Dogana

ADVANCED SOCIAL ENGINEERING AND VULNERABILITY ASSESMENT FRAMEWORK

D5.1 Legal and ethical challenges

Work Package:	5
Lead partner:	KUL
Author(s):	Stephanie Mihail (KUL), Yung Shin Van Der Sype (KUL), Angelo Consoli (SUPSI), Anton Vedder (KUL)
Submission date:	March 2016
Version number:	1.0 Status: Final

Grant Agreement N°:	653618
Project Acronym:	DOGANA
Project Title:	Advanced Social Engineering and Vulnerability Assessment Framework
Call identifier:	H2020-DS-06-2014-1
Instrument:	IA
Thematic Priority:	Trustworthy ICT
Start date of the project:	September 1st, 2015
Duration:	36 months

Dissemination Level	
PU: Public	✓
PP: Restricted to other programme participants (including the Commission)	
RE: Restricted to a group specified by the consortium (including the Commission)	
CO: Confidential, only for members of the consortium (including the Commission)	

Horizon 2020 European Union Funding for Research & Innovation

Project co-funded by the European Commission under the Horizon 2020 Programme.

Revision History

Revision	Date	Who	Description
D5.1 version 0.1	28/01/2016	Yung Shin Van Der Sype & Anton Vedder (KUL)	Input in sections 2 and 3
D5.1 version 0.1	26/02/2016	Angelo Consoli (SUPSI)	Input in sections 4.1.2 - 4.1.4 "Security by design" and "Data Handling"
D5.1 version 0.2	15/03/2016	Yung Shin Van Der Sype (KUL)	Editorial review (consistency of references etc.), addition of Danish data protection legislation and pertinent case law
D5.1 version 1.0	30/03/2016	Stephanie Mihail (KUL), Angelo Consoli (SUPSI), Yung Shin Van Der Sype (KUL)	Integration internal review comments

Quality Control

Role	Date	Who	Approved/Comment
Review Partner	26/03/2016	CNIT	Approved
Review Partner	x/03/2016	DBI	Approved

Disclaimer:

Contents

Definitions and acronyms

CC	CyberConnector: internal knowledge collaboration site and social network that is used to share all the information among partners.
CJEU	Court of Justice of the European Union
DOW	Description of Work
DPA	Data Protection Authority
DPD	Data Protection Directive (95/46/EC)
ECHR	European Convention for the protection of human rights and fundamental freedoms
ECtHR	European Court of Human Rights
GDPR	General Data Protection Regulation Proposal
MST	Management and Support Team
PbD	Privacy by Design
PC	Project Coordinator
SbD	Security by Design
SC	Scientific Coordinator
SDVA	Social Driven Vulnerability Assessment

1. INTRODUCTION

1.1. The Dogana project

One of the major threats that companies are facing in terms of security nowadays is the phenomenon of social engineering attacks. Careless behaviour of employees creates considerable vulnerabilities for companies.[1] Despite the attempts of many companies to highly secure their resources, security incidents still occur, since the employees have been generally considered as the prime weakness for company security. Employees "can initiate great harm to the confidentiality, integrity or availability of the information system through deliberate activities (disgruntled employee or espionage) or they may introduce risk via passive non-compliance with security policies, poor training or lack of motivation"[2]. In response to this problem, Dogana will provide an effective solution, by developing a framework that delivers an Advanced Social Engineering and Vulnerability Assessment. The conceptual basis for Dogana's framework is that Social Driven Vulnerability Assessments (SDVAs) help deploy effective mitigation strategies and lead to reducing the risks created by social engineering attacks.

Social engineering is "the art of exploiting the weakest link of information security systems"[3]. In terms of the Dogana project, the weakest link refers to the employees of companies. Social engineering, operating on the basis of gathering information of potential targets via several tools, such as email phishing, psychological profiling or memetics and the techniques of humans' manipulation, represents a really serious threat to companies. The risks for companies having employees sharing too much information or simply having bad online habits are considerable.[4] Taking into account that mainstream entities have been demonstrated to be incredibly weak against social engineering based attacks and they can be launched even by a single attacker, while current awareness programs and classical protection technologies are inefficient, the consequences for companies can be catastrophic and therefore, an efficient solution is required.

Current Social Vulnerability Assessments only supply companies with an analysis of several identified weaknesses, by providing a list of assets, susceptible to cause potential vulnerabilities. This method has been proven insufficient in practice, since patching security holes is not (only) a technological matter, but mostly a matter of changing the employees' behaviour. The novelty of the Dogana project is that, unlike the currently used methods, Dogana will instead, include social engineering based attacks in the assessment process. Moreover, Dogana aims to consolidate existing heterogeneous tools and merge the technical aspects and the legal and organisational procedures with the social vulnerability verification processes. The innovative feature of Dogana lies to the fact that, to date,

[1] "Successful phishing attacks can have serious direct consequences, such as financial loss if a phisher obtains access to a bank account, and indirect consequences, such as damaged reputation" in L. Tam, M. Glassman, M. Vandenwauver, "The psychology of password management: a trade-off between security and convenience", Behav. Inf. Technol., 2010, 233–244 and "Despite considerable research to better understand and protect against phishing attacks, they still pose a significant threat, and their frequency continues to increase" in S. Furnell, Still on the hook: the persistent problem of phishing, 2013, 7–12 and R. Gowtham, I. Krishnamurthi, A comprehensive and efficacious architecture for detecting phishing webpages, Comput. Secur. 2014, 23–37.

[2] M. Warkentin, and R. Willison, Behavioral and policy issues in information security systems: the insider threat, European Journal of Information Systems, 2009, 90-101.

[3] M. Huber, S. Kowalski, M. Nohlberg and S. Tjoa, Towards Automating Social Engineering Using Social Networking Sites, International Conference on Computational Science and Engineering, 2009, 1-8.

[4] B. Schneier, The Human side of Heart Bleed, The Mark News, 2014, https://www.schneier.com/blog/archives/2014/06/the_human_side_.html.

nothing similar has been attempted and that Dogana's ultimate purpose is not only to deliver strategic innovations, but to pave the way for introducing this innovation to the market.

Dogana will provide companies with a risk management framework, in order to assess their exposure and weaknesses and to consequently, adopt secure countermeasures. This goal will be achieved by the creation of a tool chain to perform assessments, alongside with a framework to perform trainings for employees, based on the EU legal framework, addressing information trustworthy topics and ethical questions in a holistic approach. The Dogana platform will be based on three pillars, namely, the pillars of (a) risk assessment, through an integrated framework for Social Vulnerability Assessments (identification/analysis/evaluation of risks), (b) risk mitigation, through innovative awareness methods, and (c) risk acceptance, through an extensive set of field trials with end-users. In order to achieve the above mentioned goals, Dogana will perform user-studies and trials.

Having outlined the innovative features of Dogana, it is important to note that, due to its nature, the execution of an SDVA is a very delicate process. For this reason, Dogana must be in accordance with legal and ethical rules, while simultaneously, appearing as close as possible to a real attack. By this method, the vulnerabilities of companies, introduced by their employees will be efficiently assessed and will consequently, lead to an effective solution for the company. One of the main legal implications for the Dogana project is for instance, during the research concerning human participants, how to respect the legal obligation of providing employees with prior consent, since it inserts a bias in the testing process and can alter the test results[5]. Compliance with legal and ethical requirements is crucial in the development of the Dogana framework and therefore, guidance for the implementation is included in the workflow from within the early stages of the project. Thus, the ethical and legal considerations, as outlined hereinafter will not only be part of the research results, but they will also constitute an aspect to be assessed during the lifetime of the project.

1.2. Purpose of the deliverable in relation to the work package and in the project

In order to identify and tackle all potential legal and ethical obstacles, a separate work package, WP5. 'Legal and ethical foundations', was included in the work planning of Dogana. More specifically, this work package will deal with these challenges, by providing the consortium with a single point of contact for all ethical and legal issues that may arise during the Dogana project and by providing policy recommendations for law-makers and organisational policy-makers.

