the right to communicate between each other.
Free communication is essential, also for the exercising of democratic rights. On the one hand, the breach of privacy can be intentional from the governmental side – mainly under the cover of crime and terrorism prevention, there can on the other hand also be interceptions of communication from private companies, especially with e-mail communication.

**Privacy of association (including group privacy)**

Finally the privacy of association means that people should be able to meet with other people – in public as well as in private – without being specifically monitored. This relates to the privacy of location, which is why this type of privacy also can be challenged by CCTV surveillance, especially if surveillance is targeted on specific groups of citizens (on the basis of gender, race, appearance, etc.).

These are insofar important here as different technologies can be a risk for different types of privacy\(^{165}\) and thus should be taken into consideration for the evaluation of security PSS. RFID-enabled travel documents for example can be a risk for the privacy of location and space, data and image as well as of behaviour and action.

The right to respect for private and family life as established in Article 8(1) of the ECHR\(^ {166}\): “Everyone has the right to respect for his private and family life, his home and his correspondence”. This provision however focuses on the right from interference by a public authority, whereas Article 7 of the Charter of Fundamental Rights of the European Union speaks about the right to privacy from any kind of interference – public or private\(^ {167}\): “Everyone has the right to respect for his or her private and family life, home and communications”.

Since one of the major impacts of security products and services on human rights regards the interference with the right to privacy, a more detailed analysis is in place of when exactly an individual interference (a security product or service) is legally (not)allowed. The issue was elaborated specially through extensive case law of the ECtHR.

Article 8(2) of the ECHR provides that:

> “There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

Interference therefore requires justification; that is, under Article 8 of the ECHR:

a) it must be in accordance with the law,

b) it must pursue one or more legitimate aims and, in addition,

\(^{165}\) Ib., p. 15.

\(^{166}\) Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8.

c) it must be “necessary in a democratic society” to achieve those aims.

An interference with an individual’s Article 8 rights by a security measure must therefore satisfy all three criteria of the test in order for it to be justified.

In the case of *MM v United Kingdom*\(^\text{168}\) the ECtHR set out the criteria that must be met for an act or activity to be “in accordance with the law”. An activity must:

- have basis in domestic law and be compatible with the rule of law; and
- the law must be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual to regulate his or her conduct.

The second criterion, the pursuit of a legitimate aim, requires that an activity is carried out in pursuance of one of the aims set out in Article 8(2), e.g. public safety, the prevention or detection of disorder or crime, protection of the rights and freedoms of others, the economic well-being of the country.

The criterion “necessary in a democratic society” is probably the most difficult one. There have been a number of cases before the ECtHR that have all referred to one or more of the tests the ECtHR has set for itself when determining whether a measure is “necessary in a democratic society”\(^\text{169}\):

- **Pressing social need** - Does the interference by the security measure correspond to a pressing social need?
- **Proportionality** – Is the interference caused by the measure proportionate to the legitimate aim being pursued?
- **Relevant and sufficient reasons** – Were the reasons given to justify the interference relevant and sufficient?

The Court of Justice of the European Union (CJEU) also developed its own understanding of the principles of necessity and proportionality relating to the application of Articles 7 and 8 of the Charter. In its *Schwartz case*\(^\text{170}\) the CJEU started its analysis with Article 52(1) and reiterated that limitations to fundamental rights must:

a) be provided for by law,

b) respect the essence of those rights,

c) and, in accordance with the principle of proportionality, be necessary,

d) and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

---

\(^{168}\) European Court of Human Rights, case of MM v United Kingdom, No. 24029/07, 13 November 2012.


\(^{170}\) Court of Justice of the European Union, case of Schwarz v. Stadt Bochum, C-291/12, 17 October 2013.
Having a closer look at the question of proportionality and necessity, the CJEU said that it “must establish whether the limitations placed on those rights are proportionate to the aims” and “to the objectives” (of the relevant legislation). “It must therefore be ascertained whether the measures implemented are appropriate for attaining those aims and do not go beyond what is necessary to achieve them”. Furthermore, the Court said that: “in assessing whether such processing is necessary, the legislature is obliged, inter alia, to examine whether it is possible to envisage measures which will interfere less with the rights recognised by Articles 7 and 8 of the Charter but will still contribute effectively to the objectives of the EU rules in question”. More recently still in its judgement on the Data Retention Directive 2006/24/EC, the CJEU declared that since the directive entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary, it is invalid.

The interpretation of when a security service/product is in line with the requirements of Article 7 of the Charter is similar to the one elaborated by the ECHR as regards Article 8 of the Convention. Any interference with the right to privacy caused by a security PSS (1) must be provided for by law, (2) must respect the essence of the right to privacy, (3) must be necessary and (4) must genuinely meet the objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

Regarding the certification of security PSS, upon considering the important separation between privacy and data protection, one has thus to evaluate the PSS regarding two different legal compliances. A PSS that does not risk a person’s freedom rights needs to make

---


173 Court of Justice of the European Union, Joined cases C-293/12 and C-594/12 - Digital Rights Ireland, Seitlinger and Others, 8. April 2014.

174 De Hert and Gutwirth draw the line on the distinction between the two notions and human rights: data protection is a lot more than just what is related to privacy, it formulates the conditions under which processing is legitimate. The wording of the Convention on Data Protection (1981) provides guidance on the relation of the two rights: data protection is both wider and more specific than the protection of privacy. They explain that “it is wider since it also relates to other fundamental rights and freedoms of individuals, such as equality and due process. It is at the same time more specific, since it only deals with the processing of personal data”: De Hert Paul, Gutwirth Serge, “Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. Reinventing data protection”, 2009, pp.3 - 45, eds. S. Gutwirth, Y. Poullet, P. De Hert, J. Nouwt, C. De Terwangne, Springer.
sure not to interfere with the private and family life as well as with his home and communications, but also that when personal data is processed, that this is done in a – for the concerned person – transparent manner and his rights to access to his personal data, including the right to correction, are always granted.

<table>
<thead>
<tr>
<th>Source of legal obligation</th>
<th>Relevant article</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Convention for the Protection of Human Rights and Fundamental Freedoms</td>
<td>Article 8 – Right to respect for private and family life</td>
</tr>
<tr>
<td>Charter of Fundamental Rights of the European Union</td>
<td>Article 7 – Respect for private and family life</td>
</tr>
<tr>
<td></td>
<td>Article 52(1) - Scope of guaranteed rights</td>
</tr>
<tr>
<td>Treaty of the European Union</td>
<td>Title I – Common Provisions – Article 6</td>
</tr>
</tbody>
</table>

Table 6: Normative on the right to protection of personal life
Source: Own table

To conclude with, in terms of standardisation and certification, a security PSS that interferes with the right to private life of the individual(s), should:

- Interfere with the right to privacy only when this is prescribed by a specific law, which provides clearly defined rules governing the legal framework in which the security activity will operate. The law has to be accessible to the individuals whose privacy is restricted eg. published, sufficiently clear and precise.
- Pursue a legitimate aim; that is national security, public safety, public order, health or morals, protects rights or freedoms of others.
- The interference caused by the security product/service must in addition be “necessary in a democratic society” to achieve the aim being pursued, which means that (1) it must be based on a pressing social need, (2) its interference must be proportionate to the legitimate aim being pursued and (3) based on relevant and sufficient reasons. The security measure that interferes with the right to private life of the scrutinised must be the ultimate means available. In case there are less intrusive means available then the latter must be chosen.
6.1.2  The right to the protection of personal data

The fundamental legal provisions for personal data protection in Europe\(^{175}\) are laid down in the Charter of Fundamental Rights of the European Union and in the 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 (the Data Protection Directive)\(^{176}\). The Convention 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe has also been historically of great importance in the protection of personal data in setting the principles and fundaments on which the EU legislation was based\(^{177}\).

The Charter of Fundamental Rights of the European Union, legally binding as EU primary law since the entry into force of the Lisbon Treaty in 2009, not only guarantees the respect for private and family life (Article 7), but also establishes the right to data protection (Article 8), explicitly raising the level of this protection to that of a fundamental right in EU law. Formulated several years after the Data Protection Directive, Article 8 of the Charter must be understood as embodying pre-existing EU data protection law. The Charter, therefore, not only explicitly mentions a right to data protection in Article 8 (1), but also refers to key data protection principles in Article 8 (2). Finally, Article 8 (3) of the Charter ensures that an independent authority will control the implementation of these principles.

6.1.2.1  The Data Protection Directive in the context of Security Products, Systems and Services

Before examining the provisions of the Directive that are relevant to the security products, systems and services, it should be noted that art. 3 of the Directive provides that the Directive is not applicable to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law (art.3). However, the WP29 draws attention to the lack of definition of “national security” which stimulates legal uncertainty as to the scope of the exemption. The WP29 also observes that Directive should not be considered irrelevant in the context of law enforcement and national security matters, since the national laws implementing the Directive do govern the transmission of personal data from data controllers and processors when they are ordered to submit information to intelligence services and law enforcement authorities. As a result, even though


\(^{176}\) Read further on the distinction of the right to private life and the right to protection of personal data in the jurisprudence of the Court of Justice of the European Union: Gonzalez Fuster Gloria, “Fighting For Your Right to What Exactly? The Convoluted Case Law of the EU Court of Justice on Privacy and/or Personal Data Protection”, Birkbeck Law Review Volume 2(2), 2014

a security measure might pursue national security purposes, the Data Protection Directive should not be disregarded. Moreover, the right to personal data is protected as a fundamental right, on the basis of the art. 8 of the Charter of Fundamental Rights of the EU and may be restricted only to the extend and under the conditions foreseen in the Charter; it is also protected by the Convention 108 of the Council of Europe and the European Convention of Human Rights as an aspect of the right to private life.

The concept of “personal data” is defined in the Data Protection Directive. Article 2 provides that “personal data” shall mean any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

A thorough analysis on the concept of personal data is provided by the Article 29 Working Party (WP29)\textsuperscript{178} in its opinion No 4/2007\textsuperscript{179}. The WP29’s analysis is otherwise based on four main “building blocks” that can be distinguished in the definition of “personal data”: i.e. “any information”, “relating to”, “an identified or identifiable”, “natural person”. These elements are closely intertwined and feed on each other, but together determine whether a piece of information should be considered as “personal data”\textsuperscript{180, 181}.

\textsuperscript{178} Article 29 Working Party was set up under the Data Protection Directive and is composed of representatives of national supervisory authorities, the European Data Protection Supervisor and a representative of the European Commission.


\textsuperscript{180} The first element – “any information” – calls for a wide interpretation of the concept, regardless of the nature or content of the information, and the technical format in which it is presented. This means that both objective and subjective information about a person in whatever capacity may be considered as “personal data”, and irrespective of the technical medium on which it is contained. The second element – “relating to” – has so far been often overlooked, but plays a crucial role in determining the substantive scope of the concept, especially in relation to objects and new technologies (also security). The third element – “identified or identifiable” – focuses on the conditions under which an individual should be considered as “identifiable”, and especially on “the means likely reasonably to be used” by the controller or by any other person to identify that person. The particular context and circumstances of a specific case play an important role. The opinion also deals with “pseudonymised data”, which are often used in the context of security products and services, which still present personal data. The fourth element is – “natural person” – and deals with the requirement that “personal data” are about “living individuals”. The opinion also discusses the interfaces with data on deceased persons, unborn children and legal persons.

\textsuperscript{181} The CJEU issued in 2014 a significant decision on the meaning of personal data: YS v Minister voor Immigratie. It suggested a narrow definition limited to the facts and/or information necessary for the data subject to exercise their rights. The most obvious relevance is to limit the information that must be provided in response to a subject access request, though the decision will have wider ramifications as well. In deciding whether the minutes made by the Dutch immigration office in deciding on immigration applications contain personal data and should as such be provided to applications based on subject access requests, the Court found that factual data about the applicants, i.e. “name, date of birth, nationality, gender, ethnicity, religion and language”, was the applicants’ personal data. In contrast, the legal analysis, whilst it may contain personal data, was not itself personal data. See Court of Justice of European Union, joined cases of C-141/12 and C-372/12 - YS and Others, 17 July 2014.
The Directive speaks also of special categories of personal data, which, by their nature, may pose a risk to the data subjects, when processed, and need enhanced protection. The processing of these special categories of data ("sensitive data") is in principle prohibited, unless the specific conditions of art. 8(2) are met. On the definition of sensitive data, the Data Protection Directive (Article 8) names the personal data revealing racial or ethnic origin; political opinions, religious or philosophical beliefs; trade-union membership, health or sexual life. Security measures such as access control alarm systems using biometrics, might need to comply with the provisions of the Directive on sensitive data, since biometric data might reveal information on the health of a person\(^{182}\).\(^{183}\)

For example, the CJEU in *Bodil Lindqvist*\(^{184}\) case stated that “reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8 (1) of Directive 95/46”. In case a security product/service includes the processing of (also) sensitive data, specific safeguards are provided for such processing in Article 8 of the Data Protection Directive.

An important aspect of the protection of personal data in the case of security measures is the data controller. Data controller is the natural or legal person who defines the means and the purposes of the processing of the personal data (art.2 DPD). Looking at the case studies of this Report, we see that among other elements, the context in which every security measure operates helps determine who is the data controller. In the case of CCTV systems in public spaces for crime prevention and detention, the authority that decides the purposes processing operations and how the images and other personal data are processed and handled is data controller. Biometric alarm systems for access and intruder control established in private spaces indicate the data controller as the person, natural or legal, who decided the installation of the system, processes the data for the purposes of protection of the private property (or other) and determines the means for the processing of the personal data. One should also note that, the several entities deciding on issues relevant to the security measure quite often outsource or sub-contract the whole or part of the processing operations. For example biometric alarm systems established in private properties might be centrally operated by a private security company. In those more complex cases, specific attention should be paid on the question of distribution of responsibilities and to the determination of the person to the controller or joint-controller, which is may be assessed according to the factual circumstances\(^{185}\).

---

\(^{182}\) Article 29 Data Protection Working Party, Opinion 3/2012 on developments on biometric technologies, WP193, 27 April 2012

\(^{183}\) Read further on biometric data and the data protection risks on the section on “Impact of biometrics alarm systems on the right to protection of personal data” of this study

\(^{184}\) Court of Justice of European Union, case of Bodil Lindqvist, C-101, 6 November 2003.

\(^{185}\) The WP29 in its opinion 1/ 2010 on the concepts of “controller” and “processor” underlines the difficulty of determining the data controller due to the organisational differentiation in the several sectors and the globalisation of the ICT sector. The opinion suggests three approaches to the concept of controller: 1) the control stems from explicit legal competence. “The law may impose an obligation on either public or private...
A security PSS that processes personal data needs to comply with the principles related to the quality of the personal (article 6, the DPD). In particular, in terms of standardisation and certification, the right to protection of personal data, entails that the security PSS which processes personal data, encompasses the following principles:

- principle of fair and lawful processing;
- principle of purpose limitation;
- principle of necessity and proportionality;
- principle of accuracy and up-to-date.

Fair processing requires transparency of processing. The controller of the personal data is obliged to inform the data subject, before starting to process personal data, about the identity of the controller and the purpose of the data processing (art.10). Further information should be given where this is necessary, having regard to the specific circumstances in which the data are collected in order to guarantee fair processing in respect of the data subject – information on the recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, the existence of the right of access to and the right to rectify the data concerning him.

Purpose limitation and purpose specification aim to ensure that security organisations/authorities/entities are open about the reasons for obtaining personal data through the functioning of their security products/services, as well as that what they do with the information is in line with the reasonable expectations of the individuals concerned. In practice, the principle of purpose limitation and specification means that security organisations must be clear from the outset about why they are collecting personal data and what they intend to do with it. Any new purpose of processing, incompatible with the original one, requires a separate new legal basis. Also disclosure of data to third parties usually constitutes a new purpose and therefore requires a legal basis distinct from the one for collecting the data. For an example, all airlines collect data from its passengers to make bookings to operate the flight properly. If an airline is asked to transfer these data (the so called PNR data)186 to the immigration authorities at the port of landing, which will use them for security and immigration control purposes, which differ from the initial data collection purpose, this transfer of data to an immigration authority requires a new and separate legal basis.

186 “Passenger Name Record (PNR) data is information provided by passengers and collected by air carriers during reservation and check-in procedures. It includes several different types of information, such as travel dates, travel itinerary, ticket information, contact details, baggage information and payment information”: European Parliament EU Passenger Name Record (PNR) proposal: what’s at stake, 26 January 2015, http://www.europarl.europa.eu/news/el/news-room/content/20150123BKG12902/html/EU-Passenger-Name-Record-%28PNR%29-proposal-what%27s-at-stake; also: European Commission, Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, February 2011
The principle of proportionality means that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. A CCTV installed in a car park in order to insure better protection of cars could collect more images—for example on people going to shop in the nearby mall—than necessary to fulfil the purpose of their collection, i.e. to raise the security level in the car park. This purpose could namely also be achieved by employing a security guide or at least by improving the lightning in the car park (which means no processing of personal data at all)\(^{187}\). Moreover, data collected and processed need to be accurate and up-to-date. A controller should take reasonable steps to ensure the accuracy of any personal data it processes; that the source of any personal data is clear; that any challenges to the accuracy of information and whether (or when) it is necessary to update the information should be carefully considered. Retention of the personal data should be only for as long as is justified for the purposes for which they are collected\(^{188}\).

The main purpose of these principles is to protect the interests of the individuals whose personal data is being processed. If applied to security products and services, the principle of fairness and legality refers to the requirement that all security measures functioning based on or at least including some data processing (e.g. CCTV filming images of identifiable individuals, drones fitted with a cameras and not used for domestic purposes\(^{189}\)) need to have legitimate grounds for collecting and using the personal data (basically this refers to the need for a legal basis or consent of the data subject); must not use the data in ways that have unjustified adverse effects on the individuals concerned; the data controller must be transparent about how he intends to use the data, and give individuals appropriate privacy notices when collecting their personal data; must handle people’s personal data only in ways they would reasonably expect; and must make sure noting unlawful is done with the data processed.

The criteria for making data processing legitimate is further elaborated in Article 7 of the Directive, which provides that personal data may be processed based on:

a) unambiguous consent of the data subject;

b) (pre-)contractual relationship of the data subject;

c) compliance with a legal obligation of the controller;

d) protection of vital interests of the data subject;

---

\(^{187}\) See Information Commissioner’s Office, “In the picture; A data protection code of practice for surveillance cameras and personal information”, v. 1, 15 October 2015, p.8

\(^{188}\) Read on retention: Court of Justice of the European Union, Joined cases C-293/12 and C-594/12 - Digital Rights Ireland, Seitlinger and Others, 8. April 2014.

\(^{189}\) The use of personal data by private individuals is completely exempt from the Data Protection Directive’s remit where such use falls within the boundaries of the so-called household exemption. The household exemption is the use of personal data by a natural person in the course of purely personal or household activity (Article 3 (2)). Besides, the Directive also doesn’t apply to the processing of personal data for purposes concerning public security, defense, State security and the activities of the State in areas of criminal law and/or in the course of any other activity which falls outside the scope of Community law.
D4.1: Legal Analysis of Existing Schemes

The entity employing the security measure needs to fulfil one of the above criteria. The legal basis for the legitimacy of the processing depends on the nature of the security product, as well as to other factors, such as the purposes and the environment to which the security measure operates. For instance, in the case of UAVs (drones) recording images in public spaces, one cannot easily imagine how any data processing would be based on the consent of the data subjects, given the vast amount of images and the number of data subjects. In this case, the controller would need – prior to the collection of the data - another legal basis for the processing.

The security obligation of art. 17 DPD means that data controller must have appropriate security measures in place to prevent the personal data it holds being accidentally or deliberately compromised. In order to do so, the data controller needs to:

- design and organise its security to fit the nature of the personal data it holds and the harm that may result from a security breach;
- be clear about who in its organisation is responsible for ensuring information security;
- make sure it has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff;
- and be ready to respond to any breach of security swiftly and effectively.

Information security breaches may cause real harm and distress to the individuals they affect. Examples of the harm caused by the loss or abuse of personal data (sometimes linked to identity fraud) include: fake credit card transactions, witnesses at risk of physical harm or intimidation, offenders at risk from vigilantes, fake applications for tax credits, mortgage fraud etc. Not all security breaches have such grave consequences, of course. Information security breaches have made it clear that information security is an issue of public concern as well as technical compliance. If personal data is not properly safeguarded, this can seriously damage an organisation’s reputation and prosperity and can compromise the safety of individuals190,191.

Finally, it is essential that the data controller facilitates the exercise of the rights of the data subjects. The controller of a security measure that is collecting personal data, such as names,
ages, addresses, images, biometrics, travel information and others, has to guarantee that the scrutinised has access to the personal data and to information relating to processing, rectify incomplete or inaccurate data, block the data whose accuracy is contested, erase the data if the processing is unlawful\textsuperscript{192}.

\subsection*{6.1.2.2 Core Requirements applicable to Security PSS from the General Data Protection Regulation}

In order to provide for a harmonisation of the data protection regulations throughout the EU and in order to also consider important aspects like globalisation and technological developments sufficiently, the European Commission proposed a reform of the EU’s data protection rules. The reform consists of a draft regulation setting out a general EU framework for data protection and a draft directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. The proposals are currently being discussed by the two EU co-legislators.

The European Commission draft of the General Data Protection Regulation\textsuperscript{193} though still in the process of negotiation, offers additional safeguards and requirements for security PSS in the context of CRISP\textsuperscript{194,195}. Currently, based on the initial draft Regulation (EC) and the amendments made in the European Parliament, the provisions that are relevant for security products and services are primarily the following:

\textbf{Accountability}

Article 22 takes account of the debate on a “principle of accountability” and details the obligation of responsibility of the controller to comply with the GDPR and to demonstrate the compliance to its provisions, including by way of adoption of internal policies and

\textsuperscript{192}~Read further on the rights of the data subjects in European Data Protection Supervisor, Guidelines on the Rights of Individuals with regard to the Processing of Personal Data, no date, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/14-02-25_GL_DS_rights_EN.pdf


\textsuperscript{194}~On territorial scope, flexibility in the rules for organisations and one stop shop concept. It is not yet clear, to what extent the provisions relevant for security services and products will be affected by amendments and negotiations in the future.

mechanisms for ensuring compliance. The measures the controller needs to undertake, relevant in the context of security products and services, include keeping documentation of data processing, implementing security requirements, performing a data protection impact assessment.

**Data Protection by Design and by Default**

Article 23 sets out the obligation of the controller arising from the principles of data protection by design and default. Having regard to the state of the art and the cost of implementation, the controller is supposed to, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures in such a way that the processing will meet the requirements of the regulation and ensure the protection of the rights of the data subject. This provision takes into account the so called data protection by design principle. Another principle, introduced by the regulation, is the data protection by default principle. The controller must ensure that by default only those personal data that are necessary for each specific purpose are processed and are especially not collected or retained beyond the minimum necessary for those purposes.

Substantial for the implementation of these principles by the industry is the role of the Data Protection Authorities providing guidance or with other similar endeavours such as the Internet Privacy Engineering Network (IPEN). IPEN was founded by the European Data Protection Supervisor together with other Data Protection Authorities, with the aim “to integrate data protection and privacy into all phases of the development process, from the requirements phase to production, as it is most appropriate for the development model and the application environment”.

**Secure processing**

Article 30 obliges the controller and the processor to implement appropriate measures for the security of processing, extending that obligation to processors, irrespective of the contract with the controller. The measures must be appropriate to the risks represented by the processing and the nature of personal data to be protected, having regard to the state of the art and the costs of implementation. The measures must protect personal data against accidental or unlawful destruction or accidental loss, unauthorised disclosure, dissemination or access, or alteration. Security PSS need to ensure secure processing of personal data. A biometric access alarm for instance requires a security level appropriate to the risks and the nature of

---


197 Read further on IPEN and its work: [https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN](https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/IPEN)
the data and requires that potential vulnerabilities are adequately handled\textsuperscript{198}. Solutions such as encryption and logging and access control measures are essential to that end\textsuperscript{199}.

**Security breach notification**

Articles 31 and 32 introduce an obligation to notify personal data breaches, building on the personal data breach notification in the ePrivacy Directive. In case of a personal data breach the controller must notify the supervisory authority, and in case the breach may have adverse effect on the privacy of individuals, inform the affected individuals as well. The latter do not need to be informed if the controller has implemented appropriate technological protection measures that render data unintelligible to any person unauthorised to access it.

**Data Protection Impact Assessment**

Article 33 introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to risky processing operations. Such especially include cases of extensive profiling that may produce legal effects concerning individual or significantly affect the individual, cases when especially sensitive data are being processed, when monitoring publicly accessible areas, etc.\textsuperscript{200}

**Certification**

A significant provision, related to the work of CRISP, is introduced by article 39 of the GDPR. The proposed article encourages certification mechanisms and data protection seals and marks, which will allow the data subjects to quickly assess the level of data protection provided by controllers and processors. The role of the data protection certification mechanisms is to contribute to the proper application of the GDPR, by taking account of the specific features of the various sectors and different processing operations. The suggested amendment ( amend. 136) of the European Parliament includes more detailed provisions for

\textsuperscript{198} Kindt Els, *Privacy and Data Protection Issues of Biometric Applications, A comparative legal analysis*, Springer 2013, p.873

\textsuperscript{199} See further section 6.1.3.3. of this Report on the Impact of biometrics of alarm systems to the right to protection of personal data.

\textsuperscript{200} SAPIENT describes a method for identifying, assessing (or evaluating) and prioritising that allows for treating risks arising from the development and deployment of surveillance technologies, systems and applications. This builds on long-standing approaches under the umbrella term of Privacy Impact Assessment (PIA). Such a methodology assesses any surveillance deployments with regard to their impacts on privacy. The purpose of a surveillance impact assessment (SIA) is to assess the risks a surveillance-related project, policy, programme, service, product or other initiative poses for privacy, as well as for other human rights and ethical values. One of the main tenets is that the further upstream any PIA is built into the process of PSS development and deployment, the greater the chances to succeed – in terms of leading to the design of societally robust security measures. This includes aspects such as: how to configure a surveillance system in such a way as to avoid being unduly intrusive and what safeguards should be put in place to ensure that it does not infringe upon democratic aspirations. A PIA, therefore, aims to identify consequences from proposed projects or actions and prioritise those (unintended, negative) consequences with regard to likelihood in terms of classical risk management. It is through the implementation of a PIA in a specific setting and geared at a specific (proposed or implemented security measure) that anticipatory knowledge about negative effects on privacy can be delineated.
the role, purposes and organisation of such schemes, including provision for a “European Data Protection Seal”.

### 6.1.2.3 ePrivacy Directive and Security Products, Systems and Services

The Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) - as amended and valid - has been drafted specifically to address the requirements of new digital technologies and ease the advance of electronic communications services\(^{201}\). The Directive complements the Data Protection Directive and applies to all matters in the electronic communications sector which are not specifically covered by that Directive. Contrary to Data Protection Directive, which specifically addresses only individuals, ePrivacy Directive also applies to legal persons. In case of the security products, systems and services the ePrivacy has limited applicability; it is not applicable to public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Moreover, in the context of security PSS, the provisions of the Directive are applicable to the extent they concern or are related to the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices (art.3). Confidentiality of information, secure processing, data breach notification and location data are safeguarded in the Directive. When information collected from a security measure or in the context of a security service is communicated, over a public communications network, then the above requirements are substantial for the protection of such information.

### 6.1.3 Impact of Security Employed Technologies on Privacy and Data Protection

This section aims to illustrate through the case studies of this Work Package the potential multi-layered risks of the security measures with regard to the privacy and personal data protection of the individuals affected by the measures.

#### 6.1.3.1 Impact of CCTV systems on the right to privacy and data protection

The Article 29 Data Protection Working Party, in its Opinion on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities, points out that\(^{202}\):


"Surveillance activities can be well-intentioned and bring benefits. So far the expansion of these activities has developed in relatively benign and piecemeal ways in democratic societies – not because governments or businesses necessarily wish to intrude into the lives of individuals in an unwarranted way. Some of these activities are necessary or desirable in principle - for example, to fight terrorism and serious crime, to improve entitlement and access to public services, and to improve healthcare. But unseen, uncontrolled or excessive surveillance activities also pose risks that go much further than just affecting privacy. They can foster a climate of suspicion and undermine trust. The collection and use of vast amounts of personal information by public and private organisations leads to decisions which directly influence peoples’ lives. By classifying and profiling automatically or arbitrarily, they can stigmatise in ways which create risks for individuals and affect their access to services. There is particularly an increasing risk of social exclusion."

Special attention is given to the principle of proportionality. According to the WP29, this implies the obligation to demonstrate that any measure taken corresponds to an “imperative social need” and that any measures which are simply "useful" or "wished" may not restrict the fundamental rights and freedoms.

The Committee on Civil Liberties, Justice and Home Affairs of the European Parliament published a Note in 2009 on the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe. In this Note, highlighted the results from the broad use of CCTV for crime prevention purposes. The results include digitalisation, face recognition, behavioural recognition and the risks of discrimination and social exclusion. The CCTV systems may also have a risk of an impact on dignity and autonomy of the individual, depending on the places where the images/ videos are recorded.

The technical sophistication of the CCTV systems and their organisational arrangement play a substantial role in their capabilities to detect crime and gather evidence. Although quite often the CCTV systems are cited as being a major tool in assisting police, quite often they fail to perform as intended. On the other hand, digitalisation has led to capturing, storing, retrieval and transfer of big amounts of images. The processing of those images by intelligent algorithms to extract information from an image enhances the data processing and accordingly creates the need for monitoring of the application of the data protection legislation.

In this regard, several Data Protection Authorities have published guidelines on how to apply the legislation in the CCTV systems. Taking the example of the UK Surveillance Commissioner, a “self-assessment tool” was published recently for this purpose. The tool helps organisations that operate CCTV systems to assess how well they comply with the

---

203 Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, A Review the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe, April 2009

204 Burgess Peter, Kloza Dariusz, “Monitoring Reports on emerging ethical challenges in the developing and implementing the video archives”, Deliverable D2.4. for the ADVISE project, November 2013, p.15

principles of the relevant data protection legislation and surveillance code of practice. The document embraces principles such as accountability, transparency and mechanisms such as Privacy Impact Assessments, certification and alternative interventions (security measures) to surveillance cameras.

Another aspect of the impact of camera surveillance to the right to protection of personal data is the one with regard to the data subject rights, and especially the right to access to personal data. The right to access is the sine qua non for the exercise of informational rights. Accessing the CCTV footage might prove problematic in several occasions, such as when the use of a CCTV system is not covered by the personal data protection legislation (eg. law enforcement purposes), there is no clear notification on who is the data controller and no contact information for the data subject to address its request.

Legal grounds for processing of the images is also very substantial to the protection of the right: consent of the data subject cannot usually be the legal basis for processing in the case of CCTV systems, as the consent needs to be freely given, specific and informed according to art. 7 of the Data Protection Directive. The Proposal for a General Data Protection Regulation, introduced additional qualifications: the consent should be given for specific purposes; and the consent for data processing should not be a precondition for execution of a contract or the provision of a service, when such processing is not necessary for the contract or the service. However, even with the additional conditions for consent as legitimate ground of processing, the CCTV system needs additional safeguards.

WP29 focuses on the prerequisites and limitations applying to the installation of equipment giving rise to video surveillance as well as on the necessary safeguards for data subjects. In the analysis the WP29 divided video surveillance based on its purposes which may be: (1) the protection of individuals, (2) protection of property, (3) public interest, (4) detection, prevention and control of offences, (5) making available of evidence, (6) other legitimate interests.

---

The opinion sets forth the following obligations and appropriate precautions applying to the data controller of a CCTV:

1. **Lawfulness of the processing** – surveillance must be compliant with the general and specific provisions applying to the sector in question (such as laws, regulations, codes of conduct having legal relevance); these provisions may also be laid down in connection with public security purposes as well as with purposes other than those related to personal data protection - e.g. the need to obtain ad-hoc authorisations by specific administrative bodies and comply with their instructions;

2. **Specificity, specification and lawfulness of purposes** – the purposes sought must be clear and unambiguous; a clarification on the purposes should be provided in the information provided to data subjects;

3. **Criteria making the processing legitimate** – video surveillance must comply also with at least one of the criteria making the processing legitimate under Article 7 of the Data Protection Directive;

4. **Proportionality of the recourse to video surveillance** – CCTV and similar video surveillance equipment may only be deployed on a subsidiary basis, that is to say for purposes that actually justify recourse to such systems;

5. **Proportionality in carrying out video surveillance activities** – filming arrangements (e.g. angle of filming, type of equipment, location of cameras, possibility of zooming in,…) and the retention period must be relevant and not excessive; cases in which identification of a person is facilitated by associating the images of the person’s face with other information concerning imaged conduct/activities and the possible communication of the data to third parties should also be carefully considered;

6. **Information to data subjects** – data subjects must be appropriately informed of the fact that video surveillance is in operation and of the exact places monitored;

7. **Appropriate security measures should be in place; data subjects’ rights** – data subjects have the right to access their data processed by CCTV, the right to object to the processing and the right to oblivion;

The PRISE project includes CCTV surveillance in the sensor technologies section as part of the electro-optical sensors. CCTV surveillance is probably one of the most prominent surveillance systems and are therefore also present in many European cities, be it as part of the governmental public security system or as part of a private security scheme (e.g. in shopping malls). One of the main problems with CCTV systems is thus the ubiquitous surveillance that is almost unavoidable. The compliance with data protection regulations and recommendations is thus highly important, which could be part of a certification scheme based on the STEFi model.

A secure – encrypted – data storage is therefore the most important aspect, but also other aspects like function creep, which is “the use of the data for something other than the original intention”212 or the sharing of the data with third persons without the consent of the

212 Ib., p. 62.
data subject are among the big freedom infringement risks with data storage technologies. The unauthorised access to the stored personal data is also a serious risk; it applies on the one hand to the database where this information is stored (this will be described in more detail in the database section) but on the other hand also on the access during communication, mainly through interception.

6.1.3.2 Impact of drones on the right to privacy and data protection

Although drones have primarily developed in the context of military operations, non-military RPAS are increasingly used in the civil sphere through policing and security measures. However, despite the obvious range of drones’ practical applications and capabilities, drones are incontestably considered to be a new source and way of intrusiveness in people’s privacy: their main function is based on visual surveillance.²¹³ As a European Commission study mentions, “these uses of visual photography payloads, the potential extension to other types of payloads (for example, thermal imaging cameras, communications relay and biometric identification), the decreasing size of RPAS devices and their use by commercial organisations and private individuals introduce privacy, data protection and ethical concerns that extend beyond analogies such as CCTV and police helicopter surveillance.”²¹⁴

In Europe, the use of aerial technologies for photography, surveillance and other applications is covered by Article 7 (Respect for private life) and Article 8 (Data protection) of the Charter of Fundamental Rights of the European Union (EU Charter) and by the Right to respect for private life of Article 8 European Convention on Human Rights (ECHR). The use of drones for civil purposes must also be in compliance with the obligations set out in the Data Protection Directive 95/46/EC, when personal data is collected, processed or stored during the monitoring of public space, especially if the images are recorded and these images of natural persons are clear enough to lead to identification. Consequently, any use of RPAs for aerial photography that captures members of the, public and records the footage must comply with this instrument. Furthermore, national-level legislation related to privacy and data protection (particularly national laws which implement the Data Protection Directive) as well as national laws relevant to telecommunications, CCTV and police surveillance activities are also applicable to drones usage.²¹⁵


The term “visual surveillance” includes visual photography, video streaming, surveillance via high resolution cameras, thermal imaging cameras and infrared cameras. There is also “non-visual surveillance”, which is surveillance monitored through the means of other sensors e.g. microphones, automated number plates recognition, GPS sensors, facial recognition. [European Commission, Privacy, data protection and ethical risks in civil RPAS operations - Final Report (27/01/2015), available at: http://ec.europa.eu/DocsRoom/documents/8550, p.30]


²¹⁵ Ibis
EU Member States do not currently provide for RPA-specific privacy or data protection regulations, although certain countries have permitted some RPAs to fly through safety regulations. The United Kingdom, France, Germany, Italy, Sweden and Denmark are examples of member states implementing RPA-related laws. RPA applications in the Member States are either regulated by the data protection legislation in case they are processing personal data or in fewer cases there is specific legislation which includes privacy elements. France, Italy, Sweden have drafted surveillance-oriented regulations, which include regulations for CCTV systems and police surveillance; such legislative instruments could regulate some RPAS applications such as aerial photography or visual surveillance. The Italian National Authority for Civil Aviation (Ente Nazionale per l’Aviazione Civile; ENAC) adopted new regulations governing the operation of RPAS on 16 December 2013 and they entered into force on 30 April 2014. The Swedish Transport Agency has issued an Act governing civilian RPAS in 2013. It requires that operators hold a permission for commercial and research and development using drones. Although this Act provides that civilian RPAS are limited to flying within sight of the pilot, and at a height lower than that at which most manned vehicles fly, there are no specific privacy measures included in the Act. In Belgium the use of drones is permitted for test flights and for scientific purposes, but not in the context of commercial activities yet. Recently, the federal government has proposed legislation governing the commercial operation of drones\textsuperscript{216}. As far as Spain is concerned, the Spanish regulation (temporary regulation – Law 18/2014) allows the use drones for aerial activities such as: research and development activities; aerial treatments, pesticides and other treatments involving spreading substances in the soil or atmosphere, including activities for firefighting; observation and aerial surveillance activities including filming and monitoring of forest fires; aerial advertising, radio and TV emissions and emergency, search and rescue operations as well as other special works. Provisions in Law 18/2014 have to be completed with some extra legislation applicable to operators, in particular with regard to use of the radio spectrum, data protection or the taking of aerial photographs, nor from his/her liability for any loss, damage or injury caused by the operation of the aircraft (Section 50.1).

Privacy-related concerns of drones usage are connected with either the drone itself, as a vehicle/aircraft or the software it carries (e.g. CCTV, thermal cameras, GPS etc)\textsuperscript{217}. The potential impact of this new technology depends on many factors: the purpose for which


\textsuperscript{217} Although there is no universal definition of the concept of privacy, it may be defined as “the presumption that individuals should have an area of autonomous development, interaction and liberty, namely a "private sphere" with or without interaction with others, free from state intervention and from excessive unsolicited intervention by other uninvited individuals”. [La Rue, Frank, “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression”, A/HRC/23/40, 17 April 2013, pp 6-7, available at: \url{http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf}
D4.1: Legal Analysis of Existing Schemes

CRISP project

drones are used, the extent and type of personal information they collect, the context and location of the vehicle, the technological equipment they carry, the operator.\textsuperscript{218}

RPA technology has taken surveillance to the next level. It is much more advanced than CCTV systems, as the aircrafts are equipped with advanced sensors which are able to process various types of images and information and, therefore, undertake various types of surveillance (e.g. physical surveillance, surveillance of communications, body surveillance, data surveillance). These sense-enhancing technologies “greatly magnify the human capacity to observe”, as drones not only record but also recognise faces, intercept electronic communications, detect abnormal behaviours or locate human targets. Furthermore, drones offer secrecy due to their size and can monitor in locations which do not require access to their premises and they can even observe and follow individuals without being noticed. The breadth and duration of the observation are also expanded. For instance, solar-powered RPAS will be able to stay in the air forever.\textsuperscript{219} Clarke argues that drones have significantly changed visual surveillance in at least three ways: 1) they offer new angles and enable ground-level obstructions to be overcome, 2) they avoid ground-level congestion and increase the feasibility of pursuit and 3) they reduce the cost-profile by combining inexpensive devices with low operating costs.\textsuperscript{220}

Drones add a further dimension to the surveillance threats that society faces.

“By looming above people, and by following them relatively unhindered in comparison with terrestrial stalking, drones could well usurp the CCTV camera as the popular symbol for the surveillance society.”\textsuperscript{221}

According to the EDPS,

“When combined with other technologies, RPAS may become extremely powerful surveillance tools. Because they can carry a multitude of sensors, perform systematic surveillance (overt and covert) of an individual or groups (in case of demonstrations for example) and be extremely versatile (can go almost anywhere), they offer a superior level of surveillance.”\textsuperscript{222}

\textsuperscript{218} European Commission, Privacy, data protection and ethical risks in civil RPAS operations - Final Report, (27/01/2015), available at: \url{http://ec.europa.eu/DocsRoom/documents/8550}, p.24


\textsuperscript{222} Ibis

\textsuperscript{222} European Data Protection Supervisor, Opinion of 26 November 2014, op.cit. p.5
Taking all the above into consideration, we can very easily conclude that drones are an extremely effective means for the performance of monitoring and surveillance activities. In that sense, as EPIC states, “drones present a unique threat to privacy. Drones are designed to undertake constant, persistent surveillance to a degree that former methods of surveillance were unable to achieve”\(^\text{223}\). The fact that in most of the cases drones are undetectable from the ground means that citizens have no means of knowing what payload is used, whether the drone is equipped with a camera or a recognition sensor, who is the pilot, whom he represents, whether data is gathered and by whom. This situation leads to a so-called “panoptic effect”. Drones as the new perfect tool for blanket surveillance activities because of its capability to be invisible, to capture images, sounds and to intercept phone calls and texts also raises transparency issues. Additionally, conventional surveillance aircraft, such as helicopters, provide auditory notice that they are approaching and allow a person “to take measures to keep private those activities that they do not wish to expose to public view”. In contrast, RPAS, and especially small RPAS, offer no such warning. Invisibility impacts enforcement of individuals’ rights: data subjects are unaware of their personal data being collected and transmitted. There is no knowledge or consent.\(^\text{224}\)

There are also some issues associated with accountability. “In case of infringements to their right to private life, individuals do usually expect to identify a legal or physical entity to be responsible for damages they suffered”\(^\text{225}\). However, as the surveillance will be mostly anonymous and capable of being carried out by anyone with a drone and attachments, the ability to detect those responsible for the surveillance is diminished. Furthermore, by recording images of a person or vehicle in public places, drones allow their operator to locate individuals in particular spaces and at particular times and also enable operators to reveal a person’s movements.\(^\text{226}\)

As such, RPAs aircraft systems do not per se process personal data. However, when combined with other technologies they offer many applications. As it has already been mentioned, drones are equipped with devices. These devices and embedded technologies thus offer the possibility to collect, record, organise, store, use, combine data allowing drones operators to identify persons directly or indirectly. The most common types of personal data

\(^{223}\) EPIC Org, “Domestic Unmanned Aerial Vehicles (UAVs) and Drones 2013”, \url{https://epic.org/privacy/drones/}


\(^{226}\) European Commission, Privacy, data protection and ethical risks in civil RPAS operations - Final Report, op.cit., p.32-38

collected include photographs, biometric data and location data. As a result, RPAs can be used to process personal data, in the meaning of Article 2(a) of Directive 95/46/EC18 227, 228.

Article 29 Working Party on the Protection of Individuals with regard to the processing of Personal Data states that:

“There is unquestionably a real need to focus on the threats that an uncontrolled proliferation of drone applications could bring about for individuals’ fundamental rights and freedoms. From a data protection point of view, what is relevant is not so much the use of RPAs as such, but mainly the different technologies they can be equipped with (i.e. high-resolution cameras and microphones, thermal imaging equipment, or devices to intercept wireless communications) and the subsequent collection and processing of personal data that may take place.”229

Drones entail the feature of “invisibility”, due to their small size and altitude of operation. This practically means that any collection of personal data takes place without the knowledge of the data subject and without the drone being noticed. Furthermore, the transfer of data collected between the RPAs and the collector takes place in an invisible way. Apart from invisibility, drones also have an “indiscriminate” character in the way they collect personal data. They collect massive amounts of data as they cannot distinguish the subjects and elements filmed. The collection of personal information subjects to no criteria and no pre-selection of information relevant to a specific purpose. This feature of drones contradicts to data protection principles which require, in general, that personal data are processed for a pre-defined purpose, that processing should not be excessive to the purpose pursued and that the less intrusive technological means should be used.230 RPAs technology itself also inherits some risks: drones process personal data in a manner that poses security risks to the data collected as there is lack of confidentiality. Data security and integrity can be endangered by wireless modes of transmission. These modes of transmission also increase the potential risk of hacking.231

---

227 European Data Protection Supervisor, Opinion of 26 November 2014, op.cit., p.5
228 European Commission, Privacy, data protection and ethical risks in civil RPAS operations - Final Report, op.cit.p.43
RPAS technologies do not present any new data protection issues that has not already been raised in relation to other existing technologies, because the payloads that can be fitted to drones for the processing of personal information are not new technologies. [Ibis]
231 Ibis, p.45
Drones usage may also lead to *profiling* based on the data the drones collect\(^{232}\). Profiling means “any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person’s health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements”\(^{233}\).

To conclude with, the usage of drones and their capability of processing personal information have attributed new dimensions to surveillance systems. Panoptic effect, profiling, excessive collection and processing of personal data, lack of notification to data subjects and others are only few of the main challenges of the RPAs. Uses of RPAs involving the processing of personal data constitute in most cases an interference with the right to the respect for private and family life guaranteed by Article 8 of the Council of Europe Convention on Human Rights and Article 7 of the Charter of Fundamental Rights of the European Union, as they challenge the right to intimacy and privacy guaranteed to all individuals in the EU and can therefore be allowed only under specific conditions and safeguards. In any event, whenever personal data are processed by RPAs operated in the EU, which is common, the right to the protection of personal data enshrined in Article 8 of the Charter applies and the EU legal framework for data protection should be complied with.\(^{234}\)

### 6.1.3.3 Impact of biometrics of alarm systems on the right to personal data protection

Intruder and access control alarm systems can use biometric methods for identification and access authorisation of the individual. WP29 defines biometrics data as:

> “biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and

---

\(^{232}\) Article 29 Working Party defines profiling as “*any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person’s health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movements*”. [Article 29 Data Protection Working Party: “Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation” (13 May 2013), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/annex_one-stop_shop_20130513_advice-paper-on-profiling_en.pdf]


measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.”

Alarm systems that use biometrics are included in the category of biometric systems, i.e. applications which use biometric technologies which allow the automatic identification, and/or authentication/verification of a person. The biometric techniques can be either physiological, behavioural or both. Usually, a biometric alarm system would employ physiological techniques measuring the physical or physiological characteristics of an individual, such as fingerprint verification, iris recognition, face recognition, DNA pattern analysis, outline of hand patterns and others.

Sensor technologies are often used for biometric security applications like face recognition, fingerprinting or iris scanning which all aim at the flawless identification of persons – as a result of the unambiguous identifying character of biometric features of individuals. This requires although the processing of really sensitive data, which is why here data protection is even more important and for instance also handled legally more restrictive, especially concerning the processing of genetic data. Therefore it should be important that the certification of security PSS strictly evaluates the secure processing of biometric data. Also, in case a biometric identification system is implemented using a centralised database, the compromise of the database would mean the data of the individuals enrolled in the database would also be compromised.

De Hert emphasizes the implications of the use of biometrics in relation to the protection of personal data; the increasing volume of data, the linking of data bases and datasets and function creep are a few of the potential risks. Other risks include data breach, identity fraud especially in case of identification and authentication, and purpose diversion.

CNIL states:

“In particular that processing of such data, in an automated and centralised form, would be acceptable only to the extent that it may be justified by a compelling necessity linked to national security or public order.”

---

235 Article 29 Data Protection Working Party, Opinion 3/2012 on developments on biometric technologies, WP193, 27 April 2012, p.3
237 Article 29 Data Protection Working Party, Working Document on Biometrics, WP80, 1 August 2003, p.3
241 Article 29 Data Protection Working Party, Opinion 3/2012 op.cit., p.28f
The European Data Protection Supervisor drew attention particularly to the storage of biometric data using in relation to the use of the data for additional purposes from the ones originally collected and the enrolment and matching processes in relation to the possible Failure to Enrol Rates\textsuperscript{243}. In his opinion on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), the EDPS assesses the EES in relation to art.8 ECHR based on the following questions\textsuperscript{244}:

- Does EES constitute an interference and to what extent?
- Is the interference provided for by a clear legal basis?
- Is the measure necessary and proportionate in a democratic society for any of the purposes listed in Article 8(2) ECHR or Article 52(1) Charter?