The present deliverable has the purpose to report the outcome of Task 5.1. and to provide a general description of the legal and ethical obstacles and challenges of the Dogana project. In particular, it will provide an overview of the legal and ethical issues that the consortium might encounter during the project provided from a practitioner's point of view. The output of this task will be further applied and specified from the different viewpoints of the relevant stakeholders in Dogana during the lifetime of the project.

The scope of this deliverable is thus twofold. Firstly, this deliverable will provide the basic legal and ethical framework covering all aspects and features of the Dogana project. Secondly, this deliverable will provide the basic legal and ethical framework, which will constitute the basis for a further detailed development in the future deliverables, as follows.

[5] P. Finn, The ethics of deception in research, Indiana University Press, 1995, 87–118.

In this respect, section 2 will provide the legal and ethical framework applicable to Dogana. Therefore, the relevant privacy and data protection provisions, as well as security, intellectual property and liability regulations will be outlined.

In section 3, the description of the ethical and legal challenges for conducting SDVAs in organisational settings will be provided. This section will serve as a basis for a further detailed analysis for D 5.3 'Legal and ethical conditions for cautious organisations'.

In section 4, the ethical and legal challenges regarding the set-up of the Dogana project will be described, with a particular focus on the concept of Privacy by Design. This section will provide the basis for an in depth analysis in D 5.2 'Legal requirements for Privacy by Design'.

Section 5 will describe the legal challenges for involving human participants in trials and testings for the Dogana project. This will constitute the starting point for creating guidelines for the partners, which will be the subject of D 5.4 'Legal and ethical aspects of the Dogana trials'.

Finally, section 6 will conclude the analysis of this deliverable, summarising the key elements provided.

2. LEGAL AND ETHICAL FRAMEWORK

2.1. Criteria to determine the relevant legal and ethical framework

The applicable legal and ethical framework of Dogana is determined by the following criteria. Firstly, since Dogana will be used by companies in the EU, the EU law must apply. As mentioned above, the main legal and ethical concerns in the Dogana project relate to the protection of privacy and personal data of individuals, both regarding performed research activities, as well as regarding the potential implementation of the results in the EU, such as the disclosure of employees' personal data due to email phishing attacks. Therefore, the analysis of the framework will be primarily based on the Treaty on the Functioning of the EU[6], the Charter of Fundamental Rights of the European Union[7], and Directive 95/46/EC on the protection of personal data[8]. Regarding the Charter of Fundamental Rights, it should be noted that it was originally only a political document, and became legally binding as EU primary law[9] with the coming into force of the Lisbon Treaty[10] on 1 December 2009.

Due to the obligations posed from the above mentioned instruments, the European Convention on Human Rights[11] (ECHR) of the Council of Europe is also of high importance, as well as Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[12] and Recommendation No. 89 (2) on the Protection of Personal Data used for Employment Purposes[13]. Regarding non-binding guidelines, it is of essence to refer to the ILO Guide of Practice on the Protection of Workers' Personal Data[14]. In addition, of particular relevance for the Dogana project are the following opinions issued by the Article 29 Working Group, namely, Opinion 8/2001 on the processing

[6] Article 16.1.of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2010, C 83/01.

[7] Charter of fundamental rights of the European Union, 30 March 2010, C83/389.

[8] 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, further referred to as DP Directive or Data Protection Directive, 1995, c281/31.

[9] Charter of Fundamental rights of the European Union, 26 October 2012, C326/02.

[10] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 13 December 2007, C306/01.

[11] Convention of the Council of Europe of 4 November 1950 for the Protection of Human Rights and Fundamental Freedoms (ECHR), http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[12] Convention No. 108 of the Council of Europe of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[13] Recommendation No. (89) 2 of the Council of Europe on the protection of personal data used for employment purposes, adopted by the Committee of Ministers on 18 January 1989, further referred to as EU Charter, http://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf.

[14] The International Labour Office Code of Practice on protection of workers' personal data of 1997, http://www.ilo.org/wcmsp5/groups/public/@ed_protect/@protrav/@safework/documents/normativeinstrument/wcms_107797.pdf.

of personal data in the employment context[15], Opinion 15/2011 on the definition of consent[16], and Opinion 03/2013 on purpose limitation[17].

Moreover, taking into account that the EU law is implemented to the Member States by national laws, it is important to outline the national legislations applicable to Dogana. In particular importance for Dogana are the different existing labour legislations in the Member States. Also, since the trials and tests for the development of the Dogana project will be conducted in EU Member States, namely, in Italy, Austria, Romania, Denmark and Greece, the different national legal provisions must also be taken into consideration for the purposes of this analysis.

Regarding the ethical framework applicable to Dogana, the main potential issues relate to the intrusive nature of SDVAs and the involvement of human participants in the project research. In other words, the ethical questions relate to the nature of SDVAs, which will most likely interfere with the personal data and privacy of the employees. Therefore, during the trials, particular attention must be drawn to the requirement of informed consent of all participants, thus, taking into account the applicable national and European legislation. Finally, taking into account that Dogana is an EU project, funded by the Horizon 2020 Framework, as established by Regulation 1291/2013/EU[18], the rules for the participation and dissemination in Horizon 2020, as set out in Regulation 1290/2013/EU[19] must be taken into consideration. Additionally, the Opinions of the European Group on Ethics and other advisory boards should be considered, namely, Opinions No. 26 on Ethics of information and communication technologies, and No. 28 on Ethics of Security and Surveillance Technologies, which provide the basis for the development of the checklists mentioned in D1.3 'Compliance checklist', will be taken into consideration for the purposes of this analysis.

2.2. The legal framework

Taking into account the specific features of Dogana, the relevant legal provisions will be outlined under this section, serving as a basis for the development of the project, as well as for further implementation in future deliverables. Therefore, in order to decipher the key legal requirements, this section will provide the basic legal framework related to Dogana, namely privacy (2.2.1), data protection (2.2.2.), intellectual property (2.2.3), and liability (2.2.4) provisions.

[15] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf; and Article 29 Working Party, Working document on the surveillance of electronic communications in the workplace, adopted on 29 May 2002, WP55, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf.

[16] Article 29 Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, WP187, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[17] Article 29 Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP203, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[18] Regulation 1291/2013/EU of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No. 1982/2006/EC, OJ L 347/104, 20.12.2013.

[19] Regulation 1290/2013/EU of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Regulation No. 1906/2006, OJ L 347/81, 20.12.2013.

2.2.1. Right to respect for private life

As specified by the aims of the project, Dogana has a clear focus on privacy issues, relevant for the implementation of a legally compliant Dogana solution. More specifically, the legal requirements and considerations regarding Dogana mainly concern matters of privacy in the workplace. For achieving Dogana's purpose to increase company security, via social engineering tools, an interference with the employee's privacy rights is most likely. The right of the company to control its employees and to monitor employees' behaviour, among other things, for the purposes of company security has to be balanced with the rights of employees to respect for their private life[20]. Therefore, the right of the employer to exercise authority over his employees shall be restricted in accordance with the applicable legal framework on privacy. Before describing how to comply with these requirements, it is necessary to firstly refer to the basic key notions and principles relating to employee's privacy rights, as provided by legislation and case law.

Article 8 of the ECHR[21], states that everyone has the right to respect for his private life, his home and his correspondence. In terms of the Dogana project, where the interference of the employers with the private life of the employees will be possible, during the process of the vulnerability assessment, it must be examined whether workplace privacy falls under the protection of the ECHR. More specifically, we will examine whether this general right to respect one's private life, home and correspondence covers as well the aspects of one's professional life. The European Court of Human Rights (ECtHR) has interpreted the notion of private life very broadly,[22] in order to avoid the exclusion of too many intrusions from the scope of Article 8 of the ECHR, stating that this provision also applies in public spaces and that "there might be a zone of interaction of a person with others, even in a public space, which may fall within the scope of "private life"[23] and therefore, that such private life can also be found in the workplace.

From the case law, it is clear that Article 8 of the ECHR is also applicable in the area of control and surveillance in the workplace. Therefore, whenever issues relating to employees are raised, the following two questions must be answered, namely if there is an interference with one's right to respect for privacy and if there is a violation of Article 8 of the ECHR.

In order to answer the first question, whether or not an interference with one's right to privacy has occurred, the ECtHR uses the notion of "reasonable expectations" of privacy, meaning that the right to respect for one's private life, only extents to what the employee can reasonably expect, without however this being the only criterion.[24] Therefore, the definition of the notion of reasonable

[20] Protecting the right to respect for private and family life under the European Convention on Human Rights Council of Europe human rights handbooks, 2012, 56.

[21]European Convention of Human Rights (ECHR), as amended by the provisions of Protocol No. 14 (CETS no. 194), http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[22] For example, see: ECtHR 22 October 1981, No. 7525/76, Dudgeon v. the United Kingdom; ECtHR 15 May 1992, No. 15666/89, Kerkhoven and Hinke v. the Netherlands; ECtHR 16 December 1992 No. 13710/88, Niemietz v. Germany; ECtHR 25 March 1993, No. 13134/87, Costello-Roberts v. the United Kingdom; ECtHR 25 June 1997, No. 20605/92, Halford v. the United Kingdom.

[23] ECtHR 25 December 2001, No. 44787/98, P.G. and J.H. v. the United Kingdom, §56; ECtHR 28 April 2003, No. 44647/98, Peck v. the United Kingdom, §57.

[24] F. Dorssemont, K. Lörcher, I. Schömann, The European Convention on Human Rights and the Employment Relation, Bloomsbury Publishing, 2013, 482.

expectations of privacy[25], should be carried out on a case-by-case basis, since different situations, such as the worker's task or the place where he/she is working, are able to entail different privacy expectations and different protections. Moreover, the reasonable expectations of privacy in the workplace are crucially affected by the Organizational Security Policies, by which companies inform their employees about the fact that an interference with their private life might occur, under which specific circumstances such an interference might occur, and what the implications and the duration, of the interference might be. The level of privacy therefore granted to the employees remains under the discretion of the company. However, the companies' authority, as well as the content of their policies cannot be arbitrary nor unrestricted.

Whether the interference can be justified is analysed in the second step, which examines if and to what extent, companies are still allowed to take organizational or technical measures which might interfere with the private lives of their workers. In conclusion, an interference with the employees' private life can be justified in specific circumstances and under the condition that the restriction and the means used are in proportion with the objectives sought. In order for the interference to be justified, it must be"[...] In accordance with the law [...]", as required by the principle of legality and transparency. Thus, interferences must be based on a clear legal basis, providing sufficient, transparent and readily accessible procedures when invading individuals" right to respect for private life. Additional requirements for the interference to be justified, is that the interference with the right to respect for private life should pursue a legitimate aim and more specifically on the grounds of "[...] 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 and morals, or for the protection of the rights and freedoms of others [...]". Finally, in respect of the proportionality principle, the interference must be "[...] necessary in a democratic society [...]",meaning that it should be proportionate to the legitimate aim pursued and not any further than necessary, relevant and sufficient for achieving the legitimate purpose. Moreover, when alternative measures could reach the same goals, the least intrusive measure should be chosen over a more intrusive one. Therefore, the above mentioned principles could be displayed in the following six questions that should be answered for all interferences with the right to respect for privacy.

Table 1 'Proportionality test'

Is the interference in accordance with law?
Is that law foreseeable, accessible and specific?
Does the interference pursue a legitimate aim?
Is the interference necessary to achieve the aimed purpose?
Is there no other way to achieve the purpose?
Is it the least intrusive measure to achieve the purpose?

[25] Y.S. Van Der Sype, E. Frumento, and Z. Hodaie, "Legal Privacy and Data Security Requirements for the MUSES Platform", MUSES project, D7.1, 2013, 7.

Another milestone decision is the Niemietz case, where the ECtHR has held that "virtually all professional and business activities may involve, to a greater or lesser degree, matters that are confidential"[26] and that "respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world"[27]. In addition, in the Halford case, the ECtHR held that the interception of a worker's telephone calls at work violated the right to protection of private life, since all correspondence from the workplace falls within the scope of Article 8 of the ECHR.[28] Also, in the Copland case[29], the ECtHR restated its opinion on the wide scope of application of Article 8 of the ECHR in the workplace. More specifically, the ECtHR broadened the scope of privacy protection by including the Internet use and the electronic communication of workers, such as e-mails and related files attached thereto. The ECtHR held that it is only logical that "e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage".[30] The use of information relating to the date and length of telephone conversations and in particular the numbers dialed can give rise to an issue under Article 8, since "such information constitutes an integral element of the communications made by telephone"[31]. Accordingly, the ECtHR considered that "the collection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and Internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8"[32].

It is worth mentioning a prominent recent case of the ECtHR in this matter, which decided that an employer in Romania did not breach its employee's privacy rights by monitoring and reading the employee's instant messages.[33] The applicant, Bogdan Mihai Bărbulescu, is a Romanian national who lived in Bucharest and from 1 August 2004 until 6 August 2007, was employed by a private company as an engineer in charge of sales.[34] At his employer's request, he created a Yahoo Messenger account for the purpose of responding to clients' enquiries. On 13 July 2007, Mr. Bărbulescu was informed by his employer that his Yahoo Messenger communications had been monitored and that the records showed he had used the internet for personal purposes. Mr. Bărbulescu replied in writing that he had only used the service for professional purposes. He was presented with a transcript of his communication, including transcripts of messages he had exchanged with his brother and his fiancée relating to personal matters. On 1 August 2007, the employer terminated Mr. Bărbulescu's employment contract for breach of the company's internal regulations, which prohibited the use of

[26] ECtHR 16 December 1992, No. 13710/88, Niemietz v. Germany.

[27] ECtHR 16 December 1992, No. 13710/88, Niemietz v. Germany, §29.

[28] ECtHR 25 June 1997, No. 20605/92, Halford v. the United Kingdom.

[30] ECtHR 3 April 2007, No. 62617/00, Copland v. the United Kingdom.

[31] ECtHR 3 April 2007, No. 62617/00, Copland v. the United Kingdom, §43.

[32] ECtHR 3 April 2007, No. 62617/00, Copland v. the United Kingdom, §44.

[33] ECtHR 12 January 2016, No. 61496/08, Bărbulescu v. Romania.

[34] ECtHR, Press Release of the Registrar, 12 January 2016, http://www.statewatch.org/news/2016/jan/echr-workplace-surveillance-barbalescu-v-romania-prel.pdf, 1.

company resources for personal purposes. Mr. Bărbulescu challenged his employer's decision before the courts complaining that the decision to terminate his contract was null and void as his employer had violated his right to correspondence in accessing his communications in breach of the Constitution and Criminal Code. His complaint was dismissed on the grounds that the employer had complied with the dismissal proceedings provided for by the Labour Code and that Mr. Bărbulescu had been duly informed of the company's regulations. Mr. Bărbulescu appealed, claiming that e-mails were protected by Article 8 (right to respect for private and family life, the home and correspondence) of the ECHR and that the first-instance court had not allowed him to call witnesses to prove that his employer had not suffered as a result of his actions. In a final decision on 17 June 2008, the Court of Appeal dismissed his appeal and, relying on EU law, held that the employer's conduct had been reasonable and that the monitoring of Mr. Bărbulescu's communications had been the only method of establishing whether there had been a disciplinary breach. Furthermore, the Court of Appeal held that the evidence before the first-instance Court had been sufficient. Relying on Article 8 of the ECHR, Mr. Bărbulescu complained that his employer's decision to terminate his contract had been based on a breach of his privacy. Furthermore, relying on Article 6 §§ 1 and 3 (d) of the ECHR (right to a fair trial and right to obtain attendance and examination of witnesses), he complained that the proceedings before the domestic courts had been unfair.