The ISO/IEC 19792:2009- Security evaluation for Biometrics provides a comprehensive approach to evaluating the security aspects of biometrics systems, based on the concepts of measurement of statistical error rates, the biometric specific vulnerabilities and privacy\textsuperscript{245}.

Vielhauer, Dittmann and Katzenbeisser identify five key security requirements for biometric data: confidentiality, integrity, authenticity, non-repudiation and availability\textsuperscript{246}. Confidentiality in the cases of biometric systems refers to the secrecy biometric and authentication information and its protection from unauthorised access. Additionally, during the verification process the scrutinised needs to be restricted with security measures, as a stolen fingerprint reference can facilitate identity theft\textsuperscript{247}. Also other biometric modalities can lead to the revelation of medical patterns. The requirement of integrity refers to the integrity of all resources and all software and hardware components. Authenticity refers to the entity authenticity and to data origin authenticity. Non-repudiation is highly related to accountability and enforceability; it involves an identification of involved parties and proves a performed action or the occurrence of an event. Last but not least, availability is substantial to all information systems.


\textsuperscript{244} EDPS, Opinion on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), July 2013


\textsuperscript{247} Read further on the risk of biometric spoofing, i.e. “the ability to fool a biometric system into recognizing an illegitimate user as the genuine one, by means of presenting to the sensor a synthetic forged version of the original biometric trait” : Galbally Javier, Satta Riccardo, Gemo Monica, Beslay Laurent, “Biometric Spoofing: A JRC Case Study in 3D Face Recognition”, Joint Research Center Technical Reports, 2014
6.2 **Bodily Integrity**

The concept of bodily integrity refers to inviolability of the physical body. It emphasizes the importance of the right to self-determination of individuals in matters relating to their own body. In this context one can also think of the right to self-determination regarding medical procedures and removal or processing of an individual’s tissues and genetic material.\(^{248}\) And, on another level, a right of the state to infringe upon bodily integrity in lawfully permitted instances, such as forced blood tests, forced feeding of a person dying from the eating disorder, etc. Security products and services must, by all means, respect constitutional freedoms including the bodily integrity of the scrutinised.

There are no provisions specifically mentioning bodily integrity in the laws applicable at the EU level\(^ {249} \), but nonetheless, bodily integrity as a concept is protected by a number of general provisions concerning fundamental human rights, placing emphasis on a person’s mental and bodily integrity, dignity and privacy. The Charter of Fundamental Rights of the European Union is one of the general legal references that provides for safeguards against infringements of bodily integrity in Article 1, which states that human dignity is inviolable and must be respected and protected. Article 3 speaks about integrity of the person, and grants everyone the right to respect for his or her physical and mental integrity. In the fields of medicine and biology free and informed consent of the person concerned must be provided. Article 4 provides that no one shall be subjected to torture or to inhuman or degrading treatment or punishment. Article 6 provides that everyone has the right to liberty and security of person. The Court of Justice of the EU argued in *Schwartz case* that limitations to fundamental rights must be provided for by law, respect the essence of those rights, and, in accordance with the principle of proportionality, be necessary, and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others\(^ {250} \).

The Convention for the Protection of Human Rights and Fundamental Freedoms also prohibits torture or inhuman or degrading treatment or punishment (art.3) and establishes the right to liberty and security of a person in article 5. Regarding interference with fundamental rights, especially privacy, the European Court of Human Rights developed an understanding that such interference must be in accordance with the law, must pursue one or more legitimate aims and, in addition, it must be “necessary in a democratic society” to achieve those aims.

---


\(^ {249} \) Most countries have laws and rules for bodily searches in order to protect the rights of the individuals against potential infringement from law enforcement authorities. These rules specify under which conditions an individual can be required to undergo a bodily search, provide fingerprints or other material, etc.

\(^ {250} \) Court of Justice of the European Union, case of *Schwarz v. Stadt Bochum*, C-291/12, 17 October 2013.
Security products and services (such as cameras, access control technologies) facilitating the above activities should therefore fully respect the right of individuals to self-determination regarding bodily integrity. When recording of medical procedures is in place as a security measure in order to provide for evidence of the procedures data protection standards are applicable as well.

Self-determination regarding biological material is imperative in upholding bodily integrity, and security products and services need to respect this. Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003 setting standards of quality and safety for the collection, testing, processing, storage and distribution of human blood and blood components and amending Directive 2001/83/EC applies to collection and testing of human blood and blood components, and to their processing, storage, and distribution when intended for transfusion (Article 1). It provides that any personnel involved in handling is properly qualified (may also be applicable to access rights managed by a security system). Perfect traceability of blood samples is prescribed in Article 14, which, again, applies to blood establishments which need to have a security system in place to ensure such traceability and unmistakeable identifiability of samples. Article 24 provides that data security measures must be in place as well as safeguards against unauthorised data additions, deletions or modifications to donor files or deferral records, and transfer of information. Similarly, Directive 2004/23/EC of the European Parliament and of the Council of 31 March 2004 on setting standards of quality and safety for the donation, procurement, testing, processing, preservation, storage and distribution of human tissues and cells provides for the rules in handling of human tissues and cells. Security system in a facility that performs such actions is of utmost importance to ensure that only authorised persons have access to biological material, that the tissues must always be traceable and that anonymity of the donor is always ensured (Article 8). That tissues establishments must always keep records of their activities, including the types and quantities of tissues and/or cells procured, tested, preserved, processed, stored and distributed (Article 10) and that all data, including genetic information, collated within the scope of this Directive and to which third parties have access, have been rendered anonymous so that neither donors nor recipients remain identifiable (Article 14).

The right to be secure against violent assault, torture, inhumane treatment is another aspect of the right to bodily integrity. It is easy to imagine security products and services impinging on this right in cases of monitoring by CCTV or drones in inhumane imprisonment conditions (for example monitoring prisoners, naked, 24/7, etc.).

In addition, national provisions detailing a right of the state to infringe upon bodily integrity in lawfully permitted instances, such as forced blood tests, smear tests, etc. under criminal procedure legislation. Proportionally of such infringements upon bodily integrity is normally

---

achieved by limiting such procedures only to suspects of criminal acts, if such is unavoidably necessary for the purpose of criminal investigation.

The legal requirements and obligations regarding the right to bodily integrity of an individual, will predominantly be binding for the users (operators) of a security PSS, for example law enforcement, intelligence or security authorities, using advanced security technologies or systems (such as nanodrones, biometric systems, bodyscanners) to monitor the citizens for different purposes or discover evidence in criminal procedures. When security measures, such as CCTV, IT access control systems are used by institutions facilitating activities related to medical procedures, having tissues removed/processed, such institutions as operators of the security PSS should also fully respect the right of individuals to self-determination regarding bodily integrity.

Following some specific cases of security PSS will be illustrated, specifying under which conditions the use of such security PSS would constitute a breach of the concept of the right to bodily integrity.

A body scanner used at airports to monitor the passengers and discover whether they are in possession of unauthorised/dangerous items, may have an impact on the health of the scrutinised due to radiation. This would trigger Article 1, 3 and 6 of the Charter and Article 5 of the Convention. The right to bodily integrity may also be breached if the scanner produces an image that depicts bodily characteristics that may be hidden under the clothes of a person, such as breast implants. This would additionally trigger the provision of Article 8 related to respect for private life from the Convention, since such interference with the right to privacy is not necessary in relation to the aim of the use of scanner, which is airport security. The SIAM project highlighted that to the extent that data from the bodyscanner, such as images, are stored and shared with third parties or used afterwards, the scope of infringement of the bodily integrity extends in time and space. The infringement of the right to bodily integrity by security scanners depends highly on the type of technology employed in the scanner. For example, X-ray backscatter scanners emit low energy x-rays and thus may have implications to the health and bodily integrity. On the other hand, millimetre-wave scanners do not use X-rays. These rights...

---

252 There is a discussion on the violation to the right to bodily integrity when there is no actual touching of the body, such as for example with x-rays. The question relates to whether the invasiveness to the bodily integrity relates to the health risk it involves or the fact that the representation of the human body in the resulting picture. Van der Ploeg also discusses the issue of DNA sample as a breach of the bodily integrity. The DNA samples as such do not always breach the integrity of the human body. However, it is also the subsequent use of the acquired information: Irma van der Ploeg, “Biometrics and the body as information. Normative issues of the socio-technical coding of the body” in **Surveillance as Social Sorting, Privacy Risk and Digital Discrimination**, Routledge, 2003, p.69.


must be respected by the airport authorities, operating such body scanners and monitoring passengers, as well as any other stakeholders that may be authorised to further use the material gathered by the scanners.

The relevant rules for the use of body scanners have been introduced by Regulations 1141/2011\textsuperscript{255} and 1147/2011\textsuperscript{256} which provide in particular that security scanners are not mandatory for Member States and/or airports and can only be used at EU airports in accordance with minimum conditions such as: security scanners shall not store, retain, copy, print or retrieve images; any unauthorised access and use of the image is prohibited and shall be prevented; the human reviewer analysing the image shall be in a separate location and the image shall not be linked to the screened person and others. Passengers must be informed about the conditions under which the security scanner control takes place. In addition, passengers are given the right to opt out of a control with scanners and be subject to an alternative method of screening. In order to safeguard citizens' health and safety the European Commission allowed Member States and/or airports to deploy only security scanners which do not use ionising radiation. To the extent that the use of body scanners entails personal data processing, it also falls under the provisions of Data Protection Directive.

Another example of a security PSS that might cause a breach of a number of fundamental rights is a nano drone, with a size of an insect, capable of collecting samples of DNA from individuals, even without being noticed\textsuperscript{257}. As argued above an introduction of the use of such security devices by the law enforcement, military or intelligence services would have to have firm basis in law, after proportionality of such measures and its impact on fundamental rights would have been assessed. To the extent that the information or samples collected by the drone would constitute personal data, the Data Protection Directive would apply to the data controller.

Technologies that enable biometric recognition of persons, such as iris scans, may also impinge on the right to bodily integrity. Biometric features of an individual are unique physical features that cannot be changed or replaced\textsuperscript{258}. Typically biometric features are regarded as personal data in the EU. Introduction of biometric measures by a data controller

\begin{footnotesize}
\begin{enumerate}
\item Whitehead, John W., \textit{Forced Blood Draws, DNA Collection and Biometric Scans: What Country Is This?}, https://www.rutherford.org/publications_resources/john_whiteheads_commentary/forced_blood_draws_dna_collection_and_biometric_scans_what_country_is_this
\end{enumerate}
\end{footnotesize}
therefore has to satisfy the conditions set by Data Protection Directive. In some EU Member States a permit from the Data Protection Authority is obligatory before introduction.\textsuperscript{259}

6.3 \textbf{EQUAL TREATMENT AND NON-DISCRIMINATION}

The prohibition on discrimination is guaranteed in both the ECHR and the Charter of Fundamental Rights of the EU. More specifically, the article 14 of the ECHR provides\textsuperscript{260,261}:

\begin{quote}
\textit{``The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status``.}
\end{quote}

The wording of ECHR relates the prohibition of non-discrimination to rights and freedoms protected by the Convention. Additionally, the Protocol 12 to the ECHR, expands the scope of the prohibition on discrimination to cover any right which is guaranteed at the national level, even where this does not fall within the scope the Convention\textsuperscript{262}.

According to the Charter of Fundamental Rights of the European Union, which became legally binding when the Lisbon Treaty came into force in 2009, also prohibits the discrimination on various grounds as provided in Article 21.

\begin{quote}
\textit{``Non-discrimination}

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited``.
\end{quote}

The aim of the fundamental right is to allow all individuals equal and fair prospects to access opportunities available in society\textsuperscript{263}. In the context of security PSS, the right means the prohibition of different treatment of the scrutinized based on the grounds established in the ECHR and Charter.

\textsuperscript{259} See for example Slovenia: Slovenian Personal Data Protection Act provides that a data controller must obtain a permit from the national data protection agency before introduction of biometric measures, concerning its employees (Articles 78 – 81). Available at https://www.ip-rs.si/index.php?id=339

\textsuperscript{260} Council of Europe, European Convention on Protection of Human Rights, art. 14

\textsuperscript{261} The EU has accessed as a party in its own right the ECHR

\textsuperscript{262} The Protocol which entered into force in 2005 had not been yet ratified by all members of the Council of Europe.

\textsuperscript{263} Fundamental Rights Agency, Handbook on non-discrimination, 2011, p. 21
6.3.1 Direct and indirect discrimination

The discrimination is seen in two forms: direct and indirect\textsuperscript{264}. Direct discrimination stipulates that individuals in similar situations receive similar treatment. Thus, they should not be treated less favorably because of a characteristic they possess, such as a religious symbol or their social origin. The less favorable treatment is key concept. The wording includes a comparison, which means that whether someone is discriminated is relative to the treatment the other individuals without the characteristic receive in similar circumstances. The less favorable treatment needs to be causally linked to the protected ground.

In the area of security, this would mean that in an airport security check, persons with some or one of the protected grounds would undergo extensive controls and intensive scrutiny measures, not because there is substantial suspicion against them for criminal activity, but because they are categorised and discriminated as such due to their characteristic. The direct discrimination may take place from anyone in power to impose or in control of the security measures. Persons in this position are the security guards providing security services, the operator or programmer of a CCTV system, etc. Also in a higher level of administration, the entities setting the rules and guidance for the security controls, might also create the circumstances for discrimination scrutinized\textsuperscript{265}. The risk of infringement of the right is higher when there is person to person contact, for example in border security measures (bodyscanners, security guards, etc.). This does not mean the discrimination cannot take place in the virtual world, from the controller of a CCTV system against individuals whose images are captured by the camera.

The indirect discrimination protects the specific characteristics against neutral treatment that would discriminate a group of individuals with those characteristics. The ECtHR in the case D.H. v. Czech Republic provides that “difference in treatment may take the form of disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, discriminates against a group”\textsuperscript{266}. Two requirements can be extracted from this definition: the first is the neutral criterion, practice or rule, which disregards the special characteristics and thus leads to discriminatory behavior. The second requirement is that this rule has negative effects on the protected group. It is not enough that the rule has effects; these effects have to be significantly more negative. Last, there also needs to exist a measure for comparison, a comparator factor.

The Fundamental Rights Agency highlights the case of discrimination by association, where an individual is treated less favorably because of their association with another individual, which possesses a specific characteristic. Hypothetically, this would be the case if the a

\textsuperscript{264} ibid
\textsuperscript{265} Analogy from the EU Directives on non-discrimination: ”an instruction to discriminate is deemed to constitute discrimination” : Article 2(4), Employment Equality Directive; Article 4(1), Gender Goods and Services Directive; Article 2(2)(b), Gender Equality Directive (Recast); Article 2(4), Racial Equality Directive.
\textsuperscript{266} ECtHR, D.H. and Others v. the Czech Republic [GC] (No. 57325/00), 13 November 2007, para. 184; ECtHR, Opuz v. Turkey (No. 33401/02), 9 June 2009, para. 183; ECtHR, Zarb Adami v. Malta (No. 17209/02), 20 June 2006, para. 80.
CCTV camera was programmed to focus on Muslims and the individuals that accompany them, independently on whether they bear similar religious symbols. This is a discrimination against the individual bearing the religious symbol and against the individuals that accompany him or her, on the grounds that they are associated with someone having a specific characteristic, in this case the religion.

6.3.2 Differential Treatment

The differential treatment can be justified in the EU law under two conditions: First, the rule or practice needs to pursue a legitimate aim and second it needs to be proportionate. The concept of proportionality has been the matter of enquiry in several cases in the national and EU case law, with the reply not always being crystal clear. The ECtHR has developed criteria for testing the proportionality of the discriminatory behavior. The differential treatment is proportionate to the result to be achieved, when:

- There is no other means of achieving that aim that interferes less to the right to equal treatment.
- The aim of the differential treatment is important enough to justify this level of interference.

Non-discrimination is met in many aspects. The EU has set into force a set of Directives that address and regulate the non-discrimination and equal treatment. Taking as starting point the Directives, there are the following areas where the right to equal treatment and non-discrimination are relevant:

- Employment
- Access to welfare and forms of social security
- Access to supply of goods and services
- Access to justice

6.3.3 Protected grounds of non-discrimination and Security PSS

The protected grounds, thus the characteristics that is prohibited to form a basis for discrimination of the individuals are the sex (gender equality), disability, the race, ethnicity, color and membership of a national minority, nationality or national origin, religion or belief, language, political or other opinion and ‘other status’. At EU level the above protected grounds are listed in an exhaustive manner, whereas in the ECHR the list is indicative, which means other grounds might fall under the protection of the right of equal treatment and non-discrimination.

---

In the context of security products, an important factor is the way the capabilities of the technologies employed in security PSS are used/abused. In the case of services, the human behavior can lead directly to discrimination which is normally apparent to the scrutinized. Taking the example of full body scanners for airport security, the implications of the employment of the security solution to the right of equal treatment might be significant, depending on the use. As a study on the ethical aspects of the full body scanners (FBS) shows, the FBS is quite often used in two types of passengers: either passengers holding passports from countries included in a list for enhanced screening, or taking flights that originated or passed through any of these countries or passengers who they have set off the metal detector alarm. The second case employs a differential behavior towards the passengers who activated the metal detector alarm, but not on the basis of a protected ground, but on actual facts giving reasonable justification to the security guards to proceed with the security checks, since these passengers failed the check of metal detector alarm. However, the first case, the FBS control is a behavior based on the nationality or the national origin and constitutes differentiation of the citizens being nationals of the enlisted countries and differentiation by association for the citizens who visited these countries. The legitimate aim of and the proportionality of the behavior to the potential harm from the infringement of the right needs then to be examined in order to establish whether the interference to the right is justified.

In relation to CCTV and the prohibition of discrimination, there is discussion on CCTV surveillance and social sorting. As Norris argues, CCTV systems offer the possibility of social control and “threat of authoritative intervention to any deviant acts”. Raising the issue of sheer volume of images, Norris explains that the operators of CCTV need to narrow down to images to concentrate on and thus a selection is inevitable. The criterion for this selection can be no other than the suspicious behavior; however, as a study from Norris and Armstrong showed, suspicion does not fall equally on all social groups: teenagers, black people and men were targeted more than other scrutinized. Drones used for law enforcement purposes may have the same consequences, taking into account their technical capabilities for recording personal data without the spatial limitations of the CCTV systems.

Biometrics may also have implications for the right to equal treatment and the prohibition of discrimination. Biometric control may expose disabilities or oblige the person with a protected ground to disclose the specific characteristic. Even in the case of provision of an alternative conventional method, the establishment of biometric control may lead to prohibited differential treatment: removing the person with the protected ground from the “regular” biometric control procedure and obliging him or her to undergo the alternative measure, draws attention and questions to the person.

---

268 Norris Clive, “From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control” in David Lyon (ed.), Surveillance as Social Sorting, Privacy, risk and digital discrimination, Routledge, 2003, p. 249f

269 Albrecht Astrid, “Understanding the issues behind user acceptance”, Biometric Technology Today, Volume 9, Issue 1, 1 January 2001, Pages 7–8
To conclude, **in terms of standardisation and certification, the right to equal treatment and the prohibition of discrimination shall mean that the security PSS:**

- Does not establish, promote or in any way facilitate the differential treatment of the scrutinized based on sex (gender equality), disability, the race, ethnicity, color and membership of a national minority, nationality or national origin, religion or belief, language, political or other opinion and ‘other status’.
- Does not establish, promote or in any way facilitate less favorable treatment of the scrutinized due to their association to an individual with specific characteristics related to sex (gender equality), disability, the race, ethnicity, color and membership of a national minority, nationality or national origin, religion or belief, language, political or other opinion and ‘other status’.
- Does not stigmatise individuals, which in the past have show
- In cases that the security PSS establishes differential treatment based on the above grounds, the interference with the right of the scrutinized should be proportionate to the aimed objective, which entails that there should be no other means available to achieve the important aim with less or minimum interference to the right of the individual.

### 6.4 FREEDOM OF MOVEMENT AND FREEDOM FROM UNLAWFUL DETENTION

Freedom of movement is the human right that poses major challenges to security as it is rooted in the idea of liberty and the tension between security and freedom constitutes a profound, classical and recurrent legal debate. Furthermore, “the right to liberty and security is of the highest importance in a “democratic society” within the meaning of the European Convention of Human Rights"\(^{270}\).

Freedom of movement is enshrined in international documents such as Article 13 of the Universal Declaration of Human Rights and Article 12 of the International Covenant on Civil and Political Rights and for some groups of persons, such as children or disabled people\(^{271}\).

Apart from its universal character, freedom of movement has also been established as one of the founding principles of the EU and constitutes a fundamental liberty of the internal EU market, which comprises an area without internal frontiers\(^{272}\).

\(^{270}\) European Court on Human Rights, case Medvedyev and Others vs France, 29 March 2010 or case Ladent vs Poland, 18 March 2008.

\(^{271}\) United Nations Human Rights, International Covenant on Civil and Political Rights, General Assembly resolution 2200A (XXI) of 16 December 1966

\(^{272}\) The principle of freedom of movement of people, goods and services is justly emphasized as the cornerstone of the European Community. For many Member States the opportunity of access for their goods to a single, Community-wide market was, and still remains, a primary reason for membership in the European construction. Equally, the freedoms of circulation and establishment are perceived as essential by the citizens of the Union.
Obviously, the accomplishment of a right to free movement and the abolition of border controls implies “compensatory” measures concerning a common visa policy and transfer of checks to the external borders of the State members in order to ensure that internal border checks could be abolished without a loss of security. After the 9/11 terrorist attacks many European governments became aware about their vulnerability to terrorism and new measures regarding the security dimension appeared within the frontiers of Europe. As Gibbs states “we are all acutely aware of how our transit through airports changes in light of the current risks about security and possible attacks”. New technologies of security – as surveillance – and instruments of research and information have been developed to complement the former security measures. The Schengen Information System or the creations of Europol are examples. The moment towards technical and information systems as providing the basis for security is also evident in the Stockholm Action Plan that established that “Smart use of modern technologies in border management to complement existing tools as part of a risk management process can also make Europe more accessible to bona fide travelers and stimulate innovation among EU industries, security of Union’s citizens. The coming into operation of the SIS II and VIS systems will be a high priority” but some restrictions and obstacles on the freedom of movement will persist on the grounds of security basically as a consequence of the challenges currently confronting Europe.

As any other fundamental right, freedom of movement is not an absolute right and States have submitted this freedom to some restrictions and limitations on international freedom of movement (immigration or emigration) are very common. Security may operate to limit this freedom and States impose restrictions based on this concept to get some purposes: fight against any kinds of terrorism, protection of persons and buildings, traffic of dangerous goods or substances, etc. In response to the increased European concerns about security in the aftermath of 9/11/2001 in New York as well as 3/11/2004 in Madrid or 7/7/2005 in London, there has been an over-zealous application of security measures in relation to mobility, immigration, and asylum policies. The principle of free movement of persons has been equally affected by security policies intending to fight what has been commonly

For individuals, these freedom of establishment of individuals in any Member State and the freedom to provide services granted to EU nationals (as well as to companies and to firms) comprise the rights to freely leave, enter and reside in a Member State for the purposes of work or establishment (or the provision of services) and the right to be treated in the host Member State free of discrimination on the grounds of nationality. In parallel, Member States have joined forces to combat international phenomena such as terrorism, drug trafficking or illegal immigration since the foundation of EU.


labelled as “international terrorism”. These restrictions have been justified on behalf of our safety and security. The Schengen Convention, the most representative agreement on this topic, highlights this circumstance. The Schengen agreement aimed at establishing the principle of free movement of persons in the European Community and, at the same time, allows Member States to decide in a rather discretionary manner whether reintroducing border checks on individuals is justified by special security concerns [Article 2(2)]. A significant part of the Schengen regime was transferred by the Amsterdam Treaty into the European framework on 1 May 1999. As the European Council stressed, “The European Union has already put in place for its citizens the major ingredients of a shared area of prosperity and peace: a single market, economic and monetary union, and the capacity to take on global political and economic challenges. The challenge of the Amsterdam Treaty is now to ensure that freedom, which includes the right to move freely throughout the Union, can be enjoyed in conditions of security and justice accessible to all.”