The ECtHR considered that the fact that the employer had accessed Mr. Bărbulescu's professional Internet account and that the record of his communications had been used in the domestic litigation to prove the employer's case was sufficient to engage the applicant's "private life" and "correspondence". It therefore found that Article 8 was applicable. Firstly, however, it did not find it unreasonable that an employer would want to verify that employees were completing their professional tasks during working hours and noted that the employer had accessed Mr Bărbulescu's account in the belief that it contained client-related communications. Secondly, Mr. Bărbulescu had been able to raise his arguments related to the alleged breach of his private life and correspondence before the domestic courts and there was no mention in the ensuing decisions of the actual content of the communications. Notably, the domestic courts had used the transcript of his communications only to the extent that it proved that he had used the company's computer for his own private purposes during working hours and the identity of the people with whom he had communicated was not revealed. The ECtHR therefore concluded that the domestic courts had struck a fair balance between Mr. Bărbulescu's right to respect for his private life and correspondence under Article 8 and the interests of his employer. It particularly found that "[…] it is not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours." and "[…] the employer's monitoring was limited in scope and proportionate […]. There had therefore been no violation of Article 8 of the ECHR.

However, the judgment of the ECtHR must not be seen as "carte blanche" for employers to monitor their employees' communications at work. Employers should always bear in mind that the fact that the monitoring measure is not in breach of Article 8 of the ECHR does not automatically mean that such measure is indeed permitted at the end of the day. Further limitations, in particular under national, general and sector specific data protection, telecommunication and employment laws will apply and differ from jurisdiction to jurisdiction.

2.2.2. Data Protection

The Data Protection framework is relevant to the development of the Dogana project, as well as for the Dogana platform, which will operate on the basis of employees' personal data. Therefore, in this

sub-section the relevant legal provisions related to data protection on EU level will be examined. In particular, the requirements under the current Directive 95/46/EC, the key notions of data protection, the data protection principles, the rights of employees-as data subjects, as well as the recent legislative developments.

The current legal framework of data protection legislation in Europe

The text of reference, addressing all data protection issues on the EU level is 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 protection of personal data and on the free movement of such data,[35] hereafter referred to as the Data Protection Directive (DPD). The DPD was implemented by national laws in the EU Member States and is still valid, although the General Data Protection Regulation was adopted in December 2015[36] and will enter into force in 2018, will be directly applicable to all Member States, in the sense that no national laws will be required to implement the provisions. Further information about the recent developments in the data protection legislation will be provided below. In order to have a clear interpretation of the provisions of the Directive, the case law of the European Court of Justice, the opinions of the Article 29 Data Protection Working Party, the opinions of the European Data Protection Supervisor and the opinions of the national Data Protection Authorities have also been taken into consideration. While Directive 95/46/EC does not explicitly mention the monitoring of employees, however, the Article 29 Working Party has repeatedly stated that the EU data protection requirements, fully apply in this field.[37]

The Dogana project will operate on the employees' personal data and in order to apply the legal requirements of the Data Protection Directive, it is important to describe the key notions and principles related to data protection legislation.

2.2.2.1.1. Notions of the Data Protection Directive

The key concepts related to data protection legislation are the following.

- **Personal Data[38]:** Personal data are any information relating to an identified or identifiable natural person ('data subject'), which in terms of Dogana are the employees. This provision states also that 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

[35] 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. Currently this EU framework on data protection is under reform and the proposed General Data Protection Regulation should harmonize the national data protection laws of the EU Member States.

[36] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), 15 December 2015, Interinstitutional file 2012/0011.

[37] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 4; and Article 29 Working Party, Working document on the surveillance of electronic communications in the workplace, adopted on 29 May 2002, WP55, 7.

[38] Article 2 (a) of the Data Protection Directive.

physical, physiological, mental, economic, cultural or social identity, for example IP addresses[39], emails etc.[40]

- **Processing of Personal Data[41]:** Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration. The operating procedures of Dogana, such as the collection, use, storage etc. of the employees' personal data fall into this description.

- **Personal Data Filing System[42]:** Personal data filing system means any structured set of personal data, accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis. The personal data of the employees stored in the records and processed in the Dogana platform fall under this definition, as well as data files by the companies.

- **Controller and Processor[43]**: A controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data, while a processor is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

  In terms of Dogana, the companies will probably have the quality of controllers, since they determine the purpose and the means for the processing of their employees' personal data. The concept of controller contains three main building blocks.[44] Firstly, there is a personal aspect referring to 'the natural or legal person, public authority, agency or any other body'. Secondly, there is the possibility of pluralistic control, since the provision states 'alone or jointly with others', meaning that different actors can act as controllers.[45] Finally, the third element is that the controller determines 'the purposes and the means of the processing of personal data'. The processor's role depends on a decision taken by the controller. The controller decides either to process the personal data within his own organisation or to delegate all or part of the processing operations to one or more external natural or legal persons. If so, the processor can only act on behalf of the controller, meaning that he must implement the instructions given by the controller, at least with regard to the purpose of the processing and

[39] CJEU 24 November 2011, No. C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM).

[40] EDPS Comments on selected issues that arise from the IMCO Report on the review of Directive 2002/22/EC and Directive 2002/58/EC (ePrivacy), 2008, available at https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2008/08-09-02_Comments_ePrivacy_EN.pdf, 1-13.

[41] Article 2 (b) of the Data Protection Directive.

[42] Article 2 (c) of the Data Protection Directive.

[43] Article 2 (d) (e) of the Data Protection Directive.

[44] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, WP169, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf, 7 and 24.

[45] Article 29 WP, Opinion 1/2010, on the concepts of "controller" and "processor", adopted on 16 February 2010, WP169, 17.

the essential elements of the means.[46] The distinction and interaction between these two actors is very important, since it entails consequences relating to liability issues, which will be further developed below.

- **Third Party[47]:** A third party is any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data. For example, a data controller may decide to disclose to one of its employees (X) personal data relating to another of its employees (Y), for X to use as evidence in possible legal action (unconnected with X's employment). In this situation, X is not receiving the information in the course of his employment with the data controller, and will hence be a third party.[48]

- **Recipient[49]:** A recipient is a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not, with the exception of authorities which may receive data in the framework of a particular inquiry.

- **Consent[50]**: The data subject's consent must be a freely given, specific and informed indication of his wishes by which he/she agrees to personal data relating to him/her being processed. It should be noted that for the processing of non-sensitive data, consent must be given unambiguously, whether it is given explicit or implicit,[51] while for the processing of sensitive data, an explicit consent is required.[52] A specific difficulty rises on the employee consent, since where there is a clear imbalance between the data subject and the controller, consent should not provide a valid legal ground for the processing of personal data. The Article 29 Working Party "takes the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent"[53]. Reliance on consent should therefore be "confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment"[54]. The employer must therefore legitimise the processing of personal data of employees on other bases than the employee's consent and in

[46] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, WP169, 33 states that "the role of the processor may be limited to a very specific task or context or may accommodate a certain degree of discretion about how to serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means".

[47] Article 2 (f) of the Data Protection Directive.

[48] Information Commissioner's Office, "Key definitions of the Data Protection Act", https://ico.org.uk/for-organisations/guide-to-data-protection/key-definitions/, last visited on 14 March 2016.

[49] Article 2 (g) of the Data Protection Directive.

[50] Article 2 (h) of the Data Protection Directive.

[51] Article 7 (a) of the Data Protection Directive.

[52] Article 8 (2) (a) of the Data Protection Directive.

[53] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 23.

[54] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 3 and 23.

Dogana, the basis is the legitimate interest of the company to maintain an efficient security solution in the threat of social engineering attacks.

- **Sensitive personal data[55]:** This special category of data concerns data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life. The general rule is that the processing of sensitive personal data is prohibited.[56] The exception[57] to this rule is that sensitive data can be processed when this is necessary and based on one of the legal grounds set out in paragraph 2 of Article 8. Namely, where the data subject has given his explicit consent to the processing of those data or where processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law, in so far as it is authorized by national law or where processing is necessary to protect the vital interests of the data subject or of another person, where he/she is physically or legally incapable of giving consent. Also, where processing is carried out, in the course if its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body, or where the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims. Although the processing of sensitive personal data is not the aim of the monitoring measures that will be used in Dogana, it cannot be excluded that such monitoring actions may reveal sensitive personal data, such as sex, age or the organizational/social position and network characteristics of an employee.