This way, European institutions have underlined and strengthened the full exercise of the right to free movement in the legislation without neglecting the security aspects. The Stockholm Program is another example of this policy as it aims for “an open and secure Europe serving and protecting citizens”. With regard to the former, the Program contains guidelines for a common politics on the topics of protection of fundamental rights, privacy, minority rights and rights of groups of people in need of special protection as well as a citizenship of the European Union. As to the second, the program includes also plans for a new European security architecture through the extension of cooperation in the areas of police, military and secret services and measures in the area of border-crossing data exchange between state authorities and surveillance of the internet.

Airports scanners, detectors, alarm systems and sensors, all the security tools based on the technologies of surveillance such as drones, closed-circuit television, and data bases as the Schengen Information System are examples of security PSS that in practical might impede...

---


277 The Schengen Agreement was signed in June 1985 and has passed through several revisions with the incorporation of new members. Nowadays, the Schengen Agreement provides an area made up of twenty six European countries where no visis are required and no border controls are needed.


279 “Public security” is an explicit and general condition in the European framework that may restrict the freedom of movement. See, by all, Article 27 of Directive 2004/38/EC: “[...] Member States may restrict the freedom of movement [...] of Union citizens and their family members, irrespective of nationality, on grounds of public policy, public security or public health. These grounds shall not be invoked to serve economic ends.”

280 At the heart of the Schengen mechanism, an information system was set up (SIS). It allows national border control and judicial authorities to obtain information on persons or objects. The second generation Schengen Information System (SIS II) has replaced the former system, providing enhanced functionalities. The SIS II is a large-scale information system containing alerts on persons and objects. It is used by border guards, customs officers, visa- and law-enforcement authorities throughout the Schengen area, with a view to ensuring a high level of security. The Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) constitutes the necessary legislative basis for governing SIS II with respect to alert procedures falling under Title IV of the Treaty establishing the European Community (former first pillar). It is
the full exercise of the freedom to move. The non-compatibility of these instruments with free movement can derive from their consideration as physical barriers but also from what has usually been called “indirect obstacles”, as the report of the High Level Panel underlined. Indirect discrimination occurs whenever a Member State imposes less-favorable treatment of a group. Transferred into the evaluation of security PSS, this restriction means that controls on persons are practiced over discrimination based on criteria such as nationality, gender, religion, etc.  

The opposite to freedom of movement is detention. Detention of a person constitutes an interference with personal liberty and Article 5.1 of the European Convention of Human Rights states that “Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law…”. Any deprivation of liberty must therefore respect the safeguards which have been established in relevant European and domestic law and European normative, including general principles expressed or implied in it. Again, the performance of some security systems can imply a limitation of freedom of movement and, in some cases, they can be assimilated to detention in the sense of temporal deprivation of that liberty. That is why the assessment of security PSS should fall on the conditions that European normative imposes so as to result unlawful (legitimate motivations, principles of necessity and proportionality; maximum period of detention, alternatives to detention, particularities with vulnerable groups, etc.).

The deprivation of liberty can be legitimate under conditions. In this sense, the second limb of Article 5.1(b) of the Convention on Human Rights allows for detention only to “secure the fulfilment” of any obligation prescribed by law. There must therefore be an unfulfilled obligation incumbent on the person concerned and the arrest and detention must be for the purpose of securing its fulfilment and not punitive in character. As soon as the relevant obligation has been fulfilled, the basis for detention under Article 5.1(b) ceases to exist. For our purposes, situations examined under the second limb of Article 5.1(b) include, for example, an obligation to submit to a security check when entering a country, to disclose supplemented by a decision relating to procedures (Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)) falling under Title VI of the Treaty on European Union (former third pillar).  

281 The Court of Justice held in case Pietro Pinna vs Caisse d’allocations familiales de la Savoie, 15 January 1986, that equal treatment prohibits not only “overt discrimination based on the nationality but also all covert forms of discrimination which by applying other distinguishing criteria arrive at the same result”.  

282 As the European Court on Human Rights describes “The notion of deprivation of liberty within the meaning of Article 5.1 contains both an objective element of a person’s confinement in a particular restricted space for a not negligible length of time, and an additional subjective element in that the person has not validly consented to the confinement in question” (European Court of Human Rights, case Storck v. Germany, 16 June 2005).  

283 The duration of the measure is not relevant to qualify it as a deprivation of liberty. In this sense, the European Court of Human Rights has affirmed that “An element of coercion in the exercise of police powers of stop and search is indicative of a deprivation of liberty, notwithstanding the short duration of the measure (case Brega and Others v. Moldova, 24 January 2012).  

284 European Court of Human Rights, case Vasileva vs Denmark, 25 September 2003.
details of one’s personal identity, stops and searches by the police and to keep the peace by not committing a criminal offence, among others. The Article 5.1(c) also offers a legitimate case of detention “the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so”.

Detention can become arbitrary. The notion of arbitrariness varies to a certain extent depending on the type of detention involved. The European Court of Human Rights has indicated that arbitrariness may arise where there has been an element of bad faith or deception on the part of the authorities or where there was no relationship of proportionality between the ground of detention relied on and the detention in question.

These principles (necessity and proportionality) have also to be respected by is also if the measure isn’t necessary, that is, the purpose for which it was ordered can also be achieved by applying less restrictive measures in the same way (principle of subsidiarity). Security PSS have to be submitted to this control. The principle of proportionality dictates that a balance must be struck between the importance in a democratic society of securing the immediate fulfilment of the obligation in question, and the importance of the right to liberty. The test of proportionality imposes a weighing exercise is to establish whether the deprivation of liberty is proportional to the objective to be achieved (does the aim justify the means), or whether security controls could be implemented successfully also by imposing less restrictive measures (are the means subsidiary), i.e. alternatives to detention, or a shorter period of detention. Regarding the last, deprivation of liberty has to be a measure of last resort and for the shortest appropriate period of time as indefinite detention is arbitrary because it loses its initial purpose.

In terms of standardisation and certification, “freedom of movement” and “freedom of unlawful detention” mean that the product or system has to respect these conditions

- Observes the quality of the EU is an area without internal frontiers where EU citizens and their family members exercise their right of free movement and residence. Family members, irrespective of their nationality, have the right to accompany or join someone in an EU country other than that of his nationality (it includes; spouses, (registered) partners, descendants and ascendants are your

---

285 European Court of Human Rights, case McVeigh and Others vs the United Kingdom, 18 March 1981; case Sarigiannis vs Italy, 5 April 2012; case Foka vs Turkey, 24 June 2008 and case Ostendorf vs Germany, 7 March 2013, respectively.

286 European Court of Human Rights, case James, Wells and Lee vs the United Kingdom, 18 September 2012 and case Saadi vs the United Kingdom, 11 July 2006. The prohibition of arbitrariness also of course means than depravations of liberty must not be motivated by discrimination.

287 See European Court of Human Rights, case Peck v. the United Kingdom, judgment of 28 January 2003, to hand over CCTV images to the media violates Article 8 European Convention of Human Rights and in particular the requirements of proportionality and subsidiarity, since other alternatives to generate publicity for the CCTV initiative exist.
family members). This right applies regardless of whether they have previously been residing in another EU country or with which visa the family member entered the host EU country (Articles 4 and 5 of Directive 2004/38/EC).

- Any restriction of the freedom of movement and residence of Union citizens and their family members, irrespective of nationality, on grounds of public policy, public security or public health has to comply with some conditions and procedural safeguards. Any such restrictions, such as a denial of entry, a refusal of residence or an expulsion measure, must comply with the terms and conditions laid down in the Directive.

- Complies with general principles of legal certainty, no arbitrariness, necessity and proportionality. When it comes to public policy and public security, measures taken on these grounds must be proportionate and no arbitrary. Expulsion is a very considerable interference in a person’s life and must be covered by legal prevision and based exclusively on the personal conduct of the individual concerned which must represent a genuine, present and sufficiently serious threat affecting one of the fundamental interests of society.

- Ensures there is no discrimination on grounds such as sex, race, colour, ethnic or social origin, genetic characteristics, language, religion or beliefs, political or other opinion, membership of an ethnic minority, property, birth, disability, age or sexual orientation. The most important of these rights is the right to equal treatment. Article 18 TFEU stipulates that, within the scope of application of EU law and without affecting any special provisions, any discrimination on grounds of nationality is prohibited.

6.5 PRESUMPTION OF INNOCENCE

The impact of security PSS on human rights, significantly on the due process rights, and first and foremost, on the right to be presumed innocent is well known for academy, judiciary, practitioners, police forces as well as people in general. But this impact is becoming greater with the development of new technologies and security PSS used today not only to detect but also to prevent crime. The effect of some events – remarkably, the 9/11 – on European security policies has been translated in regular and more intrusive practices.

---


As some authors note, “a more proactive, predictive and pre-crime society is emerging”\(^{291}\). This new approach poses extreme challenges to fundamental rights because in a preventive society every single person is submitted to security barriers: scanners at airports, recording cameras in closed or public spaces, surveillance by drones, etc. and security P/S/S don’t target only criminals or suspected individuals but the whole society. As a general obligation, none of these instruments may treat individuals like suspected or even accused creating the perception that they are not innocent as it implies the reversal of the presumption of innocence. In the literature, some studies have discussed the consequences of the current transition from a global focus on prevention to one on the so-called pre-emption\(^{292}\). Massumi explains the differences between these two concepts: “Although the goal of both is to neutralize threat, they fundamentally differ epistemologically and ontologically. Epistemologically, prevention assumes an ability to assess threats empirically and identify their causes. Once the causes are identified, appropriate curative methods are sought to avoid their realization. Prevention operates in an objectively knowable world in which uncertainty is a function of a lack of information, and in which events run a predictable, linear course from cause to effect”\(^{293}\). Pre-emption, on the other hand, differs from prevention in that it acts on threats that have not yet fully formed or that have not even emerged yet, “(i)n other words, the threat is still indeterminately in potential”\(^{294}\). Pre-emption appears, thus, as a challenge of rationalizing the unknown, an effort of predicting the unpredictable.

From a strict legal point of view, presumption of innocence has a limited application as it can only be invoked in the framework of a criminal proceeding. The limited scope of the right to presumption of innocence is reflected on Article 6.2 of the European Convention on Human Rights although has made several attempts to extend the interpretation and application of this provision by recognizing that the presumption of innocence offers some guarantees in the pre-trial (and post-trial) stages of criminal proceedings\(^{295}\). The Article 48.1 of the EU Charter of Fundamental Rights endorses this principle in similar terms. In an international level, the presumption of innocence is nowadays enshrined in different instruments, such as at Article 11.1 of the Universal Declaration of Human Rights of 1948 which states that “Everyone


\(^{294}\) Massumi, B., op. cit., p. 13.

\(^{295}\) As Vervaele affirms “The wording of this right is somewhat misleading, as the combination of “charged” and “proved guilty” could be understood as applying to the trial stage. However, thanks to the interpretation by the European Court of Human Rights it is knew that article 6(2) does apply during the procedure as a whole, which means from the formal opening of a criminal judicial investigation onwards or from the first investigative acts from which a person can deduce that he/she is suspected of committed an offence” (Vervaele, J. A. E., “Surveillance and criminal investigation: blurring of thresholds and boundaries in the criminal justice system?”, in *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges*, S. Gutwirth, R. Leenes and P. De Hert (editors), Springer, London, 2014, pp. 115-128. Quote on page 115).
charged with a penal offence has the right to be presumed innocent until proved guilty according to law in public trial at which he has had all the guarantees necessary for his defense” and at Article 14.2 of the International Covenant on Civil and Political Rights that establishing that “Everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law”.

In this sense, the most important feature – even an ethical imperative - that should be required to these security PSS is to remain technology-neutral and to respect constitutional freedoms. Many other requirements derive from these characteristics so, in terms of standardisation, “presumption of innocence” means that the security PSS:

- Prevents the creation of suspicion. The PSS must obtain sufficient and accurate information and it cannot be activated by a simple suspicion (Article 5 European Convention of Human Rights).
- Protects individuals from undue duress and improve the quality of investigations and thus the reliability of convictions. The prosecution must prove beyond a reasonable doubt every element of a crime in order to convict a defendant. The burden of proof imposed on the prosecution and the presumption of innocence granted every defendant are based on the "Due Process" (Article. 14.3 ICCPR).
- Ensures that the use of pre-trial detention does not undermine the presumption of innocence, using of pre-trial detention as a last resort. Pre-trial detention is not a sanction, but a measure to safeguard a criminal procedure. Pre-trial detention undermines the chance of a fair trial and the presumption of innocence. It increases the risk of a confession or statement being coerced by torture or ill-treatment. Thus, it lessens a suspect’s possibilities of defence (Article 3 Proposal for a Directive on the strengthening of certain aspects of the presumption of innocence and the right to be present at trial in criminal proceedings).
- Require audio-visual recording of interrogation in order to protect against undue compulsion, granting the right to silence or not to incriminate oneself. The P/S/S shall collect sufficient evidences such as video recording to incriminate someone. The suspect has the right to silence and self-crimination (Article 6 and 7 Proposal for a Directive on the strengthening of certain aspects of the presumption of innocence and the right to be present at trial in criminal proceedings).

These requirements have been selected because security PSS provide, in many cases, the proof(s) required to reach a guilty verdict. More precisely, until proven guilty is a provision that guarantee the presumption of innocence: security PSS cannot lead to wrongful and illegitimate convictions because the right to be presumed innocent must be ensured not only by the judicial authorities but also by other public authorities (such as the police, European Court of Human Rights case Allenet de Ribemont v. France296) or private users. The use of security PSS cannot attach criminal labels imprudently nor create suspicion (European Court

of Human Rights case *S. and Marper v. United Kingdom*\textsuperscript{297} in order to not create the so-called “technologies of suspicion” because they undermine the relationship of trust that links citizens to the state, as well as the presumption of the individual's innocence. The technologies of suspicion have been developed under what has come to be called the \textit{maximum security society} (Marx, 1988)\textsuperscript{298}. This society relies on a refined technological framework to influence and even programme the daily lives of citizens as harsh investigation and surveillance techniques are replaced by softer versions that can be applied without knowledge of the persons observed. The technologies of suspicion constitute a set of empirical modes for producing and interpreting “data” results acting as technological forms of supervision, monitoring, supposed deterrence, and ultimately control. Data are collected from people, suspected or not, as the technologies gathered the data not occasionally but via routinized discovery systems. The conjunction of older technologies with newer ones\textsuperscript{299} make almost impossible for people to remain anonymous as they enable tracking people where they are, where they have been and where they are going and they inevitably shape and influence people’s behavior.

Studies have evidenced that highly intrusive security practices (such as massive surveillance\textsuperscript{300}: metal detectors, scanners, CCTV’s, iris recognition systems, alarms, locks, intercoms, and other forms of surveillance, detection, access control and biometric equipment) both in public and private areas threaten the citizens’ trust of democratic institutions because they promote the view “that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted”\textsuperscript{301}. And this suspicion attacks one of the two aspects of the presumption of innocence: the reputation-related aspect which is aimed to protect the image of the person deemed to be innocent. The second aspect, the legal one, imposes on the prosecution the burden of proving the charge, guarantees that no guilt can be presumed until the charge has been proved beyond reasonable doubt, ensures that the accused has the benefit of doubt, and requires that persons accused of a criminal act must be treated in

\textsuperscript{297} European Court of Human Rights, case of *S. and Marper v. United Kingdom*, 4 December 2008.


\textsuperscript{299} De Hert exemplifies it naming the combination of national ID (older technologies) with such as biometrics and facial recognition by CCTV software (new technologies). De Hert, P. “Balancing security and liberty within the European human rights framework…”, pp. 69-70.


accordance with this principle. Finally, all security measures (video-recording, data storage, etc.) must respect the principle of proportionality, which ultimately means, whenever possible, take less intrusive to the privacy and physical integrity of individuals means to prevent unjustified rights and fundamental freedoms interference.

The inadmissibility of the evidence obtained in breach of one of the aspect of the presumption of innocence is a principle enshrined by the European Court of Human Rights that’s infringement may lead to the violation of article 6 of the Convention of Human rights. As highlighted by the European Court of Human Rights, case Gäfgen v. Germany and case Jalloh vs Germany\(^\text{302}\), the Court held that the “use of evidence obtained in breach of the right to remain silent and the privilege against self-incrimination are generally recognised international standards which lie at the heart of the notion of fair procedures under Article 6 […] and therefore] that the prosecution in a criminal case has to seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused”\(^\text{302}\). This requirement is also linked to respect for articles 2 and 3 European Convention of Human Rights which stem implicitly at the bottom are implicitly of the presumption of innocence principle. In more general terms, the European Court of Human Rights has declared that the fight against crime and terrorism in order to maintain public order can never be understood as an unlimited legitimation for authorities\(^\text{303}\).

In the proposal for a Directive, for a start, Article 3 explicitly recognises the presumption of innocence until proven guilty according to law\(^\text{304}\). Article 4 prohibits public references to

---

\(^{302}\) European Court of Human Rights, case of Gäfgen v. Germany and case Jalloh vs Germany, 1 June 2010.

\(^{303}\) “When the level of crime is perceived to threaten the ordre public, there may be pressure to take repressive measures at the expense of human rights. It appears from the case law that the Court is prepared to accept the legitimacy of the fight against crime and terrorism as well as to acknowledge the need to take effective measures, but obviously that does not mean that the authorities have carte blanche” (European Court of Human Rights, case Brogan and others v. the United Kingdom, 29 November 1988; European Court of Human Rights, Kostovski v. the Netherlands, of 20 November 1989).


\(^{305}\) The establishment of a European area of freedom, security and justice has led to the need of reinforce the cooperation of European countries in criminal matters and numerous initiatives have been endeavored to reach a specific legislative framework from presumption of innocence. In this sense, the adoption of Directive on the right to interpretation and translation in criminal proceedings, the Directive on the right to information in criminal proceedings, and the Directive on the right of access to a lawyer in criminal proceedings aimed to ensure that all Member States uphold a common minimum level of procedural rights with a view to make the principle of mutual recognition operating satisfactorily. Some of the rights contained in the above mentioned Directives imply obligations that should be observed by security PSS in the sense that they can have an adverse effect on the right of the presumption of innocence. That is the case of the conditions imposed by Articles 2 to 8 of the Directive 2010/64/EU of the European Parliament and of the Council on the right to interpretation and translation in criminal proceedings. The articles guarantee the right to interpretation and translation provided to persons who do not speak or understand the language of the procedure. In the case of security PSS, the citizens have the right to fully understand the performance, consequences of use, etc. of the PSS in order to decide to
guilt before conviction. Article 5 obliges the Member States to ensure that the burden of proof is in principle on the prosecution. Rebuttable presumptions are only allowed if justified by sufficiently important circumstances. According to Articles 6 and 7 of the proposal, the exercise by the suspect of his right to silence or privilege against self-crimination may not be used against him and, importantly, may not even be considered as a corroboration of facts.

6.6 FAIR TRIAL AND DUE PROCESS

6.6.1 The right to a fair trial

The right to a fair trial is not only a fundamental human right but also, at the same time, a procedural right which enables and empowers the protection and enforcement of other fundamental human rights. Its basic principles are enshrined in both the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and, in general, these two norms are conceived and interpreted in the same way.

“Right to an effective remedy and to a fair trial

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

exercise their rights (freedom of movement, freedom of association, freedom of speech, presumption of innocence, etc.).


307 Art. 6 ECHR: “1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.

2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.

3. Everyone charged with a criminal offence has the following minimum rights:

(a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;

(b) to have adequate time and facilities for the preparation of his defence;

(c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;

(d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court.”
Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice”.

The right to a fair trial includes a number of constituent elements such as:

1. The right to a court, which includes the following structural elements:
   - Access to a court;
   - Finality of court decisions, which means that once a civil judgment, or a criminal acquittal, has become final, it must instantly become binding and there should be no risk of its being overturned;
   - Timely execution of final judgments, which allows for no delays in the execution of a court decision.308

2. The right to an independent and impartial court, established by law;
   - The requirement “established by law” is intended to ensure that the judicial organisation does not depend on the discretion of the executive, but that it is regulated by law emanating from the parliament.309 Also, the body envisaged by this phrase is a body whose function is to determine matters within its competence on the basis of rules of law, following proceedings conducted in a prescribed manner; it must also have the power to make binding decisions.310
   - The notion of “independence” overlaps with the element of “establishment by law”, as it entails the existence of procedural safeguards to separate the judiciary from other powers, e.g. the executive. The tribunal must also be independent of the parties.311
   - “Impartiality” entails inquiry into the court’s independence vis-à-vis the parties of a particular case and also of other authorities. Practically, it is the lack of bias or prejudice towards the parties.312

3. The right to fair proceedings;
   The fairness principle depends on whether the applicants are afforded sufficient opportunities to state their case and contest the evidence that they consider false and

311 “When deciding whether a tribunal is independent, the European Court considers: 1) the manner of appointment of its members, 2) the duration of their office, 3) the existence of guarantees against outside pressures , 4) the question whether the body presents an appearance of independence.” (Naula Mole and Catharina Harby, op.cit., p.30)
312 Dovydas Vitkauskas et. al. op.cit., p.40; See also: Naula Mole et. al. , op.cit., “p.32
not on whether the courts reached a right or wrong decision. Furthermore, it includes the following implied requirements in civil and criminal cases:

- The adversarial principle, which provides for having an opportunity to know and comment at trial on the observations filed or evidence adduced by the other party;
- The equality of arms, which usually overlaps with the adversarial principle. It basically states that each party be afforded a reasonable opportunity to present its case under the conditions that do not place it at a substantial disadvantage compared to another party;
- The requirement to personal presence and publicity (public hearing). This element of fairness consists of four implied rights: 1) the right to an oral hearing and personal presence by a civil litigant or criminal defendant before the court, 2) the right to effective participation, 3) the right to publicity, or the right for the applicant to claim that third persons and media be allowed to attend the hearing and 4) the right to publication of the court decision, or, the obligation for a court to make its judgment public. 313

4. the right to be advised, defended and represented;
5. The right to a reasoned decision and reliable evidence;
   The decision should contain reasons that are sufficient to reply to the essential aspects of the party’s factual and legal claim. 314
6. Trial within a reasonable time;
   What time is “reasonable” is assessed by a cumulative test involving three main criteria: 1) the nature and complexity of the case, 2) the conduct of the applicant and 3) the conduct of the authorities. 315
7. Presumption of innocence. (analysed in part…)

<table>
<thead>
<tr>
<th>In the context of fair trial one should also consider:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 13 ECHR: Right to an effective remedy;</td>
</tr>
<tr>
<td>Article 48 EU Charter: Presumption of innocence and right of defense (in the same context, meaning and scope as Art.6(2) and (3) ECHR);</td>
</tr>
<tr>
<td>Articles 51-53 EU Charter: Field of application, Scope and interpretation of rights and principles, Level of protection.</td>
</tr>
</tbody>
</table>

### 6.6.2 “Due Process” Rights

Article 47 EU Charter and Article 6 ECHR states that everyone is entitled to a “fair hearing”. The requirement of “fairness” covers the proceedings as a whole, and not only those in an oral hearing or first instance. This term, therefore, is broad and incorporates many aspects of

313 Ibis, p.45, 48, 51; See also Naula Mole, et. al. op.cit., p.21, 25
314 Ibis, p.70; See also Naula Mole et. al. op.cit., p.49-50
315 Ibis, p.74; See also Naula Mole et. al. op.cit., p.24-30
the due process rights, as they have been highlighted above, such as the right to access to
court, a hearing in the presence of the accused, freedom from self-incrimination, equality of
arms, the right to adversarial proceedings and a reasoned judgment.\textsuperscript{316}

The term “due process” is interpreted as the right to be treated fairly, efficiently and
effectively by the administration of justice, in accordance with established and sanctioned
legal principles and procedures, and with safeguards for the protection of individual rights.
The rights to due process place limitations on laws and legal proceedings, in order to
guarantee fundamental fairness and justice. The rules applicable to the administration of
justice are extensive and refer to, \textit{inter alia}, fair trial, presumption of innocence and
independence and impartiality of the tribunal. However, the most crucial elements of due
process are considered to be: a) the quality in terms of administration of justice; b) the quality
in terms of protection of the rights of the parties involved; c) the right to an effective
remedy.\textsuperscript{317}

To conclude, we have to stress out that security PSS must comply with the rights to fair trial
and due process and create a respectful framework of use. \textbf{In terms of standardisation and
certification, the rights to a fair trial and due process, entail that the security PSS:}

- Respects the right to be heard; provides the opportunity to the scrutinised to
provide reasons why he or she does not wish to undergo the security measure and
offers alternative solutions, if this is feasible for reasons of national or public
security, unreasonable costs and others
- When this is relevant, the decision for employing a security measure that affects
the rights of the individuals, the decision should provide adequate justification and
be supported by reliable evidence.
- Provides reasonable time framework that gives the opportunity to the affected
individuals by the security measure to decide upon, object or appeal against the
security measure, provided this is feasible and allowed for reasons of national or
public security.
- Does not create any suspicion of dependence and/or promote or support partial
judgement from the part of the authority or entity employing the security PSS.