2.2.2.1.2. Data Protection Principles

The data protection principles constitute the guidance for striking the right balance between the data protection of the employees and the protection of the company's security. It is important to clarify that the following principles apply to all applications, phases and procedures of the Dogana project.

- **The principle of lawfulness of the processing of personal data[58]:** Personal data must be processed fairly and lawfully, and therefore, any interference has to be based on a legal basis and defined in a legal document. In other words, personal data must be processed in a way that does not bring about a breach of either data protection laws or other legal requirements,[59] taking into account the specific structure of labour and employment law, since the regulation on the protection of employees is regulated through several international treaties, codes and practices and by European and European Union legislation, as well as on national, sectorial level and company level. Due to the excessive amount of labour and employment law among the EU Member States, an individualized discussion would exceed the scope of this deliverable,

[55] Article 8 of the Data Protection Directive.

[56] Article 8 (1) of the Data Protection Directive.

[57] Article 8 (2) of the Data Protection Directive.

[58] Article 6 (1) (a) of the Data Protection Directive.

[59] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 18.

however, the basic elements of the relevant country specific regulations will be outlined below.

- **The principle of data quality[60]:** In respect of this principle, personal data must be collected fairly and lawfully; for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, except for historical, statistical or scientific purposes, under the condition that appropriate safeguards are provided. Also, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; they must be accurate and kept up to date, otherwise, they should be erased or rectified. In addition, they must be kept in a form which permits identification of data subjects for no longer than is necessary. The controller is responsible for the compliance with these obligations.

- **The principle of purpose specification and limitation[61]:** This principle requires that personal data may only be collected for specified, explicit and legitimate purposes and that they shall not be processed in a way incompatible with those purposes. There are two main building blocks in this principle: firstly, personal data must be collected for "specified, explicit and legitimate" purposes (purpose specification), and secondly, these data must not be "further processed in a way incompatible" with those purposes (compatible use)".[62]

- **The principle of data accuracy[63]:** The employee's personal data must be accurate and kept up to date and the companies have to take every reasonable step to ensure that this requirement is met.[64]

- **The data retention principle[65]:** The records on worker behaviour "must be kept in a form which permits identification of workers for no longer than is necessary for the purposes for which the data were collected or for which they are further processed"[66].

- **The security principle[67]:** Personal data should be protected by providing and implementing security safeguards against risks, such as loss or unauthorised access, destruction, use, modification or disclosure of the data. The principle of security also encompasses the employer's right to protect his networks against these unauthorised accesses or attacks.[68]

[60] Article 6 of the Data Protection Directive.

[61] Article 6 (1) (b) of the Data Protection Directive.

[62] Article 29 Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, WP203, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 15, last visited on 11 March 2016.

[63] Article 6 (1) (d) of the Data Protection Directive.

[64] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 21.

[65] Article 6 (1) (e) of the Data Protection Directive.

[66] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 21.

[67] Article 17 (1) of the Data Protection Directive.

[68] Article 29 Working Party, Opinion 3/2010 on the principle of accountability, adopted on 13 July 2010, WP173, 8.

These measures must be appropriate with regard to the risks connected with the personal data processing, as well as with regard to the nature of the data collected. The necessary level of data security is ascertained by the state of the art in the given industry, in the sense that security measures need to be reviewed on a regular basis to ensure that they are up-to-date and effective, the costs of implementation, and the sensitivity of the data being processed. Also, the ISO/IEC 27000 series[69] standardisation must be considered, and in particular ISO/IEC 27001[70], which comprises information security standards and best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS). Although not binding, the standardisation is crucial for assuring the achievement of a minimum level of security safeguards.

The Dogana project will be developed in respect of this principle, since, as mentioned above, the employees, already having a foothold in the organization by being granted access to data, pose a major risk because they are difficult to detect and stop with traditional preventative controls. It should be noted that although achieving greater information security is essential, it may also be in conflict with the rationale behind the right to data protection and therefore, the major challenge is to balance the employees' right for privacy and the right of the employers to assure the company's security. Therefore, the processing of personal data in the context of surveillance activities, in the terms of the companies' right to assure the company security, may take place under adequate safeguards defined by law and in accordance with basic data protection principles governing the processing of personal data of employees, such as the principles of purpose limitation, data minimisation, transparency and employees empowerment (transparency principle).[71]

- **The principle of legitimacy of data processing[72]:** The meaning of this principle is that the processing of personal data should only take place when it is "necessary for" the "achievement of the objective in question rather than merely incidental to its achievement"[73]. This principle, which is referred in the GDPR as "data minimisation"[74], requires that only the personal data, which are necessary for achieving the purpose, should be processed. This entails that employers should always process the personal data of employees in the least intrusive way. Different elements are considered for this evaluation, such as the risks at stake, the amount of

[69] ISO/IEC 27000 series is published jointly by the International Organization for Standardisation (ISO) and the International Electro technical Commission (IEC). The series is broad in scope, covering more than just privacy, confidentiality and IT or technical security issues and is applicable to organizations of all shapes and sizes, since all organizations are encouraged to assess their information security risks, and then implement appropriate information security controls according to their needs, using the guidance and suggestions. ISMS incorporates continuous feedback and improvement activities, summarized by W.E. Deming's "plan-do-check-act" approach, that seek to address changes in threats, vulnerabilities or impacts of information security incidents.

[70] Certification to ISO/IEC 27001 is possible but not obligatory. ISO/IEC 27001 can be used to provide sector specific and/or service-specific certifications extended to include sector-specific or service-specific requirements that are related to the management of information security.
[71] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 4.

[72] Article 7 of the Data Protection Directive.

[73] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 15.

[74] Article 6 (1) (c) of the Data Protection Directive.

data involved, the purpose of processing, etc. In order to legally process the personal data of the employees, the processing must be based on at least one of the legal grounds as laid down in Article 7 of the Data Protection Directive. However, the ground on the employees' consent (personal data may be processed only if (a) the data subject has unambiguously given his consent) is highly questionable when it concerns employment relationships.[75] Therefore, the most probable legal ground for processing employees' data in terms of Dogana will be "when the processing is necessary for the purposes of the legitimate interests pursued by the controller"[76], where 'legitimate interest' would mean safeguarding the company's security.

2.2.2.1.3. Rights of the data subjects-employees

Data subjects, hence also the employees, have the right to information, the right of access and the right to object. As mentioned above, the controller has the obligation to provide for the following rights and is liable for not meeting this requirement.

- **Right to information[77]**: The employees must at least know which of their personal data is processed, by whom and why. Therefore, when personal data of the employees are collected, the controller must provide them with the following information, namely the identity of the controller or his representative, the purposes of the processing for which the data are intended, and any further information such as the recipients or categories of 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 them. Where the data have not been obtained from the data subject directly, which could be one of the cases applicable for Dogana, the controller or his representative must at the time of undertaking the recording of personal data provide the data subjects with at least the following information, namely the identity of the controller and of his representative, the purposes of the processing, and any further information such as the categories of data concerned, the recipients or categories of recipients, the existence of the right of access to and the right to rectify the data concerning them, in so far as such further information is necessary.[78]
- **Right of access[79]**: The employees have the right to access the personal data relating to them and if appropriate, they can request rectification, erasure or blocking, and they are entitled to object on compelling legitimate grounds. It is for the controller to assure that the exercise of their right without constraint or excessive delay and expense and to provide them with confirmation as to whether or not data relating to them are being processed, alongside with all the above mentioned information.

[75] Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 23.

[76] Article 7 (f) of the Data Protection Directive.

[77] Article 10 of the Data Protection Directive.

[78] Article 11 of the Data Protection Directive.

[79] Article 12 of the Data Protection Directive.