\section*{6.7 CONCLUSION}

The challenge is safeguarding human rights while ensuring security in an increasingly
complex world. This approach is adopted, among other European documents, in the
Communication COM (2009) 691, 21 December 2009, \textit{"A European Security Research and

\textsuperscript{316} Naula Mole and Catharina Harby \textit{“The right to a fair trial: A guide to the implementation of Article 6 of the
European Convention on Human Rights"}, Human rights handbooks No.3, available at

\textsuperscript{317} Website of Icelandic Human Rights Centre: http://www.humanrights.is/en/human-rights-education-
project/comparative-analysis-of-selected-case-law-achpr-iachr-echr-hrc/the-rights-to-due-process
Innovation Agenda - Commission’s initial position on ESRIF’s key findings and recommendations. In this document, the European Commission has affirmed that security is first and foremost human and societal: “One of the EU’s main objectives is to preserve and develop the European values of justice, freedom, and security whilst addressing the increasingly complex security challenges”. The EU must strengthen the legal and ethical dimensions of all security solutions to guarantee the rights and freedoms of individuals, in particular as regards privacy. In addition, (the EU) it must reinforce the societal dimension of security technologies to ensure that they allow societies to effectively respond to risks and losses (“societal resilience”).

The analysis demonstrated that security measures may have a potential to violate human rights and freedoms, depending on their attributes and technologies, use and other factors. Privacy and protection of personal data are in the spotlight, as the impact assessment of the case studies has confirmed. Surveillance, profiling, big data analysis, lack of accountability and no possibility for exercise of the data subject rights are a few of the potential implications of CCTV and drones to the right to private life and personal data. Biometrics, as sensitive personal data, are also in great risk, if the proper security measures are not in place.

However, these two rights are not the only ones that can be easily infringed. We have seen in the chapter that non-discrimination, freedom of movement, bodily integrity, fair trial and the presumption of innocence might well be violated by a security measure depending on the technology it employs, the use and the environment it operates.

The case studies of this Work Package stressed the above issues, by highlighting the multifaceted risks the different measures pose to the freedoms and rights. The following graphic highlights the rights and freedoms at risk in each case study.

<table>
<thead>
<tr>
<th>Type of security employed technology</th>
<th>Technology typology</th>
<th>Related freedom infringement categories</th>
<th>Specific Privacy and Data Protection Risks</th>
<th>Type of affected individual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmanned Aerial Vehicles (drones)</td>
<td>Crisis management (situation awareness)</td>
<td>Presumption of innocence/Freedom of movement/ Privacy and data protection</td>
<td>Surveillance/panoptic effect/big data without legal basis/ no notification of processing/ no exercise of data subject rights/ purpose of processing/</td>
<td>All scrutinised operators/employees in outdoor areas</td>
</tr>
</tbody>
</table>


The objective should not be to lower security thresholds; security is also a human right and needs to be protected. The objective should be to find ways to protect the human rights and freedoms while preserving the security of the European citizens and individuals within the European Union.

CRISP suggests a means to achieve this twofold purpose, by including freedoms and rights requirements in the certification and evaluation schemes of the security products, systems and services.

In the following chapter, we will see how existing schemes respond to the core criteria and requirements prescribed by the European legislation and we will identify best practices and gaps.

---

319 Article 6 of Charter of Fundamental Rights of the European Union protects the right to freedom and security.
7 LEGAL ANALYSIS OF SCHEMES

In this report, the research team analysed evaluation and certification schemes on the three case studies of security measures: CCTV in public spaces for crime prevention and detention, intruder and access control alarm systems and unmanned aerial vehicles. In the area of CCTV, there is a plethora of evaluation schemes and codes of practice from community councils and other public authorities that is incorporated in our analysis. The alarm systems, as mentioned earlier in the Introduction of this report, are not a new field of certification, and as a result there was a selection of schemes based on the diversity of issuers, the diversity of scope and type of document, in order to analyse and learn from different practices. Certification on drones on the other hand is not a developed field in Europe and the main documents which are available and specifically focused on UAV are guidance documents.

In the first part of the legal analysis of schemes there is the presentation of schemes based on common variables, such as the type and nature of scheme, issuing body, and others. In the second part of the legal analysis, there is the analysis of schemes based on the core criteria and requirements identified in the legal study of this report. The purpose is neither to run a general compliance test of the schemes nor a comparative analysis, but to examine where they stand in taking into account core only issues of the societal aspects on which CRISP primarily focuses and accordingly assess how the existing schemes can be further enhanced. The legal criteria therefore do not follow strict rules regarding the scope of legislation. The rationale behind this approach is to move one step forward from the legislation silos and cross-analyze security PSS against different criteria related to each aspect in order to grasp the societal impact. This approach would have a potential drawback for the analysis; this is to ask from a scheme more than it is supposed to provide. An example would be to ask from an alarm system to positively respond to the criterion of data interference, even though it does not collect data. To mitigate any risks regarding the relevance of the criteria, we applied the relevance/applicability question before examining the actual response of the scheme to the criterion. In case the criterion is not applicable to the scheme, field of security area, functionality and technology it encompasses, then the criterion is not examined for the scheme. In the previous example, the relevance question would be whether the alarm systems processes personal data. In the case of a negative reply, then the criterion of personal data protection will not be examined for this specific alarm system. This approach was useful in particular in the case of the freedom infringement aspect.

The presentation of the results follows the division of the four aspects of the STEFi methodology, i.e. security, trust, efficiency and freedom infringement. Before the analysis of each aspect, there is a brief explanation of the relevant assessment criteria.

320 The consortium partners Dr. Simone Wurster (TUB INNO) and Thordis Sveinsdottir (Trilateral Research & Consulting, LLP) contributed to this chapter.

7.1 Criteria for General Analysis of Schemes Operating in the EU

In this section, we provide a presentation of the analysed schemes, based on the following variables.

1. Nature and type of the scheme

This category presents the nature and type of the scheme as presented in the documentation of the scheme or the website of the provider.

2. Issuing body

The intention is to examine the potential influence of the type of the issuing body (public authority, certification body, association of authorities/organisations cooperating at EU level, etc.) to the inclusion of the societal aspects of STEFi.

3. Relevant security measure

This relates to the broader category of security measure examined in relation to the case studies of the report.

4. Scope and objectives of the scheme

The scope and objectives of the scheme as defined in the documentation of the schemes are important to identify the targets of the schemes and its beneficiaries.

5. Normative references

As explained in the Report 2.1. of CRISP, the schemes might be based on standards, technical specifications, legislation or other normative documents.

6. Validity and Renewal

The validity period and the obligation for renewal is an important category to see how up-to-date is the scheme and whether it follows the regulatory and technological developments. On the other hand, too often renewal might influence the trust and certainty towards the scheme.

7. Availability

This category seeks to inform on whether the information on the scheme and the documentation is transparent and available to the interested parties.

---

322 It should be noted that the term “schemes” is used broadly, meaning every set of requirements and rules established and managed by a public authority or private organisation with the aim to evaluate and assess whether a specific security measure fulfils pre-defined criteria.
7.2 PRESENTATION OF ANALYSED SCHEMES OPERATING IN THE EU

7.2.1 Alarm systems

7.2.1.1 VdS Guidelines for Alarm Systems – Biometric recognition procedures: Requirements and Test Methods

The full name of the scheme is “VdS Guidelines for Alarm Systems – Biometric recognition procedures: Requirements and Test Methods (VdS 3112en: 2010-07)”. VdS, the issuing organisation, is one of Germany’s leading independent testing institutions for fire protection and security (private certification body). The guidelines contain the requirements and test methods for biometric recognition in alarm systems and they are applied for products of intrusion detection techniques, access control and electronic keys which use biometric identification features and contain determinations for the evaluation and testing of biometric features. They are valid from 1 July 2009, however nothing is mentioned regarding their renewal. They also contain dated and undated references to other publications. The guidelines are accessible via the VdS website.

The scheme is based on use of characteristic biometric features of a person for the determination of identity. For biometric recognition procedures this is made automatically by capturing, processing and evaluating the captured personal data in two processes:

1) Enrolment: the biometric features of a person are captured, processed and stored as reference sample of this person in a database.

2) Identification/Verification: the template which is generated during a recognition procedure is compared with all filed reference templates from the enrolment database. That identity is taken, for which the comparison has the closest similarity. After identification, verification follows. The live template is compared only with one reference template of the enrolment database which represents the indicated identity.

In the scope of these guidelines, biometric recognition procedures are treated as part of products in the field of intrusion detection, access control techniques and electronic locks. The requirements valid and specific for these products therefore are the same relevant for biometric recognition, too.

7.2.1.2 PSA Licensing Requirements for Door Supervision and Security Guarding

The full name of the scheme is “PSA Licensing Requirements - Door Supervision and Security Guarding”. We analysed the following documents:

1) PSA 28:2013 Standard for the licensing of door supervisors (Licensed Premises) and Security Guard (Static) Contractors. It provides a specification for compliance with the standards required for licensing by the Private Security Authority and applies to contractors seeking licences in the Security Guard (Static) and Door Supervisor (Licenced Premises) sectors. It took effect on 1 May 2014. Only the most recent edition of the document shall be applied, however it is not mentioned on what frequency basis any renewal takes place.
2) PSA 31:2014 Phase 1 Requirements for the licensing of Door Supervisor (Event Security), Door Supervisor (Licensed Premises), Security Guard (Event Security) and Security Guard (Static) Contractors. It provides a specification for compliance with licensing by the Private Security Authority and applies to contractors applying for a first licence in the following sectors, Security Guard (Static), Door Supervisor (Licensed Premises) and Security Guard (Event Security) and Door Supervisor (Event Security). It was issued in November 2014 and it will be reviewed occasionally.

Both documents have been developed by the Private Security Authority, the national regulatory and licensing body for the private security industry in the Republic of Ireland (public authority).

The scheme consists of the following sections:

1) General provisions regarding the organisation of the service provider (ownership, finances, insurance, premises, organisation information, compliance with legislation);

2) General provisions regarding staffing (selection and pre-employment screening, terms of employment, code of conduct, identification, uniform, threats and violence);

3) General provisions regarding training (training policy and responsibility, induction training, site-related training, basic training, trainers and training, specialist training, refresher training, supervisory and management training, training records);

4) General provisions regarding operations (risk assessments, command and control system, operations records, assignment instructions, security of information and access media, vehicles and drivers);

5) Provisions regarding compliance with PSA licensing (compliance with standards, PSA licensing requirements);

6) Specific provisions for security guarding services, additional to the general ones;

7) Specific provisions for door supervision services, additional to the general ones;


7.2.1.3 Code of Practice for Scaffold Alarm Systems (SAS)

The scheme to analyse is a Code of Practice for Scaffold Alarm Systems (SAS). This type of document has to be considered as a guide as it provides recommendations but it is based on the requirements of European standards for intruder alarm systems (EN 50131 series, for example\(^{323}\)), other codes of practice (such as BS 5979:2007\(^{324}\), for example) or guidance documents (RISC Authority document S6\(^{325}\), for example). The owner of the scheme is a certification body called SSAIB-Security Systems and Alarms Inspection Board that offers a wide range of schemes for providers of electronic security, fire systems and guarding services in the UK. SSAIB operates its certification activities in accordance with relevant accreditation standards as it requires the systems or services provided by registered organisations to comply with relevant British, European standards, International or, in this case, SSAIB Codes of Practice security standards applicable to the services provided\(^{326}\).

The scope of the scheme is to provide guidance to those responsible for specifying, designing, installing, commissioning, and where required, maintaining and repairing scaffolding alarm systems. The basic content of the document is focused in a) system functions and components; b) security grade of SAS (as it derives different requirements); c) functional and environmental requirements; d) operational and functional reliability; e) electrical safety; f) documentation; g) marking and identification; h) remote manned centre and ARC and i) a detailed list of application guidelines.

7.2.2 CCTV Systems

7.2.2.1 Code of Practice for the Cambridge City Council’s Public CCTV Scheme

The scheme to analyse is the Code of Practice for the Cambridge City Council’s Public CCTV Scheme. The Cambridge City Council is a public authority and is the owner of the Code. The Cambridge City Council’s Code of Practice sets out the aims of the CCTV system


\(^{324}\) BS 5979: 2007; Code of practice for remote centres receiving signals from security systems.


and how it will be used. The scheme has been developed in response to the growth of crime and fear of crime in the city and is designed to make Cambridge a safer and more welcoming place at any time of the day or night allowing all citizens and visitors, regardless of age, gender or race, the opportunity to participate fully and without fear in the life of the City. There are 139 cameras in the CCTV system covering Cambridge. These cameras are operated as a shared service with Huntingdonshire District Council, and are run from Huntingdon.

A significant feature of the scheme is the compliance with privacy requirements as the Code has been has been registered with the Information Commissioner’s Office and it follows the guidelines of the Data Protection Act 1998 and the principles of good practice identified by the Information Commissioner. In addition, Cambridge City Council’s CCTV system will comply with the Human Rights Act 1998, the Freedom of Information Act 2000, the Regulation of Investigatory Powers Act 2000 and the Protection of Freedoms Act 2012.

The document doesn’t specify the term of its validity or renewal. The Code of Practice for the Cambridge City Council’s Public CCTV Scheme is publicly accessible on the Internet.

7.2.2.2 Warwick District Council Code of Practice for CCTV Scheme

The scheme to analyse is the Warwick District Council Code of Practice for CCTV Scheme. This type of document has to be considered as a guide as it provides recommendations to inspire public confidence by ensuring that all public area Closed Circuit Television (CCTV) systems which are linked to the CCTV Control and Monitoring Room are operated in a manner that will secure their consistent effectiveness and preserve the civil liberty of law abiding citizens at all time.

The Code is complemented by other requirements and recommendations such as the ones contained in the Information Commissioners CCTV Code of Practice (published by the Information Commissioner Officer. ICO) or the requirements included in British standards such as such as BS 7958 and BS 7858 [(Code of practice for Closed circuit television - CCTV). Management and operation and Code of practice for Security screening of individuals employed in a security environment, respectively]. The owner of the scheme is a public authority, the Warwick District Council, who is responsible for the management, administration and security of the system.

The scope of the scheme shall apply to the CCTV surveillance known as the Warwick District Council CCTV Scheme. This scheme comprises of cameras (in a number over 180) located in specific external and internal locations within the Warwick District Council area, with control, monitoring and recording facilities at a dedicated location. These cameras have been sited to capture images of identifiable individuals or information relating to individuals which are relevant to the purposes for which the scheme has been established.

327 Website of Cambridge City Council:
The Code of Practice has a dual purpose, in that it will assist owners, management and operators to understand their legal and moral obligations whilst reassuring the public about the safeguards contained within it.

The basic content of the document is focused in a) fundamental principles and policies (related to privacy and release of information); b) data protection and legislation (as the Code of Practice is regulated according with the Data Protection Act, the Human Rights Act, the Regulation of Investigatory Powers Act and the Freedom of Information Act); c) accountability; d) control room management and operation; e) privacy and disclosure issues; g) recorded material management; and h) documentation.

The Code of Practice will be subject to annual review which will include compliance with the relevant legislation and Standards. Finally, the Warwick District Council Code of Practice for CCTV Scheme Code of Practice is publicly accessible on the Internet.\footnote{See the website: \url{https://www.warwickdc.gov.uk/download/downloads/id/208/cctv_code_of_practice}.}

\section*{7.2.2.3 Community-Based CCTV Scheme of the Irish Department of Justice, Equality and Law Reform}

The Community-Based CCTV Scheme is a procurement call under the Irish Department of Justice, Equality and Law Reform and administered by Pobal. The department devised the scheme in response to a demonstrated demand from communities across Ireland for the provision of CCTV systems. The overall purpose of the scheme is to support local communities who wish to install and maintain CCTV security systems in their area, with the aim of increasing public safety and reducing the risk of anti-social and criminal activity. This scheme is intended to support community-based organisations that wish to provide CCTV systems, in order to deter illegal or anti-social behaviour in places to which the general public have routine access, such as residential communities, city and town centres. It is not intended to cover the installation of CCTV systems in exclusively commercial areas such as shopping malls, industrial estates or business parks etc., where that is the primary objective of a proposal. It is not available to private interests such as clubs or individual groups in order to provide security for a specific building or premises.

The scheme is composed of three documents:

1) Community-based CCTV Scheme – Guidelines for application and appraisal process. They are intended to provide comprehensive information to community organisations on the application process, the appraisal process and the main issues that applicants need to consider and address when drawing up a proposal for a CCTV system and making an application for grant aid;

2) Code of Practice for Community-based CCTV Systems Authorised under Section 38 (3)( C ), Garda Síochána Act 2005. It sets out the basic conditions of use and highlights certain legal obligations set down in Data Protection Acts. It is reviewed
from times to times in order to ensure that it remains relevant in the context of technological changes and development;

3) Technical Specification for Community-based CCTV Systems Section 38 (3)( C ), Garda Síochána Act 2005. It outlines the minimum technical/operational criteria which Community-based CCTV Systems must comply with.

The above documents are downloadable from Pobal website and the Department of Justice, Equality and Law Reform at www.justice.ie. They are also available in ‘hard copy’ from Pobal. The Scheme operates under Section 38(5), Garda Síochána Act 2005. Furthermore, the camera housing assembly, complete with associated components and wiring must bear the CE mark.

7.2.2.4 NSAI Technical Annex TA-50132 for CCTV Installers

The scheme is the Technical Annex TA-50132. It is a certification scheme for CCTV installers, based on the EN 50132 series of Standards. Under the scheme, CCTV installation companies can be assessed against best practice requirements. The issuing organisation is NSAI (National Standards Authority of Ireland), the Irish Standardisation Body. It operates under the National Standards Authority of Ireland Act (1996) and is accountable to the Minister for Jobs, Enterprise and Innovation. NSAI is responsible for the standards setting in Ireland and the representation of Ireland in international and European standardisation organisations. Apart from standardisation, NSAI is also involved in issuing certification, monitoring and regulating metrology and training.


The scheme has thirteen sections including general sections, section on the marking, the certificate and the PSA 2006 and the requirements of the IS EN 50132. Under the scheme, NSAI inspectors assess the operations and procedures of alarm installers by:

- Inspecting a number of their alarm installations
- Comparing the results with the requirements of I.S. EN 50131/1
- Bringing any anomalies or non-compliances to the installer’s attention
- Specifying any necessary corrective actions
- Reviewing the corrective actions.

The successful procedure leads to an Irish Standard Mark License, which the installer is allowed to use along with the installation. After the granting of the mark, the NSAI follows-up with inspections at least once per year. Every client of the certified installer is entitled to receive a Completion Certificate after the installation. As mentioned earlier, the scheme has

329 See NSAI website: http://www.nsai.ie/About-NSAI.aspx
two normative bases, the Irish Standard PSA2006-12 and for the applicants that seek certification under the IS EN 50132, the requirements of the standard are also applicable.

### 7.2.2.5 EQA Scheme Regulations

The document examined is titled “Scheme Regulations”. It is not specific for CCTV systems, but rather the general regulations of the scheme. These are the rules governing the assessment and certification of organisations to national and international standards. Additional, more specific regulations, also apply. The issuing organisation is EQA, an Irish independent certification body providing third party verification of Management Systems, Products and Security Services in accordance with Irish, European and International standards. EQA reserves the right to revise the scheme regulations periodically. It consists of the following sections: Glossary of Terms, Authority, Enquiries, Applications, Access, Certificate, EQA Logo, Certification, Fees, Surveillance, Re-assessment, Confidentiality, Impartiality, Complaints, Withdrawal and Suspension of Certification, Multi-site Organisations, Appeals, Disputes, Accreditation, Register, Revisions.

### 7.2.3 Unmanned Aerial Vehicles (drones)

#### 7.2.3.1 JARUS Certification Specification for Light Unmanned Rotorcraft Systems

The scheme is the Certification Specification for Light Unmanned Rotorcraft Systems (CS-LURS) (version 1.0 – 30 October 2013). The issuing authority is JARUS, which stands for Joint Authorities for rulemaking of Unmanned Systems. JARUS is a group of experts from the National Aviation Authorities and the European Aviation Safety Agency. Its purpose is to “recommend a single set of proportionate technical, safety and operational requirements for the certification and safe integration of Remotely Piloted Aircraft Systems (RPAS) into airspace and at aerodromes. This requires review and consideration of existing regulations and other material applicable to manned aircraft and the drafting of specific RPAS guidance material to cover the unique features of RPAS”.

In the framework of the JARUS activities, there are several working groups (WG), such as the Operational and Personnel Requirements Group (WG1), Detect and Avoid Group (WG4) and the UAS System Safety Group (AMC UAS.1309) One of these WGs the Airworthiness Group (WG3), developed the document certification specification we examine.

The Certification specification has two parts (Books):

- The Airworthiness Code, which is applicable to Light Unmanned Rotorcraft Systems with Light Unmanned Rotorcraft maximum certified take-off weights not exceeding 750 kg

---


331 JARUS, Press release for a JARUS Information and Dissemination Workshop, 20 May 2014
• The Acceptable Means of compliance. AMC CS-LURS.1 defines the applicability of
the Book 2.

The document is freely accessible online on the website of JARUS. The scheme does not
mention its validity period and in general avoids references to legislation and other normative
references, apart from other relevant JARUS documents.

7.3 **Criteria for Legal Analysis of Schemes Operating in the EU**

The analysis of security, trust, efficiency and freedom infringement is based on criteria
extracted from the previous legal study. The analysis of schemes from a legal perspective
aims at highlighting how the existing schemes correspond to core requirements and demands
of the legislation.

7.3.1 **Criteria for Security Aspect**

1. **Risk Management**

The process, distinct from risk assessment, of weighing policy alternatives in consultation
with interested parties, considering risk assessment and other legitimate factors, and selecting
appropriate prevention and control options. The evaluation criterion aims at checking the
level of preparedness against security risks of the security PSS and whether the scheme
corresponds to this need. It is relevant also to the aspects of trust, efficiency and freedom
infringement.

2. **Data interference**

Illegal data interference is the intentional deletion, damaging, deterioration, alteration,
suppression or rendering inaccessible of computer data on an information system. The
criterion aims at examining whether there are counter-measures in place in order to avoid any
illegal data interference.

3. **System interference**

System interference in this context is the intentional serious hindering or interruption of the
functioning of an information system by inputting, transmitting, damaging, deleting,
deteriorating, altering, suppressing or rendering inaccessible computer data. The criterion is

---

332 For further analysis of the security criteria see chapter 3 of this Report “Legal Study on Security of Security
Products, Systems and Services: Mapping Legislation and Legal Demands for Security Products, Systems,
Services in the EU”

333 ENISA (2014) op.cit.

relevant to information systems and aims at examining whether there are measures in place to ensure that any intentional interference to the whole or any part of an information system is avoided.\textsuperscript{335}

4. **Performance**

Performance in this context is a measurable result, a quality with which the intended functions of the equipment are accomplished.\textsuperscript{336} The criterion examines the performance of the security PSS in relation to its function, i.e. whether it is constantly working or it activates in case of danger.\textsuperscript{338} The importance of this qualitative question does not lie with a yes/no reply, but with the differentiation under situations of the use and functionality of the security PSS. This criterion is highly relevant to the trust dimension, but also to the efficiency and freedom infringement.

5. **Accountability**

Accountability covers non repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.\textsuperscript{339} Also, it is the property that ensures that the actions of an entity may be traced uniquely to the entity.\textsuperscript{340} The criterion highlights the importance of employing policies and procedures to address the issue of accountability of the service provider or product/system manufacturer.\textsuperscript{341}

6. **User security**

By user is meant the scrutinized or observed, the person that undergoes the security process, but also the staff that is working with the equipment. The security/safety of the user is a substantial issue; the security PSS should not pose any risk to the users in the process of achieving other security objectives, such as border security. This criterion aims to tackle this specific issue, which is also very relevant to the trust and confidence of the users to the security PSS and to the freedoms and rights.\textsuperscript{342}

\textsuperscript{335} Directive 2013/40/EU, op.cit.
\textsuperscript{336} ISO 22300:2012 - Societal security -- Terminology
\textsuperscript{337} EN 60746-1:2003-02, Expression of performance of electrochemical analyzers
\textsuperscript{340} ISO/IEC PDTR 13335-1, Information technology — Security techniques — Management of information and communications technology security
\textsuperscript{341} Directive 2013/40/EU, op.cit.
7. Withdrawal mechanism

The criterion aims at examining how the security PSS responds to the possibility of security failure; what are the measures in place that aim at addressing this issue. This criterion is also relevant to the trust aspect, and to efficiency and freedom infringement.

7.3.2 Criteria for Trust Aspect

Trust encompasses the experience of the product provider as well as of the scrutinized in using the product. According to FP7 project SIAM, beside the experience, the subjective perception defines the way in which a product achieves an appropriate acceptance level. Evaluation criteria for the Trust dimension include, for example, the degree of discrimination regarding the use of product and the potential physiological and psychological invasiveness of the product. For instance, health risks such as DNA damage associated with the ionising radiation used in body scanners or other effects.

1. Actual Safety

Producers are obliged according to art. 3 of the Directive 2001/95/EC to place only safe products in the market. Art. 3§2 provides that a product is safe:

“A product shall be deemed safe, as far as the aspects covered by the relevant national legislation are concerned, when, in the absence of specific Community provisions governing the safety of the product in question, it conforms to the specific rules of national law of the Member State in whose territory the product is marketed, such rules being drawn up in conformity with the Treaty, and in particular Articles 28 and 30 thereof, and laying down the health and safety requirements which the product must satisfy in order to be marketed.

A product shall be presumed safe as far as the risks and risk categories covered by relevant national standards are concerned when it conforms to voluntary national standards transposing European standards, the references of which have been published by the Commission in the Official Journal of the European Communities in accordance with Article 4. The Member States shall publish the references of such national standards.”

For that reason, it is core obligation the PSS the provider develop and sell comply with the highest security standards not only in the time of purchase but in the entire PSS cycle-time. An optional update of the PSS at a cost to the consumer or user may only make performance improvements but in any case, it may be so substantial that makes the PSS useless.
contravening the economic interests of consumers as the TFEU, EU Directives and national legislation. Thus, providers shall ensure the PSS warrant the highest level of protection during the entire usable life. The security performance of the PSS is examined under the security aspect. In this criterion, the aim is to examine whether the user of the PSS is expected to put additional effort, such as buying updates, in order to guarantee the actual safety of the PSS.

2. Reliability

Trusting a security PSS also means to know how reliable it is. One way to test one aspect of the reliability of a security PSS through a certification scheme is to test it against the information it provides to the user. Information given in instructions should be clear and comprehensible, depending on the different technologies and areas of securities the security solution will be employed. The PSS should in any case operate as the instructions that accompany it. According to art. 5 Directive 2001/95/EC, the producer must provide consumers with the relevant information to enable them to assess the risks inherent in a product throughout the normal or reasonably foreseeable period of its use, where such risks are not immediately obvious without adequate warnings, and to take precautions against those risks.

In this way, producers must inform of risks which their product might pose taking appropriate action including, if necessary to avoid these risks, withdrawal from the market, adequately and effectively warning consumers or recall from consumers. Thus, the right to consumer information is required but not only at the time of purchase since in accordance with paragraph 3 and 4 of the above-mentioned art. 5 Directive 2001/95/EC, where producers know or ought to know that a product that they have placed on the market poses risks to the consumer that are incompatible with the general safety requirement, they shall immediately inform and cooperate with the competent authorities giving details, in particular, of action taken to prevent risk to the consumer.

It is therefore essential the producer commercialise a PSS with the attached detailed instructions adopting measures commensurate with the characteristics of the PSS they supply. They are free to decide the way of inform to the consumers (i.e. an indication, by means of the product or its packaging, of the identity and details of the producer and the product reference or, where applicable, the batch of products to which it belongs, carrying out of sample testing of marketed products, investigating and, if necessary, keeping a register of complaints and keeping distributors informed of such monitoring....) provided that this is appropriate to the characteristics of the PSS.

The criterion in this dimension, seeks exactly whether the certification schemes check the reliability of the PSS in relation to their instructions.

3. Transparency
Transparency is crucial for trust. Users need to know all information that might have an impact to the performance of the security PSS, but also to their freedoms and rights, including health and bodily integrity. This criterion seeks to examine the transparency aspect of the security PSS in relation to the information on attributes of the PSS given to the users.

4. Satisfaction of security needs

According to art. 38 CFREU, art. 114 TFEU, art. 3 and 8 Directive 2001/95/EC manufacturers have to ensure a high level of consumer protection in their PSS placing only safe products on the market. Art. 3 Directive 2001/95/EC establishes different presumptions on safety.

The clearest presumption is given by the paragraph 1, which points out that a product shall be deemed safe, when it conforms to the specific rules of national law of the Member State in whose territory the product is marketed.

In paragraph 2 establishes another presumption. A product shall be presumed safe when it conforms to voluntary national standards transposing European standards.

In this regard, codes of practice, security marks and seals are important to satisfy the needs of end users. They usually are granted by an entity to website or businesses for display for the purpose of demonstrating to customers the organisations are concerned with security and their business identity. Ultimately, the Directive establishes in art. 3 that in circumstances other than those previously mentioned, the conformity of a product to the general safety requirement shall be assessed by taking into account the following elements in particular, where they exist: (a) voluntary national standards transposing relevant European standards other than those referred to in paragraph 2; (b) the standards drawn up in the Member State in which the product is marketed; (c) Commission recommendations setting guidelines on product safety assessment; (d) product safety codes of good practice in force in the sector concerned; (e) the state of the art and technology; (f) reasonable consumer expectations concerning safety.”

This criterion differentiates from the actual security and safety in the sense that it is not necessary that the security PSS is providing actual results in order to satisfy the needs of the users, but the perception of satisfaction of the needs is sufficient to enhance the trust and confidence to the PSS. Also, since the “security needs” are subjective and there can be no criterion to cover the broad range of what users might perceive as security need and satisfaction of security need, this criterion seeks to examine how the this satisfaction or dissatisfaction of needs is communicated back to the producer. The criterion is related to the right to due process.
5. Detectability

The discussion on surveillance\textsuperscript{346} has highlighted that the scrutinized need to be aware of the security PSS and the fact that they are scrutinized. Security measures are not always observable and the scrutinized not always notified. This criterion therefore aims at examining how the existing certification and evaluation schemes deal with the issue of visibility of the security PSS and the notification of the scrutinized.

6. Maintenance

Relevant to the criterion of reliability, maintenance is important for the trust of the operators and scrutinized to the security solution. Security devices that are old and outdated can be harmful to the health of the users in a broad sense or in the case of digital solutions, gather inaccurate data. The issue of who is responsible for the maintenance of the security solution, the producer or the entity employing the PSS, is also relevant for the aspect of trust, since a clear allocation of responsibilities provides confidence to the users.

7. Respect for the environment

According to art. 114 TFEU and art. 37 Charter of Fundamental Rights, a high level of environmental protection and the improvement of the quality of the environment must be ensured in accordance with the principle of sustainable development. This provision affects not only to manufacturers and distributions but also to users and consumers. In this way, manufacturers or dealers should incorporate new technological improvements in PSS in order to increase the quality of the environment. In addition, by making the right use of the PSS, it might be possible to reduce or ever eliminate pollution. Therefore, end users should know perfectly how the PSS works. This criterion is also related to the efficiency aspect.

8. Ethical codes and Good practices

According to art. 3 Directive 2001/95/EC producers shall be obliged to place only safe products on the market. A product shall be deemed safe, as far as the aspects covered by the relevant national legislation are concerned, when, in the absence of specific Community provisions governing the safety of the product in question, it conforms to the specific rules of national law of the Member State in whose territory the product is marketed. However, there is nothing that impedes manufacturers increase the level of security in their PSS beyond what is allowed by law. For that reason, paragraph 2 of the art. 3 states that a PSS shall be presumed safe as far as the risks categories covered by relevant national standards are concerned when it conforms to voluntary national standards transposing European standards.

\textsuperscript{346}See analysis under freedom infringement Chapter
Codes of practice or ethic code of usage are voluntary guidance to increase the reliability of the marketing. Consequently, manufacturers are free to join them if they want to improve their competitiveness in the market. In this regard, there is a dual purpose to this system. On the one hand, manufacturers ensure compliance with high security standards (although it will depend on what kind of code of conduct is subscribed) and on the other hand, customers feel safer when acquire a PS that ensure greater security than others.

7.3.3 Criteria for Efficiency Aspect

From the analysis of efficiency aspect, it is clear that efficiency is not a legal term. The term of efficiency from a legal perspective is well represented in the legislation relating to energy efficiency\(^{347}\). In that respect, the term of efficiency is more extensively examined in the SWOT analysis (Deliverable 4.3.). In the legal analysis, we approached the term with the energy efficiency legislation as a driver of the content and approach in the context of CRISP. The selection of the criteria is primarily based on the previous analysis of the aspect of efficiency from a legal perspective.

1. Energy efficiency

Energy efficiency is defined as the ratio of output energy to input energy during an identified period. The criterion relates to the lifecycle costs of the security PSS and seeks to examine whether the schemes require the calculation of costs of efficiency measures during the expected economic lifecycle of the PSS and if the reply is positive, in which way\(^{348}\).

2. Optimal combination of improvements

Optimal combination of improvements is the maximum performance with least - cost combination of resources in the process of maintenance, inspection and updating. This is an efficiency criterion, derived from energy performance Directive, which however can be applicable to areas not necessarily linked to energy. Updating and regularly maintain the security PSS is substantial for the effectiveness of the PSS as a security solution. At the same time, spending too many resources for this type of procedure, might also be problematic. In that sense an optimal combination, a balance between the need for maintenance and improvements on the one hand and the costs for achieving this, should be found. Guidance and training of the human resources is a means towards achieving such balance. The criterion examines this issue, which is also of relevance to the security aspect.

\(^{347}\) For background of the efficiency criteria see chapter 5 of this Report

\(^{348}\) Dir. 2010/31/EC, op.cit.ANNEX III
3. Minimum Performance Requirements

Minimum performance requirements in this context is related to the adaptability of the security PSS to technological progress and the way that this is achieved with the less cost. According to Recital 10 Directive 2010/31/EC, it is the sole responsibility of Member States to set minimum requirements for the energy performance of buildings and building elements. Each member state has to regulate energy performance of buildings and building elements according to their needs and sources and very often, it happens with another PSS. In terms of efficiency, it must achieve the cost-optimal balance between the investments involved and the costs. For that reason, it is important manufacturers and distributors produce and sell a PSS with certain guarantees such as it works correctly and efficiently. On the other hand, consumers should take an intended purpose that will vary depending on the specific PSS. The criterion examines whether the schemes address the issue of following the technological progress and incorporating new elements in the security PSS.\(^{349}\)

4. Efficiency of Enforcement & Procedural Economy

The Communication (2013) 401 Final and the Recommendation 2013/396/EU analyse Collective redress. It is a procedural mechanism that has different interests. In a positive aspect, it allows, for reasons of procedural economy and/or efficiency of enforcement, many similar legal claims to be bundled into a single court action but in a negative aspect, it would increase abusive litigation bringing speculative claims. There is no EU legislation in such procedural aspect. However, some codes of practice, seals and marks adhered by some organisations recognize the right to consumers to adhere to collective redress. It is common in the alternative dispute resolution system (i.e. arbitration). Consequently, although it is a drawback for manufacturers or providers/distributors and it is not a current legally binding assignment, it has been considered as a high added value by consumers and users.

This criterion is examined in connection to collective redress mechanisms.\(^{350}\) Collective redress mechanisms, single claims to be bundled into a single action or (i) a legal mechanism that ensures a possibility to claim cessation of illegal behavior collectively by two or more natural or legal persons or by an entity entitled to bring a representative action (injunctive collective redress); (ii) a legal mechanism that ensures a possibility to claim compensation collectively by two or more natural or legal persons claiming to have been harmed in a mass harm situation or by an entity entitled to bring a representative action (compensatory collective redress). The criterion is related to trust and freedom infringement aspect in terms of the right of due process and fair trial.\(^{351}\)

\(^{349}\) Dir. 2010/31/EC, op.cit. Recital 10


\(^{351}\) Art. 47 Charter of Fundamental Rights EU, art. 6 ECHR op.cit.
7.3.4 Criteria for Freedom Infringement Aspect

The evaluation criteria refer to specific freedoms and rights, which are: the right to private life, the right to protection of personal data, bodily integrity, the freedom of movement and the freedom from unlawful detention, the right to due process and fair trial and the presumption of innocence. The selection of the above freedoms and rights was based on the results of other projects, such as the SIAM, SAPIENT, IRISS etc. and the wording of the CRISP Description of Work. The list of potentially affected rights and freedoms is not exhaustive. Other rights and freedoms might also be affected or infringed from security measures employed in different areas of security. Additionally, as with the other aspects, the focus is on core issues related to every criterion.

1. Due Process and fair trial

The right to due process and fair trial in the context of security PSS is related to fairness in proceedings in accordance with established and sanctioned principles. The criterion is examined from the aspect of reasonable deadlines, right to access and rectification of material. As with every criterion in the freedom infringement aspect, due process and fair trial is highly related to the trust aspect.

2. Non-discrimination and equal treatment

The differential treatment on the basis of the protected grounds of sex, race, color, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation is in principle prohibited according to art. 14 ECHR and art. 21 Charter of Fundamental Rights of the European Union. The criterion examines the rights of non-discrimination and equal treatment in relation to categorisation by the security PSS based on observable traits (eg. Religious signs, skin color, sex etc.), the exposure of the protected grounds and the protection of vulnerable groups, such as the minors and the disabled persons.

3. Freedom from unlawful detention

Freedom from unlawful detention is protected under the right to security and liberty in art. 5 of ECHR. The article establishes the right of individuals not to be deprived of their liberty unless in accordance with a procedure prescribed by law. In the context of security PSS, this article may have tremendous importance for the individuals. Freedom of movement is one of the main EU fundamental rights. Art. 5 ECHR stipulates that everyone has the right to liberty

---

352 For further analysis of the freedom infringement criteria see chapter 6 of this Report, “Legal Study on Freedom Infringement in the Context of Security Products, Systems and Services”.

353 Art.6 ECHR, op.cit.
and security of person. In addition, Protocol 4 ECHR to the Convention for the Protection of Human Rights and Fundamental Freedoms securing certain rights and freedoms other than those already included in the Convention and in the First Protocol thereto greatly expands the scope of the freedom of movement in art. 2. It is included the right to liberty of movement and freedom to choose a residence and the right to leave freely any country, including his own.

No restrictions shall be placed on the exercise of these rights except from in accordance with law and justified by the public interest in a democratic society. Thus, the general rule is that no one shall be deprived of his liberty. The retention must follow the principle of proportionality and can only be make use of them the aforementioned assumptions.

In addition, paragraph 2 states that everyone who is arrested shall be informed promptly, in a language he understands, of the reasons for his arrest and of any charge against him.

Although a mere PSS could guarantee the language that the detainee understands, they cannot indicate the cause of his arrestor or another relevant information applicable to the specific circumstances of the case. It is another evidence that PSS need highly qualified personnel to ensure compliance with this legal provision. Regarding to paragraph 3, everyone arrested shall be brought promptly before a judge or other officer authorised by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial. Only the competent court and justice officials can control these specific requirements although PSS are important to assist them to the achievement of the legal requirements. Paragraph 4 stipulates that the arrestee shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court. A PSS can be of enormous importance to facilitate rapid communication between the arrest and the competent court. To do this, the cautions required by law shall be included in the PSS and shall always be controlled by justice officials. Ultimately, in the current state of the art, freedom of a person cannot be left to a mere PSS without any other caution since they always have a margin of error. The purpose of these safeguards against possible risks is to make the system more efficient and more open based on principles that protect the fundamental rights. In case of contravention of the provisions of this Article, according to paragraph 5, the arrestee shall have an enforceable right to compensation.

4. Freedom of movement

Art. 2 of the Additional Protocol to the ECHR, establishes the liberty of individuals to move within the territory of a State, to leave the country and the freedom of choice regarding the residence. The restriction of the liberty may be justified only when in accordance with the law, necessary in a democratic society and in the interests of national security, the maintenance of ordre public, for the prevention of crime, for the protection of health or

354 The right is also protected in art. 45 of the Charter of the Fundamental Rights of the European Union
morals, or for the protection of the rights and freedoms of others. The criterion (if applicable, eg. in case the security PSS can violate the freedom of movement) aims at examining the safeguards of the security PSS for the protection of the aforesaid freedom.

5. Bodily integrity

This criterion refers to the inviolability of the physical body and emphasizes the importance of personal autonomy and the self-determination of human beings over their own bodies. Procedures such as the involuntary examination of the human body fall under the protection of the right.

6. Presumption of Innocence

The criterion examines the presumption of innocence in line with the art. 48 Charter and 6 (2) ECHR in the context of security PSS in relation to following attributes; 1. Whether the PSS presents the scrutinized in ways that tend to suggest guilt, 2. Whether the security PSS obtains any response by coercive means or in ways that lead to self-incrimination and how the security PSS addresses the right of non-incrimination of the scrutinized. 3. The clarity and accuracy of the developed evidence against the scrutinized, so that the right of defence is facilitated. According to art. 48 ECHR, everyone who has been charged shall be presumed innocent until proved guilty according to law. The respect for the rights of the defence of anyone who has been charged shall be guaranteed.

Closely related to presumption of innocence is the privilege of the person against self-incrimination that guarantees art. 49 ECHR. For that reason, for example, material recorded from CCTV cameras must not be itself a proof of charge against anybody but the scheme shall guarantee this privilege and the images will only be released (to the Police and other enforcement agencies) to conduct investigations into potential criminal offences. It must ensure CCTV system is examined in detail to ensure they are proportionate, legal, appropriate and necessary. a) Regarding to proportionality, it must be discriminated between images which are not required for the purpose for which the equipment is being used (in this case the images will not be retained for longer than is necessary) and images which may need to be retained for longer periods as a requirement of an investigation into crime. If Images are retained for evidential purposes, they will be retained in a secure place where access is controlled within the legally established framework. b) Regarding to legal aspects, for example according to art. 2 and 3 ECHR for example, it guarantees the right to interpretation and the right to translation of essential documents. c) The measures must be appropriate and/or necessary for the particular case. The presumption of innocence is a fundamental right

355 Art. 6 ECHR, arts. 48 and 49 CFREU and art. 6 Proposal for a Directive of the European Parliament and of the Council on the strengthening of certain aspects of the presumption of innocence and of the right to be present at trial in criminal proceeding.
that takes precedence over other rights. In the event this right can be in conflict with another fundamental right the conflicting interests shall be weighed (i.e. CCTV shall not record in private spaces unless the people affected give their express written consent).

7. Location of data
Location data means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service. Here the criterion examines how the security PSS handle the location data, taking one step further from the strict interpretation of the scope of the ePrivacy Directive.

8. Protection of information against automated Profiling
Automated profiling is assembling personal data, creating disproportionately large datasets that can be used for anticipatory action in an automated way. The criterion aims at examining whether the security PSS support or base part of their operations on automated profiling and how they address the matter. Art. 15 (1) of Data Protection Directive provides:

“Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.”

The article provides for acceptable cases of such conduct in two specific cases, which both involve the obligation for the responsible entity to take measures to safeguard the data subject's legitimate interests. The criterion is related also to the security and trust aspect.

9. Function Creep
Function creep in this context is the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, especially when this leads to potential invasion of privacy. The criterion in line with this definition, seeks to see whether and if yes for which purposes the security PSS can be used for further purposes.

356 art.6. 2002/58/EC as amended op.cit.
10. The right to private life

The right to private life, as analysed in the previous section of this report, is a fundamental right protected at Council of Europe and European Union level. The analysis of the impact of technologies to the right of privacy and the rich case law of both the ECtHR and the CJEU calls for an inclusion of the right as a criterion in the evaluation of schemes. More specifically, applying the three criteria for limitations of the right pursuant to art. 8 § 2 ECHR, the criterion seeks to examine whether the interference to the private life of the scrutinized by the security PSS is in accordance with the law, pursues a legitimate aim and is necessary in relation to the result that aims to achieve. As every criterion of the freedom infringement evaluation, privacy is highly relevant for the trust aspect.

11. The right to protection of personal data

The right to protection of personal data is also analysed thoroughly in the relevant section. The fundamental right is protected as a separate right from the right to private life in the Charter of Fundamental Rights of the EU (art.8) and as an aspect of the right to private life in the ECHR (art.8). The questions related to this criterion, address core issues of the right as identified in the chapter 6.1.2. of the Report, which include:

- Purpose limitation and purpose specification
- Data accuracy
- Measures relating to the fair and legitimate processing
- Necessity of processing
- The rights of the data subjects
- The handling of sensitive personal data
- The data security organisational and technical measures
- The retention periods of the personal data
- Data transfers and third party access
- Profiling
- Function creep
- Notification of processing to the data subject
- The elements of a valid consent (when consent is the legal basis of legitimate processing of the data)
- The requirement of Privacy and Data Protection Impact Assessment
- Accountability mechanisms
- Data Protection by Design
- Security Breach Notification

7.4 ANALYSIS OF EXISTING SCHEMES ON THE BASIS OF STEFI ASPECTS
The following section includes the highlights of the analysis of schemes based on the STEFi aspects.

### 7.5 Security Assessment of Existing EU Schemes

The analysed schemes responded adequately to the minimum legal requirements in relation to security. As their main objective is either to assess, evaluate or certify security products, systems or services, it is reasonable that security is one of the priorities of the schemes.

The type of the scheme plays a role in how far the scheme goes in embracing the security aspect and setting security requirements for the security measure to be certified or assessed. The schemes that lead to certification focus on ensuring that the certified security measure will fulfil security requirements at many different levels such as risk management, performance and end user security. Codes of practice and evaluation schemes on the other hand, although they contain provisions related to security, this is not their primary focus; they require several organisational and technical measures to be implemented, but these requirements are quite often limited to a minimum acceptable level.

The issuing body also plays a role. The SSAIB Code of Practice for Scaffold Alarm Systems, even though is a code of practice, it can be said its main objective is the security assessment. Evaluation schemes by public authorities may be less concerned about the security requirements and more about other aspects, such as the freedom infringement.

Another factor that also influences the security aspect, is the type of security measure and specificities of technologies employed in the security measure. For instance, the development of an information system in the framework of a security measure creates the need for security requirements in the scheme that address the information system interference risks. A CCTV system for a district in the UK, has different security requirements than an access alarm system that uses biometrics for identification. The certification specification of JARUS on drones is very much detailed in terms of security. The two books included in the documentation of the scheme have a technical character and respond to the security criteria very well. The potential impact of a drone on the security of the citizens, infrastructures and other fields of security, and the capabilities of the technologies employed on the drone, requires that the scheme covers a broader range of security criteria to be met.

Going into more detail with regard to the response to the criteria of the security assessment, the JARUS certification specification includes a series of provisions for risk management, such as contingency procedures, fire prevention risk, risk of explosion, third party prevention and failure in service risk. Moreover, there are clauses related to data integrity. An important asset of the JARUS scheme is the reference to safety of people, both of staff and other individuals.