- **Right to object**[80]**:** The employees have the right to object at any time on compelling legitimate grounds relating to their particular situation to the processing of data relating to them. In the case of Dogana, the processing will be probably based on the legal grounds of Article 7 (f)-the legitimate interests of the controller. This provision guarantees the right of the employees to object to their personal data being processed.
- **Automated decision making**[81]: The general rule is that every person and in the case of Dogana, the employees, have the right not to be subject to decisions producing legal effects concerning or significantly affecting them, which are solely based on automated processing of their personal data and intended to evaluate certain personal aspects relating to them, such as their performance at work, creditworthiness, reliability, conduct, etc., such as a dismissal, which is referred in GDPR as 'profiling'[82]. There are two exceptions to this rule, therefore permitting their profiling, namely, if the decision was taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the employee, has been satisfied or that there are suitable measures to safeguard his/her legitimate interests, such as arrangements allowing him to put his points of view or it is prescribed by a law, under the condition that adequate safeguards for the employee's legitimate interests are in place.

Recent legislative developments

On 24 June 2015, the three main institutions of the EU, European Parliament, the Council and the European Commission entered into co-decision negotiations on the proposed General Data Protection Regulation (GDPR), a procedure known as 'trilogue'. The basis for the trilogue is the Commission's proposal of January 2012, the Parliament legislative resolution of 12 March 2014[83] and the General Approach of the Council adopted on 15 June 2015[84]. The three institutions are committed to dealing with the GDPR as part of the wider data protection reform package, which also includes the proposed directive for police and judicial activities. The process should be concluded by the end of 2015 and likely allow for formal adoption of both instruments in early 2016, to be followed by a two-year transitional period[85].

According to the latest version of the general approach, the key points of the agreement can be summarised as follows: Personal data must be collected and processed lawfully, under strict conditions and for a legitimate purpose. Data controllers must respect specific rules, such as the requirement for unambiguous consent by the data subjects. Also, the data subjects' rights are reinforced and data controllers' obligations are increased. For example, among other obligations, data controllers must be

[80] Article 14 of the Data Protection Directive.

[81] Article 15 of the Data Protection Directive.

[82] Article 9 of the GDPR.

[83] Parliament legislative resolution of 12 March 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN, amendment 13-Recital 34.

[84] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, GDPR), 15 December 2015, Interinstitutional file 2012/0011 (COD).

[85] European Commission, "Reform of EU data protection rules", http://ec.europa.eu/justice/data-protection/reform/index_en.htm.

more transparent about how personal data are handled, for instance, by informing individuals about their privacy policy in clear and plain language. In addition, controllers must implement appropriate technical and organisational measures and procedures to ensure that processing safeguards the rights of the data subject (by design) and that, by default, only the minimum and necessary personal data for each specific purpose is processed and it is not disclosed more widely than necessary.[86] The proposed implementation of accountability under Article 22 of the draft GDPR[87] would further enhance the Privacy by Design principle. Indeed, with the adoption of the proposal, operators will be required to implement policies and appropriate measures to ensure and to be able to demonstrate compliance with data protection rules. Moreover, data controllers will be responsible for implementing appropriate security measures and provide, without undue delay, notification of personal data breaches to the supervisory authority, as well as to those significantly affected by the breach.[88] Also, there is now a specific obligation on a controller or a processor to appoint a data protection officer[89], where its core processing activities require regular and systematic monitoring of individuals on a large scale, or where its core activities consist of the processing of sensitive data on a large scale. Taking into account the provisions for remedies and administrative fines the impact on companies is highly important, since accountability is increased the financial consequences of non-compliance can raise up to 1 million euros or 4% of their global annual turnover.[90]

Regarding the processing of personal data in the employment context, the Member States can provide by law or by collective agreements for more specific rules to ensure the protection of the rights and freedoms of their employees, in particular regarding the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.[91] Also, Member States may determine the conditions under which personal data of the employees may be processed on the basis of their consent.[92] Therefore, the area of employee data is 'excluded' from the EU wide 'one stop shop' mechanism, since it is specifically provided that each member state shall also be empowered to regulate in this area and thus, national legislation must be taken into consideration.

It is important to make some remarks about the new Article 82 of the General Data Protection Regulation and its impact on the data protection of the employees, since a lot of criticism regarding the sufficiency of this provision has been made. More specifically, it is important to remind that the aim of the General Data protection Regulation was to provide harmonization of the data protection laws across all 28 EU countries. EU member states would, though, have a margin of maneuver. In an

[86] Article 23 of the GDPR.

[87] Article 22 of the GDPR.

[88] Article 22 of the GDPR.

[89] Article 37 of the GDPR.

[90] Article 79 of the GDPR.

[91] Article 82 of the GDPR, in conjunction with Recital 124 of the GDPR.

[92] Recital 124 of the GDPR.

attempt to provide some minimum safeguards, the Employment and Social Affairs committee at the European Parliament had proposed amendments to the Commission's Article 82 plans,[93] proposing a number of 'minimum standards' for the processing of personal data in an employment context, which member states would have to abide by, when setting any specific data protection rules in the employment context.

However, a European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee commissioned study[94] questioned whether the Employment and Social Affairs committee proposals would actually work in practice. In this study, academics P. De Hert and H. Lammerant recommended that a new EU Directive should be drafted to set specific rules on data protection in an employment context. This recommendation is based on the following arguments, namely that "the proposed minimum standards contain rules on processing with and without the knowledge of the employee, video-surveillance, medical examinations, surveillance of telecommunications, prohibition of blacklists, rights of worker representatives, transfers of information".[95] The academics stated that "in other words, an attempt is made to turn this article into an extensive framework for data processing in employment context. On the other hand, the whole gives an incoherent and ad hoc impression. It is difficult to squeeze a coherent data protection framework into one paragraph with minimum standards. The Commission should be asked to substitute the minimum standards included in Article 82 with a coherent Directive on data protection in employment relations"[96].

In addition, it is worth mentioning the most recent Recommendation regulating this issue,[97] which is the updated text on the same subject dating back to 1989, a time when the Internet was only at its beginning. The updated text aims to address the challenges for privacy resulting from the use of new information and communication technologies. "This Recommendation, which applies both to the public and private sectors, provides that employers should avoid unjustifiable and unreasonable interference with employees´ right to private life in the workplace, this being applicable to all information technology devices. It contains a number of safeguards to ensure that employees´ personal data is adequately protected, and provides guidance on how employers should collect, store and communicate personal data externally, for example to public bodies. Employees should have access to the personal data employers hold on them, and to information about their origin and the

[93] Opinion of the Committee on Employment and Social Affairs for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 04 March 2013, Rapporteur: Nadja Hirsch.

[94] P. De Hert and H. Lammerant, Study, Protection of Personal Data in Work-related Relations, 2013, 1-77.

[95] P. De Hert and H. Lammerant, Study, Protection of Personal Data in Work-related Relations, 2013, on behalf of the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee, recommending that a new EU Directive should be drafted to set specific rules on data protection in an employment context, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/474440/IPOL-LIBE_ET(2013)474440_EN.pdf, 66.

[96] Study "Protection of Personal Data in Work-related Relations", 2013, Study of Paul De Hert and Hans Lammerant on behalf of the European Parliament's Civil Liberties, Justice and Home Affairs (LIBE) Committee, recommending that a new EU Directive should be drafted to set specific rules on data protection in an employment context, available at http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/474440/IPOL-LIBE_ET(2013)474440_EN.pdf, 69, last visited on 11 March 2016.

[97] Council of Europe Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment, adopted by the Committee of Ministers on 1 April 2015 at the 1224th meeting of the Ministers' Deputies.

purpose of their processing. They should also be entitled to have data rectified or erased if they are inaccurate or have been processed contrary to the law."[98]

In order to examine the country specific regulations related to Dogana, it is important to describe the concept of 'establishment' under the current legal framework, as well as in the light of future developments. In a recent decision,[99] the European Court of Justice (ECJ) determines how the term 'establishment' used in the EU Data Protection Directive 95/46/EC must be interpreted and thereby on the applicability of national data protection law in cases with a cross-border context, as well as the power of national data protection authorities in this regard and the practical implications. More specifically, the Court states in the concluding remarks that "Article 4(1)(a) of must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity in the context of which that processing is carried out. The following should be taken into account: (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned. By contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant"[100].

Also, in May 2014[101], the ECJ decided that an affiliate of a US search engine operator located in Spain qualified as an establishment in terms of the EU Data Protection Directive, although personal data was only processed by the US parent company. The Spanish affiliate qualified as establishment, because it provided advertising services to fund the parent company's services in Spain, thereby triggering the application of Spanish data protection law. This decision by the ECJ seems to say that it is no longer necessary for an establishment of a non-European data controller to be involved effectively and directly in the data processing activities in order to lead to the application of EU data protection law.[102]

Nevertheless, it should be emphasized that the consent is not the only ground for lawfulness. Regarding consent, if and when consent is necessary, the processing concerns personal data, consent must be unambiguous[103], whereas in the case of special categories of data, the consent must be

[98] Council of Europe website, http://www.coe.int/en/web/human-rights-rule-of-law/2015-news/-/asset_publisher/8X0wvBBc60he/content/council-of-europe-committee-of-ministers-has-adopted-a-recommendation-on-the-processing-of-personal-data-in-the-context-of-employment.

[99] ECJ 1 October 2015, C-230/14, Weltimmo v. Nemzeti Adatvédelmi és Információszabadság Hatóság.

[100] ECJ 1 October 2015, C-230/14, Weltimmo v. Nemzeti Adatvédelmi és Információszabadság Hatóság, § 66.

[101] ECJ 13 May 2014, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD).

[102] Relevant provisions can be found in Recitals 95a and 97, as well as in Articles 3, 4, and 49 of the GDPR.

[103] Article 7 (4) of the GDPR.

explicit[104]. Also, the employees should be able to withdraw their consent at any time, without this affecting the lawfulness of processing which was based on consent before its withdrawal and that prior to giving consent, the employees have to be informed. The above must be taken into account alongside the Recitals of the GDPR[105].

It is relevant to mention to this point that the legal ground for processing the employees' personal data in Dogana, is the following requirement provided in the GDPR[106], namely, that the processing of data is to be made to the extent strictly necessary for the purposes of ensuring network and information security. For instance, the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data, and the security of the related services offered by, or accessible via, these networks and systems, by public authorities, Computer Emergency Response Teams – CERTs, Computer Security Incident Response Teams – CSIRTs, providers of electronic communications networks and services and by providers of security technologies and services, which constitutes a legitimate interest of the data controller. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping "denial of service" attacks and damage to computer and electronic communication systems. This concerns mostly a reactive approach into achieving company's security by comparison to a proactive approach, such as Dogana, and this point is relevant to take into consideration for an overall approach of security mechanisms.

The provision regarding automated decision making[107] is also important for Dogana, since social engineering attacks are based on profiling techniques. The GDPR enlarges considerably the protection of data subjects, in respect of automated individual decisions based on profiling, which will cover also the use of data correlations to predict behavior, or to take decisions vis-à-vis targeted people. The proposed provision protects data subjects against measures that produce legal effects for them or significantly affect them, such as a dismissal etc., when these measures are based solely on automated processing. The human element is important to include when it is intended to evaluate certain personal aspects relating to natural person or to analyse or predict the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour[108].

2.2.3. Intellectual Property Rights

Having described the key elements of the legal framework relating to privacy and data protection, it is pertinent to this point to also refer to the legal framework relating to Intellectual Property (IP) rights. Firstly, the key legislative instruments on a European level will be outlined, and secondly, the issue of IP within the project will be provided.

[104] Article 9 (2) (a) of the GDPR.

[105] Recitals 25 (on unambiguous consent), 32 (about controller's obligation to demonstrate data subject's consent), 34 (about freely given consent) and 41 (about special categories of data) of the GDPR.

[106] Article 30 of the GDPR.

[107] Article 15 of the Data Protection Directive and Article 9 of the GDPR.

[108] ECtHR 12 January 2016, No. 61496/08, Bărbulescu v. Romania.

The general legal framework regarding IP rights

The legal framework regarding the IP rights in Europe is diverged and under constant updating, due to continuous technological developments.[109] In terms of the Dogana platform the most important provisions are included under the protection of software, which as a copyright subject was harmonized through the Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs,[110] and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, aiming to harmonise the legal framework on copyright and related rights and thereto foster the substantial investment in creativity and innovation, including network infrastructure. [111]

By these instruments, the main international obligations under the two treaties on copyright and related rights[112], adopted in 1996, within the framework of the World Intellectual Property Organisation (WIPO), were transposed on EU level. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of IP rights[113], as well as Decision No 1639/2006/EC of the European Parliament and of the Council of 24 October 2006, establishing a Competitiveness and Innovation Framework Programme (2007-2013)[114], which encourages the use of information technology.

Although the above mentioned instruments provide for the rights and obligations to be considered for the Dogana platform in an EU level, however, it is of importance to emphasise that in order to safeguard the IP rights of the Dogana solution, private agreements must be signed between the creators of the Dogana platform and the companies implementing Dogana.

IP rights of material developed during the project

As already stated in the introduction of this deliverable, Dogana is an innovative project, since, unlike the current used methods for vulnerability assessments, Dogana will instead, include social engineering based attacks into the assessment process. Therefore, the Dogana consortium follows principles related to open source, IP rights and patents and these aspects were addressed in the Consortium Agreement (CA)[115]. More specifically, these matters are dealt in detail in Articles 5.1 to 5.4 in Section 5 of the Consortium Agreement of 27 April 2015. IP will be protected by patents, if applicable,

[109] For more information, see also the European Commission's website, http://ec.europa.eu/internal_market/copyright/prot-comp-progs/index_en.htm.

[110] Directive 91/250/EEC on the legal protection of computer programs of 17 May 1991, OJ L 122, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31991L0250:EN:HTML.

[111] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L167, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0029.

[112]Council Decision of 16 March 2000, on the approval on behalf of the European Community of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l26054&from=EN.

[113] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l26057a&from=EN.

[114] Decision 1639/2006/EC of the European Parliament and of the Council of 24 October 2006 establishing a Competitiveness and Innovation Framework Programme (2007-2013), as amended by Regulation (EU) No. 670/2012 of 31 July 2012, OJ L 204, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:n26104&from=EN.

[115] Article 23 (a) on management of intellectual property of the Grant Agreement of 25 April 2015.

following the main applicable rules in the Rules for Participation and the model grant agreement for H2020 projects[116].

Management of technical knowledge within this project lies in the activities of WP1. 'Project Management'. For external knowledge management the project also relies heavily on WP8. 'Dissemination and exploitation', especially for dissemination on the project web site and in the standards communities.

2.2.4. Liability issues

The general rule for liability

The general term of liability refers to legal responsibility for one's acts or omissions[117]. Depending on the context, liability can have different meanings, however, the three determinant elements for the establishment of liability are damage resulting from an unlawful operation, causality and a certain degree of fault.[118] In other words, whenever an obligation for compliance with legislative or regulatory requirements is not met and there is a causational link between the act or omission and the damage caused due to this non-compliance, then liability issues arise. Therefore, different types of liabilities exist, according to the different types of requirements.

In terms of the Dogana platform, which deals with employees' actions and/or omissions, it is worth mentioning that the majority of the EU Member States have in place a general rule imposing strict liability on employers for the wrongdoings of their employees (e.g. vicarious liability in English law).[119] In other words, an employer will be held liable for any tort committed, while an employee is conducting his/her duties. This general rule is also the rationale behind the conception of Dogana, which aims to mitigate the employees' wrongdoings by increasing the companies' security solutions. Finally, regarding the liability of the partners involved in the Dogana project, this is provided by the Consortium Agreement[120].