Accountability is an important issue for security. Most of the schemes do not address the issue of accountability for the security aspect. The Cambridge CCTV Code refers to
accountability only briefly, requiring the “need for a well-defined structure of responsibility
to the public maintaining public support and confidence in the CCTV system”. The way it
addresses the matter of accountability however, i.e. copies of the code of practice are made
available for public inspection and formal complaint procedure for the operation of the
CCTV, seems to be insufficient to address major security questions related to accountability
such as the one of liability related to the operation of the CCTV system. The Warwick Code
of Practice for CCTV (Clause 6) affirms that Warwick District Council and the Partners
support the principle that the community at large should be satisfied that the Public
surveillance CCTV systems are being used, managed and controlled in a responsible and
accountable manner and that in order to meet this objective there will be independent
assessment and scrutiny. This clause also establishes the responsibility of all parties to
maintain a continuous review of its integrity, security, procedural efficiency, methods of
operation and retention and release of data and it enumerates the hierarchy and grades of
responsibilities (the owner, the manager, the supervisor and the operators). Accountability of
the manager/supervisor towards the owner of the scheme and periodic progress reports on the
scheme are also contemplated in the scheme (clause 6.1 to 3).

The schemes also do not address the criterion of withdrawal mechanism. In the case that the
product fails in security for any reasons that is related to the product itself and not the use,
installation etc. the manufacturer should have a mechanism in place to remove the product
from the market. However, the examined documentation of schemes does not require the
development of such mechanism. This is different from the revocation of the license or the
certificate. The schemes usually either in the normative part of the scheme or in another
document setting the general requirements for certification of the issuing certification body
address the issue of revocation. For instance, the NSAI scheme on CCTV installers foresees
several grounds for revocation of the license to provide services under the relevant mark,
such as the non-response to non-conformities.

In relation to risk management and threat response, the Vds Scheme for Biometric
Recognition addresses risk management, threat responses and system and data interference by
providing “tamper security” clauses in the text, which must be read in combination with the
respective product specific guidelines. As mentioned earlier in this section, most of the
examined schemes deal with the minimum security requirements, as the schemes are intended
to evaluate security products, systems or services. A qualitative analysis of the requirements
shows that there are varying levels in the way the schemes address the security issues.

7.6 TRUST ASSESSMENT OF EXISTING EU SCHEMES

With regard to the trust evaluation, the analysis of this STEFi aspect is mostly addressed in
schemes that are of evaluative nature but do not lead to certification. Codes of practice and
Community evaluation schemes require from the security PSS they examine to be more
transparent in relation to the information on the attributes of the product, to the detectability
of the security measure and the of awareness of the individuals.
The community-based CCTV systems of Irish Department of Justice, Equality and Law Reform (procurement call), covers the criteria of reliability, maintenance and transparency, along with detectability, which are crucial in the case of CCTV. The technical specification (clause 5.6.) requires that signs should be placed so that the public is made aware they are entering an area where CCTV cameras are in operation. Very important is the requirement that the signs show that CCTV cameras are in operation and identify the organisation legally responsible for the system. For maintenance, the Technical Specification recommends that a maintenance contract should be put in place to ensure the system is maintained in full working order. The contract should include the provision of a regular maintenance schedule and maintenance callout procedure with suitable response times. The PSA scheme for door supervision and security guarding deals well with some of the trust criteria only. It generally satisfies detectability and the users’ security needs as it is perceptible and observable. Ethical codes are also present: there is a Code of Conduct that the staff must respect. It is not mentioned, though, whether safety codes or good practices in the sector concerned are monitored by the company.

Trust of end-users can be considered one of the strongest points of Warwick’s CCTV code. The scheme imposes a high standard in terms of confidence as the system observes the recommendations contained in the Information Commissioners CCTV Code of Practice, the ICO’s code of practice to help organisations using CCTV to stay within the law (clause 1.3). Transparency is granted to end-users through various ways: first, by following a public consultation among residents before cameras are placed in residential areas (clause 4.2.11); second, by providing a point of contact to establish communication with the owners of the scheme where enquirers will be provided with the relevant documentation (clause 4.4); third, by providing clear and simple instructions to make a complaint about the system (clause 6.6). The complaint procedure assures documentation of the process, a record of the number of complaints or enquiries received together with an outline of the action taken, a deadline to response (3 working days) and a compulsory investigation (within fifteen working days) and fourth and most important, by the provisions contained in clause 4.3 as the area protected by CCTV will be indicated by the presence of signs. The signs will be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The signs will state the organisation responsible for the scheme, the purposes of the scheme and a contact telephone number.

The VdS guidelines for biometric recognition procedures in alarm systems deal with some of the trust criteria. Functional reliability requirements are applied not only regarding what is valid for the respective device and also contained in the respective products guidelines, but also the special characteristics of the biometric recognition procedures are also taken into account. The criteria of detectability and satisfaction of security needs are also met. The NSAI Technical Annex for CCTV installers addresses the actual safety criterion: the certification body, NSAI, sets routine inspections to the installations of CCCTV systems at least annually. Moreover, the installer is required to make available to the customer a
maintenance and repair service contract, which should be available throughout the lifecycle of the CCTV system.

In terms of reliability, the JARUS certification specification, requires that a reliability program should be provided in order to demonstrate that the product (engine and powerplant installation) can ensure a safe operation between the proposed normal inspections or overhauls. However, ethical codes and best practices criteria are not covered.

Trust also a prominent place in the SSAIB Code. The scheme ensures the transparency by the assessment of the quality of instructions for operating the SAS. In this regard, the SSAIB-Code of Practice determines the assessment of the system functional reliability. For this purpose, it states that SAS components shall comply with relevant standards and this objective could be achieved, among others, by “clear rules for design and installation, clear rules for adjustment and maintenance...” (clause 10). Furthermore, the scheme requires documentation relating to a SAS to be concise, complete and unambiguous. Information shall be provided sufficient to install, put into operation, operate and maintain a SAS (clause 13). Also, the scheme checks that the handover of the system to the user should be carried out by a person with the appropriate training and experience, if practical a full demonstration of the SAS should be provided including the operation of detectors and how these should be tested and an explanation of the functions of the installation should also be provided. Communication procedures with the RMC or ARC should be explained. Besides, clear and concise operating instructions should be provided, these should include both how the CIE is operated, the specific setting and un-setting procedures for the SAS and how to avoid unwanted alarms (clause 16.26.4). With regards to satisfy security needs for users as the SSAIB-Code of practice specifies a minimum of two access levels typically for use by the user, the alarm company and even additional access levels may be provided e.g. for Guards or other third party response personnel (clause 8.2.1). A location survey is also programmed by the SSAIB-Code of Practice to be successful in the objective for installing a SAS (to detect vandals and unauthorised persons who have gained access onto the scaffolding). In this regard, during the location survey there are many factors to consider when designing a SAS such as the possibility of unauthorised persons gaining access to the scaffolding from the roof, fire exit doors and other openings or adjoining property. In addition the construction, location, contents and theft history of the premises or site should be taken into account (clause 16.12.1). Reliability on the system is also assured as the scheme evaluates not only means of detecting and indicating fault conditions in many components (detectors, prime power source, alternative power source, interconnections, alarm transmission systems, warning device) but also the discrimination between genuine and false intrusions in order to minimise the risk of unwanted alarms (clause 16.14). The document sets out a quite important – but not exhaustive – list of regulations to be considered (the Health and Safety at Work etc. Act 1974; the Work at Height Regulations 2005; the Construction (Design and Management) Regulations 2007; the Personal Protective Equipment Regulations 2002; the Control of Noise at Work Regulations 2005) (clause 16.4.1). The weakness of the scheme, from our point of view, resides on the obligations to maintenance and repair and the responsibility. With respect to the first guideline, the SSAIB-Code defines that it is the client’s responsibility to
arrange for the SAS to be properly maintained (inspected and serviced) and repaired as necessary.

In terms of environmental protection, the EQA scheme is complemented by the EQA Environmental Regulations \[^{357}\] , which are developed for compliance with the ISO 14001:2004 Certification\[^{358}\].

### 7.7 Efficiency Assessment of Existing EU Schemes

Even though the legal demands in relation to the efficiency aspect are limited, the evaluation and certification schemes either do not respond to those demands or it is not clear from the documentation available the way they address the efficiency issues of security products, systems or services.

Taking as an example, the Warwick CCTV Code; the code does not include many references to the recognition of criteria for efficiency. Nevertheless, some clauses can be indirectly related to efficiency. In general terms, the scheme requires that the system will only be operated by trained and authorised personnel (clause 4.2.13). More specifically, the Warwick Code of Practice emphasizes the training and competence of all persons employed to act as operators of the system and obliges them to be trained to the highest available industry standard. For example, clause 6.7.1 imposes all personnel employed to control/operate or manage the scheme to be security screened in accordance with British Standard 7858: 2004 Code of practice for screening of personnel in a security environment. Similarly, clause 6.7.2 enforces all operators to be trained to the criteria required by the private Security Industry Act 2001 and licensed by the Security Industry Authority for Public Space Surveillance systems.

An annual assessment of the scheme is included in clause 6.4 as a mechanism to evaluate the effectiveness of the system. The annual assessment of the scheme will be undertaken by an independent consultancy appointed by the owner. This will include annual reviews of the scheme’s operation, performance and working practices and, where appropriate make recommendations for improvements. The results will be assessed against the stated purposes of the scheme. If the scheme is not achieving its purpose modification and other options will be considered. Efficacy and justification of the CCTV system by an annual review is also stipulated by the Information Commissioner’s CCTV Code of Practice. This document further states that it is necessary to establish the system’s effectiveness to ensure that it is still doing what it was intended to do. It is does not achieve its purpose, it should be stopped or modified. An important criterion to evaluate efficiency of the security system is the prevision contained in clause 6.5 as it might be put in relation with the CRISP criterion “Minimum

Performance Requirements”. The clause imposes regular independent random audits. These audits will check the operation of the scheme and the compliance with the code of practice having into consideration the following aspects: the level of attainment of objectives and procedures, random audits of the data log and release of information, the review policy, standard costs for the release of viewing of material, the complaints procedure and compliance with procedures.

The Scaffold Alarm system code scheme includes several requirements regarding efficiency of the system. Notably, the so-called “system design” has the objective of determining the extent of the SAS and select components of the appropriate functionality/performance criteria, grade and environmental classification and to prepare a system design proposal, e.g. number and type of detectors and their location (clause 16.12). Furthermore, the Code of Practice includes efficiency indications relating to operational reliability as means shall be provided to ensure that operator errors which might adversely influence the normal operation of an SAS are either prevented or indicated and components of an SAS used during the operation of an SAS shall be clearly and unambiguously marked and logically arranged in such a manner as to minimise the possibility of incorrect operation (clause 9).

Recommendations on the expertise and skills of personnel are of primary importance and the scheme imposes training for the staff to work at height and in the use of ladder/step ladder and other access equipment. Training and experience is also required for persons responsible for risk assessment and the design, installation planning, system installation, maintenance and repair of SAS. Such training should include that related to health and safety issues and related legislation with regard to the risk associated with working on scaffolding. The scheme even provides some instructions for the case of handover and it considers that, if possible the Handover of the SAS to the user, should be carried out by a person with the appropriate training and experience. Besides, the need for operatives to be registered to the CSCS scheme or another Health and Safety scheme required by the client or contractor is considered in the SSAIB-Code (clauses 16.4, 16.7 and 16.26.4). As it has been highlighted in the paragraph above, responsibility and maintenance/repair of the SAS are aspects for improvement and this might adversely influence on the performance requirements.

Schemes might indirectly refer to efficiency; the VdS guidelines for biometric recognition procedures in alarm systems deal with efficiency, even indirectly, as the foreseen test methods which aim at reviewing the minimum performance requirements, functional reliability and operational security may provide with insight in terms of efficiency as well.

Quite often, efficiency criteria are not applicable or relevant. For instance, the NSAI technical annex refers to CCTV installers and as a result some of the criteria are not applicable, such as the collective redress mechanism. However, efficiency is taken into account in the case of maintenance, inspection and repairs. More specifically, the applicant shall provide equipment and tools so that he or she enables the efficient maintenance, inspection and repair service to the clients. How efficiency is achieved or what is considered to be efficient in this case is not further specified in the document.
7.8 FREEDOM INFRINGEMENT ASSESSMENT OF EXISTING EU SCHEMES

The potential of violation of rights and freedoms of individuals by the security products, systems and services has been highlighted in the legal study of this report. The impact of the technologies to privacy and data protection, the collection and storage of big data, the tracking and profiling, the discrimination based on sex, religion, ethnicity are reasons that urge for protection of the threatened rights and freedoms. The certification schemes have the potential to contribute to the protection of aspects of the individual rights and freedoms.

The analysed schemes vary in the ways they correspond to this need for protection. A very limited number of schemes includes requirements and clauses related to freedoms and rights, mainly related to the protection of private life and personal data. Other schemes include references to the relevant legislation and indicate that the legislation is a normative requirement; alternatively, they only include the reference in an Annex and do not relate the evaluation that takes place in the framework of the scheme to the requirements of the legislation.

Last but not least, there is a number of schemes that do not make any reference to requirements for freedoms and rights. This might be for several reasons: the document is technical and it is out of its scope to cover such societal requirements; the document is part of the scheme’s documentation and such requirements are included in another document, such as the general requirements or the normative part of the scheme. As we will see later in this analysis however, the above reasons are not sufficient to exclude the freedoms and rights from requirements.

A positive example of an evaluation scheme is the Warwick District Council Code of Practice for CCTV Schemes, which deals with freedom infringements in most of its content and this dimension of the scheme must be considered as the most relevant aspect of the document. Having in mind that the object of the scheme is to assess the management and operation of CCTV systems, the issue of privacy has to be considered as the most important one to be evaluated and granted by the scheme because the system might seriously interfere with the private lives of the scrutinised. The list of fundamental principles and policies of the scheme (clause 4) is headed by the recognition of rights of privacy as “Warwick District Council and partners support the individual’s right to privacy and will insist that all agencies involved in the provision and use of Public surveillance CCTV systems connected to the control, monitoring and recording facility accept this fundamental principle as being paramount”. Among its principles of management, the Code mentions the obligation of the scheme to operate “with due regard for the privacy of the individual” (clause 4.2.10). As a final guarantee, clause 5.1 establishes that the scheme is registered with the Data Protection Commissioner.

More specifically the Code of Practice addresses the issue of privacy and data protection by devoting several chapters to the assessment of the recognition of data protection rights and facilitates persons many ways to exercising those rights in the Appendixes (A and B).
Going to the basis of this issue, the scheme is inspired in the fundamental legal documents on data protection and demands the observance of some other privacy standards (such as the ICO CCTV Code of Practice). This obligation primarily assures that the interferences of the system have a legal basis. The aim of the interference is legitimate as its finality is to reduce crime and the fear of crime across the district making the streets safer for everyone, improving security in car parks or helping Warwickshire Police identify offenders and contribute towards the management of the District.

The UK is recognized as a leading user of CCTV and such systems continue to enjoy general public support because they accept them as a helpful mean of fighting and reducing crimes. In this sense, the processing of personal data is based on *public interest*, one of the criteria of art. 7 of the Data Protection Directive. But confidence of people remains on the responsibly and proportionate use of the CCTV systems: the intrusion of privacy is then accepted and can be considered as proportionate as the scheme evaluates that the use of CCTV in Warwick District is covered by legal requirements (Acts). CCTV system involves processing of personal data such as images and information about people which is derived of these images but the scheme doesn’t allow for the automated building of large data-sets that could be used to perform predictive analysis. The Warwick Code of Practice foresees measures for the fair and lawful processing of the data as, first, it collects personal data for specified, explicit and legitimate purposes (the storage, processing and use of the recorded data obtained by the CCTV system is guided by the following general principles: recorded data will only be used for the purposes defined in the Code of Practice and in accordance with the provisions of the Data Protection Act and Human Rights Act; access to recorded data shall only take place in the circumstances defined in the Code of Practice and the provisions of the relevant legislation; recorded data will not be sold or used for commercial purposes or the provision of entertainment; the showing of recorded data to the public will only be permitted in accordance with the law in relation to the investigation, prosecution or prevention of crime. Clauses 8.2.1.e) f) h) i), 8.3 and 8.4) excluding, for example, disclosure of images of identifiable individuals to the media or place them on the internet (clause 8.12), personal data are kept for no longer than necessary for the purposes for which they were processed (clause 8.2.1. Also, Appendix C where it is established that all recordings are retained for a minimum of 31 days. If no legitimate requests for retention of the recording has been made it is then erased. All requests for retention of recordings are considered against the provisions of the Data Protection Act, Human Rights Act and the Code of Practice. Also the removal of medium on which images are recorded, for viewing purposes, will be documented in accordance with Data Protection principles and the procedural manual. Clause 8.6), the system keeps accurate and kept-up-to-date personal data, the scheme only processes personal data that are adequate, relevant and not excessive for the purposes for which they were collected and/or further processed: clause 4.2.5 determines that Help Points are to be used in conjunction with the cameras. And the clause inserts one limitation as the audio communications incorporated in the help points are initiated by those requiring assistance and cannot be used to record conversations between members of the public.
In case the processing is based on consent, is the scrutinised (data subject) duly informed on the object and consequences of consenting and that he or she does not act under pressure. The Warwick District Council gives public and open information about the location of CCTV cameras on its web page giving compliance to the legal obligation of informing the data subject about the recording of their images.

The scheme evaluates if the security system has in place procedures to enable the exercise of the data subjects rights. Access to data in the terms provided for in section 7 of the Data Protection Act 1998 are assured in the scheme by providing people a standard subject access request form. Within 40 days of receipt, a written response to the request will be provided either setting out the steps intended to take to comply with the request or setting out the reason for refusing the request (clause 8.9). Prevent processing of personal data is accepted when processing is likely to cause substantial and unwarranted damage (clause 8.11). The inclusion of comprehensive (but also simple) subject data access form to apply for access to information held on the CCTV system (Appendix A) and a precise brochure containing advice and information regarding data recorded by the CCTV system and gaining access to that data (the so-called CCTV scheme leaflet. Appendix B) are very much appreciated.

As a guarantee for data rights, the Warwick Code determines that the owner of the scheme plays the role of data controller as prescribed by the Data Protection Act 1998 Section 1 Subsection 1(1) (clause 6.2.1)

The scheme includes an explicit obligation to undertake an impact assessment, prior to the installation of cameras, to determine whether CCTV is justified and how it will be operated. This obligation is considered as a principle of management of the scheme in compliance with the Information Commissioners CCTV Code of Practice (clause 4.2.1). The impact assessment is complemented with an operational requirement for each proposed camera to dictate the quality of images required as it is a recommendation of the Information Commissioner (clause 4.2.4)

The scheme defines sensitive personal data in a general way that can be considered as ambiguous although the definition that has to be accepted is the one included in the Acts (clause 1.5.10). The scheme also stands out as the most significant of these data “The commission or alleged commission of any offences and any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings”. This definition has to be put in relation with presumption of innocence as the scheme evaluates the quality of recorded material and

359Website of Warwick District Council:
http://www.warwickdc.gov.uk/info/20109/crime_and_law_enforcement/112/cctv. The information is:
“Currently the scheme monitors over 180 cameras located primarily in the Warwick, Kenilworth and Leamington town centres and multi-storey car parks. Other locations covered by CCTV Camera’s monitored in the scheme are: Lillington Crown Way Shopping Precinct, Mason Avenue and the Community Centre’s, Whitnash Acre Close Shopping Precinct, Community Centre and Recreation Ground, Washbourne Fields and Coppice Road (Millenium Gardens) plus Jephson Gardens Temperate House, The Royal Pump Rooms and cameras covering parts of the council's housing stock”.
imposes that a) recorded material should be of high quality and b) in order for recorded material to be admissible in evidence total integrity and continuity must be maintained at all times” (clause 9.1.1). The same cautions are imposed for elements (cameras) used by the system: “High quality cameras both fully functional with pan, tilt and zoom and static are in use” (clause 1.6.5). The scheme doesn’t contain specific provisions for bodily integrity and non-discrimination on the grounds of ideological or religious reasons or disabilities as they aren’t applicable criteria to the system.

The privilege of the person against self-incrimination is assessed in the scheme as it discriminates between images which are not required for the purpose(s) for which the equipment is being used (in this case the images will not be retained for longer than is necessary) and images which may need to be retained for longer periods as a requirement of an investigation into crime (in this case, while images are retained access to and security of the images will be controlled in accordance with the requirements of the Data Protection Act) (clause 9.0. Recorded material management). If images are retained for evidential purposes, they will be retained in a secure place where access is controlled (clause 9.1.4). Video prints are regarded as an exceptional element (clause 9.7) and are subjected to rigorous conditions (for example, video Prints requested by police must be on written authority of an officer of the rank of Inspector or above or all video prints will remain the property of the scheme owner and those not handed to the police will be retained in a secure cabinet until destruction is authorized).

Besides, the disclosure policy included in the Code imposes that disclosure of data obtained by the CCTV System will only be committed in accordance with the relevant legislation and the criteria contained within the Code of Practice and, in every case, a written application in an approved format, clearly showing the reasons for the request is required (Appendix C). The Code also lists third parties from who requests to view data will be regarded as ‘primary requests’ and sets out circumstances in which such applications may be made. Third parties include: the Police; Fire Service; H.M. Customs & Excise; Warwick District Council (Specific Officers); other statutory prosecuting bodies (e.g. Trading Standards, Ministry of Defence Police; British Transport Police; etc.); solicitors; plaintiffs/defendants and persons exercising their rights of subject access under the Data Protection Act 1998.

Finally, a caution is established in the scheme before data is viewed by a third party as the manager should be satisfied that data is the subject of a complaint or dispute that is unanswered, the original data and the audit trail is maintained throughout, not part of a current criminal investigation by the Police nor a civil proceeding or likely to be so, not removed or copied without proper authority and the image obtained is aimed at identifying individuals or information relating to an individual (clause 8.2.2).

The freedom of unlawful detention is not a direct freedom affected by the system but an indirect provision can be found in clause 7.7 because the scheme establishes an alert to the police officers if the Automatic Number Plate recognition matches the number plate of a stolen car against sources such as the Police National Computer, DVLA and Customs and Excise databases.
Relating to the right to *due process and fair trial*, the policy of the Warwick Code of Practice is explicitly expressed in clause 4.6 (to assist statutory prosecuting bodies such as the Police, and statutory authorities with powers to prosecute and facilitate the legitimate use of the information derived from the scheme). In this regard, the scheme allows revision of any audiovisual recording as, first, it imposes to maintain a record of all incidents in the incident log, including any information of note that may be used for investigative or evidential purposes (clause 7.2.2); second, the Code obliges to report incidents of criminal nature to the Warwickshire Police which is responsible to make the adequate response in accordance with their policies (clause 7.3).

The Cambridge City Council’s Public CCTV Scheme limits the *interference* on private life of the scrutinized by the cameras. Although there is inevitably some loss of privacy when CCTV cameras are installed, *cameras will not be used to monitor the progress of individuals in the ordinary course of lawful business in the areas under surveillance*. The cameras must only be used to view public areas and *not to look into the interior of any private premises* or any other area where an infringement of privacy of individuals may occur with few (legal or extreme situations) exceptions. The interference is required to be necessary and proportionate as individuals will only be monitored if there is reasonable cause to suspect that an offence has been or may be about to be committed (clause 1.2).

The processing of personal data is based on one of the criteria of art. 7 of the Data Protection Directive (public interest) which has consequences on the consent of data subject as it can be avoided. In any case, the scheme guarantees the detectability of the cameras in clause 1.3 (see above. Trust dimension).

The scheme deals with the exercise of the data subjects rights in a general way as it states that the showing of recorded material to the public will only be allowed “in accordance with the law” (clause 6.1). The showing can be assimilated to the right of access of individuals but an explicit of these rights is developed in clause 6.3 by a request under the Data Protection Act or the Freedom of Information Act although it is limited to a short period of time since data is only stored for a maximum of days. A restrict access to data is contemplated in the scheme: only authorized individuals (CCTV Staff, the Director of Environment, the Head of Specialist Services) have authorised routine access to the CCTV Control Centre. Any access for contractors, individuals or even police has to be limited to that strictly necessary for the work or specifically designated or authorized (clause 4.5 and 4.6).

Some remarks can be made on this issue. First, the scheme says that photographs should be seen only by individuals stipulated by the police. This provision is restrictive as subject data has to be allowed in any case to access to his/her data. Furthermore, the scheme does not reflect any consideration on the processing for sensitive personal data and the protection of such data must be a priority for a security system.

The scheme contains an evaluation process to test the success of the CCTV system. But this evaluation is not referred to the interference on data protection rights but on the “assessment on the impact on crime”. Undoubtedly, it will be positive to include the assessment on
freedoms and fundamental rights and not only on success in reducing crimes as the evaluation could show any deviation or abuse on public rights.

The Code of Practice for the Cambridge City Council affirms in the introduction that the CCTV System has been developed to allow all citizens and visitors, regardless of age, gender or race, the opportunity to participate fully and without fear in the life of the City. This general provision can be qualified as a non-discrimination principle of the security system.

Presumption of innocence is observed in the Cambridge CCTV Code of Practice under a general rule for any recorded materials: in case of they may need to be submitted as evidence in criminal proceedings and therefore must be of good quality, and be accurate in content. All such material will be treated in accordance with strictly defined procedures to provide continuity of evidence and to avoid contamination of the evidence (clause 6.1). Closely related to presumption of innocence is the privilege of the person against self-incrimination and the scheme guarantees this privilege by stating that images will only be released (to the Police and other enforcement agencies) to conduct investigations into potential criminal offences “in connection with law enforcement processes” (clause 1.4). Regarding the presumption of innocence, a provision is remarkably positive: Cambridge City Council will ensure that all requests for assistance from the Council’s CCTV system under this Act are examined in detail to ensure that they are proportionate, legal, appropriate and necessary. Where any doubts exist, legal advice or advice from the Surveillance Commissioner’s Office (address on last page of this document) will be sought before the Council agrees to undertake action under this Act.

With regard to the SAS Code, several of the criteria such as data protection and privacy are not applicable/relevant, as security of the scaffolding structure is reached by detectors and alarms which only operate with sound. With regard to due process and notification of the scrutinised, individuals are aware of the SAS in a standard grade SAS because it includes a Warning Device as mean of notification. The WD includes both audible and visual warning (although the audible warning may be suppressed with the agreement of the client, i.e. leaving only the visual warning device operational). In case of Enhanced grade SAS, it includes remote notification and it should be provided with an Alarm Transmission System to communicate conditions to a Remote Manned Centre or an Alarm Remote Centre and if required, the service provider’s duty personnel, a third party responding company personnel or the clients own staff. But, even in this case, an Enhanced SAS shall include, as a minimum at least one audible warning device. This caution will make persons aware of the system.

The NSAI Technical Annex, addresses the privacy and data protection criterion with a reference to the relevant legislation. Although the scheme certifies CCTV installers and CCTV systems process personal data and has the potential to interfere with privacy and other fundamental rights, does not contain specific requirements that address freedom infringement issues. The scope of the technical annex is rather limited. There is a reference to the general requirements of the normative documents PSA 2006_12 and IS. EN 50132 under the clause “Documentation”, which among others provides that the System Design Proposal includes supervised area details, legislation and other regulations. It can be assumed that the
“legislation” documentation might address the data protection and other issues, but this is not clear from the text of the Annex.

In terms of freedom infringement, the most applicable criteria we had to examine in the VdS guidelines for biometric recognition procedures in alarm systems were those related to Personal Data Protection. The biometric features captured, stored and processed constitute personal data. The *purpose limitation principle* is well satisfied by the scheme (identification/verification), along with the fact that they are adequate, relevant and not excessive for the purpose. However, the general clause “storage of templates” does not satisfy the criterion of fair and lawful process and it is also unclear for how long after the termination of the purpose the data are stored.

The PSA scheme on door supervision and security guarding includes separate *Risk Assessment Guidelines* in Annex, offering a detailed description of the process to be applied by Private Security Authority Licensed Contractors when undertaking a Risk Assessment as required by the relevant section of the scheme. In general, the security criteria are dealt in a satisfactory way, apart from accountability issues.

### 7.9 Key Findings of Legal Analysis of Schemes Operating in the EU

The analysis demonstrated how the existing schemes respond to the core legal requirements of STEFi dimensions. The following tables show the results by categorising the type of scheme as a variable, the type of security measure and the type of issuing body.

<table>
<thead>
<tr>
<th>Type of scheme</th>
<th>Security aspect</th>
<th>Trust aspect</th>
<th>Efficiency aspect</th>
<th>Freedom infringement aspect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification scheme</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔</td>
<td>✔</td>
<td>✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>Certification system (general requirements of schemes of the same body)</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔</td>
<td>✔</td>
<td>✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>Code of practice/conduct Guidelines</td>
<td>✔</td>
<td>✔ ✔ ✔ ✔</td>
<td>✔</td>
<td>✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>Technical specification</td>
<td>✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔</td>
<td>✔</td>
<td>✔ ✔ ✔ ✔</td>
</tr>
</tbody>
</table>

Table 7: Responsiveness of the existing schemes to the core legal requirements of the STEFi dimensions based on type of scheme
General certification rules and codes of practice have a good rate of addressing freedom infringement requirements in relation to certification schemes and technical specifications. However, they do not cover all the core requirements. Certification scheme rules might refer to the relevant legislation or to a standard that includes relevant principles. Usually, the general rules address the freedom infringement aspect with brief clauses. Public procurement calls and codes of practice are more comprehensive. Protection of rights and enhancement of trust is priority for such schemes that tend to focus on clauses on personal data protection, security and confidentiality of data and equal treatment in the examined cases. Trust and efficiency are not sufficiently covered in the existing schemes. The lack of specific legal framework regulating the different aspects of these dimensions, specifying minimum requirements is of relevance here. On the other hand, security is the mostly addressed dimension. Depending on the technology of the product or system and its capabilities, requirements to examine performance, reliability and function aspects of the measure are more or less intense. This is well illustrated with the example of the analysed technical specification of drones, which includes very detailed controls for security, exactly due to the technological and functional capabilities of the security component.

<table>
<thead>
<tr>
<th>Type of security measure</th>
<th>Security aspect</th>
<th>Trust Aspect</th>
<th>Efficiency aspect</th>
<th>Freedom infringement aspect</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
<td>✔ ✔</td>
</tr>
<tr>
<td>Alarm system</td>
<td>✔ ✔</td>
<td>✔</td>
<td>✔ ✔</td>
<td>✔</td>
</tr>
<tr>
<td>Drone</td>
<td>✔ ✔ ✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Table 8: Responsiveness of the existing schemes to the core legal requirements of the STEFi dimensions based on type of security measure

Even though the table is not representative of the whole range of security products, systems and services and the existing certifications, it provides an overview of the examined case studies and schemes in relation to the STEFi dimensions. Alarm systems are concerned with security and efficiency, whereas the trust and freedom infringement do not have intensive presence in the requirements of such security systems. Examined CCTV schemes distribute more equally the requirements among the four dimensions. The requirements of the STEFi aspects are not usually in one document. One should note that the outcome of the analysis here is also influenced by the high number of codes of practices that exist in the CCTV field, which as we saw earlier tend to focus on freedoms and rights. Finally, the examined drone scheme, provides very detailed requirements for security purposes, but does not address other issues regarding trust, efficiency and freedom infringement.
D4.1: Legal Analysis of Existing Schemes

<table>
<thead>
<tr>
<th>Type of issuing body</th>
<th>Security aspect</th>
<th>Trust aspect</th>
<th>Efficiency aspect</th>
<th>Freedom infringement aspect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public authority</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>Certification body</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>Standardisation body</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
<tr>
<td>Industry</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
<td>✔ ✔ ✔ ✔ ✔ ✔ ✔</td>
</tr>
</tbody>
</table>

Table 9: Responsiveness of the existing schemes to the core legal requirements of the STEFi dimensions based on issuing body

Public authorities either in procurement calls or in codes of practice/evaluation schemes show a tendency to include freedom infringement and trust aspect requirements. Data protection is at the spotlight, especially in the UK schemes, which include direct detailed provisions in the scheme itself or refer to the documentation and guidance of the UK Information Commissioner (ICO). Certification and standardisation bodies on the other hand include more technical requirements relating to the function of the security PSS and the safety. To a lesser extent, minimum efficiency requirements, appear, without however covering sufficiently the efficient aspect. Important requirements which address the relation of the cost to the performance and the investments are not examined in the framework of such schemes. Industry guidance documents and best practices also prioritise the security aspect. Trust scores low in such schemes.

The key findings of the analysis can be summarised as follows:

- Security is the most common focus of the certification schemes. Technical requirements on the proper functioning of the systems and/or the components are the main objective certification schemes of security products.
- The socio-legal dimensions of trust and freedom infringements are in most of the schemes not addressed. When a scheme addressed however these two of the STEFi dimensions, the most prominent element is safety of individuals and data security.
- Codes of practice, either by industry or by public authorities tend more often to include requirements to safeguard freedoms and rights and enhance trust on the security measures.
- The scope of the certification and evaluation schemes varies significantly in terms of what is certified and for which part of the process. Schemes with a very limited scope, such as the NSAI scheme for certification of CCTV installers, address only one part of the CCTV system process and operation.
- Lack of availability or accessibility of the documentation of the schemes influences transparency and trust to the scheme, and possibly to the certified or evaluated security measure.
• *Technical standards* are the main normative reference of the evaluation and certification schemes for security products, systems and services; the requirements of the standards form the basis of the auditing and evaluation rules. In the examined case studies there is a set of European standards that are the fundament for the majority of the schemes. A prominent example is the EN 50132 standard.

• The fact that schemes might not always be stand-alone documents, but they are often complemented by other documentation (such as guidance, general rules, other scheme rules etc.) has an impact on the comprehensiveness of the requirements they test. For instance, examination of data security of a biometrics access control alarm system, when the requirements are distributed in several documents does not facilitate neither the control by the auditor nor the confidence of the end user and the scrutinised on the security measure.

• *Accountability* issues are not particularly addressed rendering the allocation of responsibilities difficult.

• Taking into account that already different types of schemes include minimum requirements on STEFi aspects, one scheme that encompasses the STEFi dimensions can be feasible in that respect.
8 CONCLUSIONS

This Report is the one of the deliverables for Work Package 4 (WP4) “Analysis of core dimensions, security, trust, efficiency and freedom infringements (STEFi)” of security products, systems and services (PSS). The Work Package aims to analyse existing schemes and standards to identify evaluation criteria based on the four core dimensions and come up with requirements for further development, enhancement, adaptation and integration of evaluation and certification schemes of products used for security purposes. The Work Package also aims to identify and analyse core issues associated with certification.

The Legal Analysis of Existing Schemes Report aims to analyse the core issues of each of the STEFi dimensions and determine special requirements and legal demands for the security PSS. The aim is achieved through a multi-level analysis, starting from the normative framework of evaluation and certification schemes, examining the core STEFi aspects of security products, systems and services in terms of legislation and implications and assessing the responsiveness of the existing schemes to the legal requirements and demands.

The analysis of the normative framework of evaluation and certification schemes revealed there is no specific regulation for evaluation and certification schemes at EU level. The Regulations and Directives of the New Approach and the New Legislative Framework refer mainly to standardisation. International standards of the ISO adopted by the European Standardisation Organisations and guidance documents by such organisations and bodies form the framework of best practices and “soft law” for certification in the EU. The soft law refers both to core issues, such as the content and management of a certification scheme, and the actual best practices or the issues that stakeholders encounter and suggest solutions, based on the accumulated experience of the experts involved. The flexibility in the existing framework might be a deterrent factor for the development of pan-European schemes, which would have to comply with the legislation and rules of each Member State. On the other hand, too specific provisions could have a negative impact on the free market of certification, by imposing too many legal obstacles, especially to small certification bodies, operating locally.

Focusing on the legal analysis of the STEFi dimensions, the legislation in the EU relating to security is sector-specific, designed to address the specificities of each field of security. Notwithstanding the significance of such approach into highlighting the unique characteristics and demands of each area of security in the European Union, there are basic aspects of security, which one encounters in the majority of the laws, that would benefit from a centralized approach. The shared competences of the EU with the Member States are a constraint in that respect towards a centralized holistic approach and to the extent the Commission can make legislative proposals to that end.

Performance of the security equipment either relating to quality of images (captured by security cameras), detection of failure, independent functioning of the security PSS or others, is also a requirement identified in the majority of the legal acts. The safety and security of the
scrutinized and the operator of the security equipment is also a substantial requirement. In order to facilitate that requirement, risk and security assessments, proper training and certification of the operators is often required by the legislation.

For the aim of CRISP, the analysis of the key legislation of the security areas at EU level, revealed important legal demands at high principle level, mainly demonstrating the direction that CRISP should focus in terms of security. Physical controls such as patrols, screening of persons and items, but also protection against digital threats such as unlawful interference in systems and databases, hold a central role in the priorities of the legislator.

The trust of the scrutinised and end users to the security measures is crucial. In the relevant chapter for trust we examined the trust aspect from a legal perspective and also from a viewpoint of actual needs and perceived threats of consumers and scrutinized individuals.

The actual safety, reliability and maintenance of the security measure are distinct requirements influencing the confidence to the measure. A measure that might harm the health of the scrutinized, thus is not safe, will not be trustworthy, even though it might serve its purpose to satisfy the security needs. Together with other requirements, transparency of information and detectability of the security measure is also crucial. Covered surveillance performed with hidden CCTV systems stands among the factors that have negative impact on trust. Finally, respect for the legislation, implementation of standards, good practices and ethical codes also play a substantial role in building confidence to the security measure.

The trust study also draws significant lessons for the further work of CRISP in relation to the role of the evaluation and certification schemes in addressing the lack of confidence to the security measures. Among others, accountability, transparency, data protection by design, Privacy and Data Protection Impact Assessments, involvement of the stakeholders and regular review of compliance mechanisms are key trust elements for an evaluation or certification scheme for security products, systems or services.

Looking at the efficiency from a legal perspective, through the legislation and the case studies on drones, CCTV systems for crime prevention and detention and biometric intruder and access control alarm systems, the relevant chapter stresses the importance of efficiency criteria and requirements such as the minimum performance requirements, the cost-optimal investments etc.

The last of the STEFi aspects, the freedom infringement aspect, stressed the risks that the different security measures and the technologies they employ pose to the freedoms and fundamental rights of the individuals. As the Fundamental Rights Agency recently highlighted there is a need to include the fundamental rights in the security agenda, which would limit “the potentially adverse effects of security measures on the rights of individuals and reduce the risk of alienating entire communities by measures that could be perceived as discriminatory”\textsuperscript{360}. The legal study in this report also identified the core requirements for the protection of those rights in the context of security measures. The case studies of the WP

\textsuperscript{360} Fundamental Rights Agency, Embedding fundamental rights in the security agenda, 01/2015
provided useful insight on the specific risks of these technologies on privacy and data protection, such as imminent surveillance and panoptic effect, profiling, security of central databases, interference with systems and data risks and others. Different technologies employed in the various security measures differ in terms of impact on the freedoms and human rights of the individuals and accordingly in the levels of acceptance from the individuals. The acceptance is strongly connected to the potential of freedom infringement: the higher the intrusiveness and potential violation of a freedom or a human right the lower the acceptance from the individual. The level of intrusiveness might depend on factors such as the potential misuse of the capabilities of the security measure, or the capabilities themselves e.g. limitation of physical movement of the scrutinised, exposure of the nakedness, collection of sensitive information and others.

Further, the Report examined to what extent the existing evaluation and certification schemes respond to the requirements identified in the legal studies of the previous chapters. Drawing lessons from the analysis of existing schemes, the type of entity operating the scheme and the type of the scheme (certification scheme, certification system, code of practice, technical specification) play a crucial role into determining the quantitative and qualitative incorporation of the STEFi requirements identified in the legal studies. Public authorities tend to prioritise trust and freedom infringement requirements, while certification and standardisation bodies, as well as the industry focus on security and safety requirements.

To conclude with, the impact of the STEFi dimensions to the function and performance, user acceptability and legal compliance of the security PSS and the difficulty to locate a scheme with a comprehensive approach to the core aspects of all the four dimensions, highlight the importance of the CRISP objective to develop an innovative evaluation methodology that integrates the security, trust, efficiency and freedom infringement assessment dimensions.
9 REFERENCES

LITERATURE, ARTICLES, PAPERS

- Albrecht Astrid, “Understanding the issues behind user acceptance”, Biometric Technology Today, Volume 9, Issue 1, 1 January 2001, pp. 7–8
- Caponetti, L., "European Union’s WMD Non-proliferation policy: the competence-sharing between EU institutions", February 2014


- Neyland Daniel, “Parasitic Accountability”, Organisation, 19(6), 2012, pp. 845-863. ISSN 1350-5084

- Norris Clive, “From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control” in David Lyon (ed.), Surveillance as Social Sorting, Privacy, risk and digital discrimination, Routledge, 2003, p. 249f


- Pecoraro, Y., “Can drones break into the commercial market?”, Portolano Cavallo Studio Legale, 3 April 2014


• Welsh Brandon C. and D. P. Farrington, "Effects of Closed Circuit Television Surveillance on Crime", Campbell Systematic Reviews, n° 17, December 2008


**POLICY PAPERS, OPINIONS AND COMMUNICATIONS – EU and Member States**


• Article 29 Data Protection Working Party, Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation”, 13.05.2013,

Article 29 Data Protection Working Party, Working Document on Biometrics, WP80, 1.08.2003


Committee on Civil Liberties, Justice and Home Affairs of the European Parliament, A Review the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe, April 2009

ENISA, Privacy and Data Protection by Design – from policy to engineering, December 2014


European Commission, Delivering an area of freedom, security and justice for Europe’s citizens. Action Plan Implementing the Stockholm Programme, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM 2010 (171) final, Brussels, 29.04.2010

European Commission, DG Enterprise and Industry, CERTIF 2012-04 REV4 – The legal personality of accredited bodies – the case of natural persons, April 2014


- European Data Protection Supervisor, Opinion on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP), July 2013
- Fundamental Rights Agency, Embedding fundamental rights in the security agenda, 01/2015
- Joint Declaration by CoESS and UNI-Europa, Towards a European Model of Private Security, Madrid, 14 & 15, October 2004
- Information Commissioner’s Office, In the picture; A data protection code of practice for surveillance cameras and personal information, v. 1, 15 October 2015


**PROJECT REPORTS**

- Burgess Peter, Kloza Dariusz, *Identification of practices and procedures of compliance for the use of video surveillance archives*, Deliverable D2.3. for the ADVISE project, v. 3.4.
- Burgess Peter, Kloza Dariusz, *Monitoring Reports on emerging ethical challenges in the developing and implementing the video archives*, Deliverable D2.4. for the ADVISE project, November 2013
- Norwegian Board of Technology, Overview of Security Technologies v 1.1, PRISE Project, Deliverable D 2.2, April 2006
- Migliorini Massimo, Sabbatelli Roberta, Ricauda Sabrina, Flore Enrico, Ijaz Faheem, *Deliverable 10.3. Checklist of attitudes mapped with the freedom infringement dimensions*, D.10.3. for SIAM project, 16 September 2013
- Norwegian Board of Technology, *Overview of Security Technologies* v 1.1, PRISE Project, Deliverable D 2.2, April 2006
D4.1: Legal Analysis of Existing Schemes  

CRISP project


- SIAM Project, State of the art report on SMT impact on the global security level Deliverable, D3.5.

LEGISLATION & PROPOSALS FOR LEGISLATION

- Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security, OJ 5/1, 5.3.2010


- Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security

- Commission Regulation No 781/2005 of 24 May 2005 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security


- Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms


- European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02
- European Parliament and the Council, Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of Eurodac for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast), OJ L 180/1, 29.6.2013


CASE LAW

- Court of Justice of the European Union, case of Digital Rights Ireland and Seitlinger and Others, Joined Cases C293/12 and C594/12
- Court of Justice of the European Union, Case C-212/13 Ryneš v. Úřad pro ochranuosobníchúdajů, 11 December 2014
- Court of Justice of the European Union, Joined cases C-293/12 and C-594/12 - Digital Rights Ireland, Seitlinger and Others, 8. April 2014
- Court of Justice of the European Union, case of Schwarz v. Stadt Bochum, C-291/12, 17 October 2013
- Court of Justice of European Union, joined cases of C-141/12 and C-372/12 - YS and Others, 17 July 2014.
- Court of Justice of European Union, case of Bodil Lindqvist, C-101, 6 November 2003.
- European Court of Human Rights, case of D.H. and Others v. the Czech Republic [GC] (No. 57325/00), 13 November 2007
- European Court of Human Rights, case of Opuz v. Turkey (No. 33401/02), 9 June 2009
- European Court of Human Rights, case of Zarb Adami v. Malta (No. 17209/02), 20 June 2006
- European Court of Human Rights, case of Medvedev and Others vs France, 29 March 2010
- European Court of Human Rights case of Ladent vs the United Kingdom, 18 March 2008
- European Court of Human Rights, case of Storck v. Germany, 16 June 2005
- European Court of Human Rights, case of Brega and Others v. Moldova, 24 January 2012
- European Court of Human Rights, case of McVeigh and Others vs the United Kingdom, 18 March 1981
- European Court of Human Rights case of Sarigiannis vs Italy, 5 April 2012
- European Court of Human Rights case of Foka vs Turkey, 24 June 2008
- European Court of Human Rights case Ostendorf vs Germany, 7 March 2013
- European Court of Human Rights, case of James, Wells
- European Court of Human Rights case of Lee vs the United Kingdom, 18 September 2012 and case Saadi vs the United Kingdom, 11 July 2006
- European Court of Human Rights, case of Peck v. the United Kingdom, judgment of 28 January 2003
- European Court of Human Rights, case of Gäfgen v. Germany and case Jalloh vs Germany, 1 June 2010.
- European Court of Human Rights, case of Brogan and others v. the United Kingdom, 29 November 1988;
- European Court of Human Rights, case of *Kostovski v. the Netherlands*, of 20 November 1989
- European Court of Human Rights, case of *MM v United Kingdom*, No. 24029/07, 13 November 2012
- European Court of Human Rights, case of *Khelili v Switzerland*, 18. 10. 2011
- European Court of Human Rights, case of *Klass and others v Germany*, 6. 9. 1978
- European Court of Human Rights, case of *Leander v Sweden*, 26. 3. 1987
- European Court of Human Rights, case of *Huvig v France*, 24. 4. 1990
- European Court of Human Rights, case of *Z v Finland*, 25. 2. 1997
- European Court of Human Rights, case of *K & T v Finland*, 12. 7. 2001

**STANDARDS AND DOCUMENTS FROM STANDARDISATION ORGANISATIONS**

- CEN/CENELEC/PT, “Guidance for the application of conformity assessment to accessibility requirements for public procurement of ICT products and services in Europe,” August 2012
- ETSI TS 101 456 (v1.4.3) technical specification “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
- ETSI TS 102 042 (v2.3.1) technical specification “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”.

**SCHEMES AND RELEVANT DOCUMENTS**

- JARUS, Press release for a JARUS Information and Dissemination Workshop, 20 May 2014
- PSA Licensing Requirements - Door Supervision and Security Guarding
  - PSA 31:2014 Phase 1 Requirements for the licensing of Door Supervisor (Event Security), Door Supervisor (Licensed Premises), Security Guard (Event Security) and Security Guard (Static) Contractors, November 2014,

• Warwick District Council Code of Practice for CCTV Scheme (BS 7958, BS 7858), April 2008, http://www.warwickdc.gov.uk/info/20109/crime_and_law_enforcement/112/cctv
• Community-Based CCTV Scheme of the Irish Department of Justice, Equality and Law Reform (procurement call), http://www.justice.ie/en/JELR/Pages/Community_CCTV
  o Community-based CCTV Scheme – Guidelines for application and appraisal process
  o Code of Practice for Community-based CCTV Systems Authorised under Section 38 (3)(C), Garda Síochána Act 2005
  o Technical Specification for Community-based CCTV Systems Section 38 (3)(C), Garda Síochána Act 2005