Software liability

Another type of liability derives from the fact that the Dogana platform will also develop and include software. Therefore, it is important to outline some basic elements regarding to software liability issues. Apart from the cases of gross negligence and intentional acts, or a liability in tort, such as releasing malicious software, it is rather difficult to construe a contractual liability only based on the Free Open Source Software licensing.[121] In a typical software license there is no obligation to deliver,

[116] Rules for Participation and the model grant agreement for H2020 projects https://ec.europa.eu/research/participants/portal/desktop/en/funding/reference_docs.html.

[117] Legal Dictionary, http://dictionary.law.com/Default.aspx?selected=1151.

[118] Greenman v Yuba Power Products, Inc., 1963, 59 Cal.2d 57.

[119] Legal Information Institute, Cornell University Law School, https://www.law.cornell.edu/wex/vicarious_liability.

[120] Section 5 of the Consortium Agreement of 27 April 2015, §5.1 to 5.4.

[121] European Commission, Report on Open Source Licensing of software developed, 16 December 2004, http://ec.europa.eu/idabc/servlets/Docbcdd.pdf?id=24394, 22.

just conditions for use, since should a downstream recipient wish to integrate the software in a larger product for a particular purpose, and the software unfit to said purpose, it would be upon the integrator – who is permitted to make all the modifications needed, including the adaptations and quality assurance activities – to make sure that this combination functions. That said, there is a considerable difference between this case and a proprietary software license.[122] In proprietary software licensing, consideration is exchanged against the delivery of software or even just against permission to use said software, which is to be qualified a sale[123]. As a sale, it bears certain statutory warranties, including that the product is free from defects that reduce its intended use. If there is a separate agreement, such as a software development agreement, the relationship between the client and the developer – in particular the liability for defective software – is governed by this specific contract and not by the license. Also, in the absence of express warranties and representation, there is also the non-contractual liability and due diligence, in this case, seems to be the only protection one has.

Finally, liability could be claimed on tort.[124] It is reasonable to believe that a principle of "caveat emptor", meaning that the risks are placed on the recipient of software in a Free Software distribution could also apply. Therefore, only the final user who receives software as a part of a device or of a software distribution could be in a position to claim damages should the software be defective, and only vis-à-vis the party who has compiled the code.

Liability in terms of data protection requirements

As above mentioned, the general rule is that for any damage resulting from any unlawful processing of the employees' data, the controller will be held liable.[125] However, the proposed GDPR will subject data processors directly to a range of data protection obligations and liabilities. Therefore, processors will also be under a legal obligation to implement "data protection by design and by default", which therefore entails liability for the processors as well.[126] However, the controller may be exempted – partially of wholly – if he or she can provide evidence that he or she was not responsible for the event that gave rise to the damage. This provision is similar to the general Aquilian liability and the tort of negligence. Liability allocation and indemnity provisions should therefore be clarified in the contracts of processors and controllers.

2.3. Country specific regulations and relation to EU law

As above mentioned, country specific legislation must always be taken into consideration for the implementation of the developed Dogana platform. In this subsection, a short description of the implementation of the Data Protection Directive in the national legislation of three Member States will be provided, namely in Austria, Denmark, Greece, Italy, and Romania, since the trials will be held in

[122] European Commission, Workshop 'Legal aspects of free and open source software', 9 July 2013, http://www.europarl.europa.eu/document/activities/cont/201307/20130708ATT69346/20130708ATT69346EN.pdf, 43.

[123] ECJ, C-128/11, UsedSoft v. Oracle, § 44-72.

[124] The Free Dictionary by Farlex, http://legal-dictionary.thefreedictionary.com/Tort+Law.

[125] Articles 17, 18, and 23 of the Data Protection Directive.

[126] Article 22 of the GDPR.

these countries. The following analysis will mainly focus on the differences and similarities on the matter of the employees' personal data set out in these three national legislations.

In Austria, the Data Protection Directive is implemented by the Federal Act concerning the Protection of Personal Data[127]. The Austrian judicature has set out very strict requirements for a data subject's consent to be valid, as indicated in the schema below. In Denmark,[128] the Act on Processing of Personal Data (Act No. 429 of 31 May 2000) entered into force on 1 July 2000. In Greece, the Data Protection Directive was implemented by the Data Protection Act (Law 2472/1997[129]). According to the Opinion of the Hellenic Data Protection Authority[130], it is rather difficult for an employer to prove that employees have freely given consent, due to the imbalance of power between the parties resulting from the employment contract. In Italy, the Data Protection Directive was originally implemented by the Protection of Individuals and Other Subjects with regard to the Processing of Personal Data Act[131], which was later replaced by the Consolidation Act regarding the Protection of Personal Data[132]. Romania has implemented the Data Protection Directive by Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and Free Circulation of Such Data[133]. Within Romanian jurisdiction, the local secondary legislation on data protection matters provides certain particularities with regard to the processing activities of personal information for HR purposes. Hence, in Romania, submission of a notification is not required when the processing of personal data, regarding their own staff and external co-workers, is performed by public and private law entities in order to fulfil their legal obligations. In other words, employers are allowed to process personal information of their employees for the purpose of fulfilling the legal requirements in this field, without being under any obligation to notify such activities with the Data Protection Authority. In the table below, the different requirements in the employment context regarding consent in Austria, Greece, Italy, Denmark and Romania are outlined. As a general remark, the consent requirement is stricter in some countries, i.e. Austria and Greece, where in Italy and Romania, the conditions are broader or even vague and absent.

Table 2 'Requirements for consent in the employment context'

[127] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000) of 17 August 1999, http://www.coe.int/t/dghl/standardsetting/dataprotection/National%20laws/Austria%20Federal%20Act%20DP.pdf, more laws and opinions can be found in the website of the Austrian Data Protection Authority, https://www.dsb.gv.at/DesktopDefault.aspx?alias=dsken.

[128] Act on Processing of Personal Data (Act No. 429 of 31 May 2000), more laws and opinions can be found in the website of the Danish Data Protection Agency, http://www.datatilsynet.dk/english/the-danish-data-protection-agency/introduction-to-the-danish-data-protection-agency/.

[129] Greek Data Protection Act (Law 2472/1997, as amended by Laws 3471/2006, 3783/2009, 3947/2011, 4024/2011, 4070/2012 and 4139/2013), http://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL.

[130] Opinion No 115/2001 of the Greek Data Protection Authority on 20 September 2001, http://www.dpa.gr/portal/pp.?_pp.id=33,43590&_dad=portal&_schema=PORTAL.. More laws and opinions can be found in the website of the Hellenic Data Protection Authority,http://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL

[131] Italian Law no. 675/96 of 31 December 1996, http://www.privacy.it/legge675encoord.html. More laws and information can be found in the website of the Italian Data Protection Authority, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1665291.

[132] Italian Data Protection Code - Legislative Decree No. 196 of 30 June 2003, http://www.privacy.it/privacycode-en.html.

[133] Romanian Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and Free Circulation of Such Data, published in the Official Gazette No. 790 of 12 December 2001, http://ec.europa.eu/justice/policies/privacy/docs/implementation/ro_law_677_2001_en_unofficial.pdf. More laws and information can be found in the website of the Romanian Data Protection Authority http://www.dataprotection.ro/index.jsp?page=home&lang=en.

Countries:	Consent in the employment context:
Austria	(i) the data subject must be provided with all relevant information about the data to be processed, the purpose of the respective data processing and any potential data recipients; (ii) the consent must be given without any restraints (the Austrian courts are frequently reluctant to accept the validity of employee consent); (iii) the data subject has to receive explicit information about his right to revoke his consent at any time, without giving reason for such revocation.
Denmark	"Consent from employees is to be obtained in the same manner as from any other data subjects. It is not a requirement to obtain consent from the data subject in writing; however, the consent must be freely given, specific and informed and, in order for the data controller to be able to prove that such consent has been obtained, it is recommended that the consent is obtained in writing. Also, due to the fact that the consent must be freely given, specific and informed, an implied consent or a consent obtained by an "opt-out" solution will not fulfil the requirements to obtain consent under the DPA."[134]
Greece	(i) it is rather difficult for an employer to prove that employees have freely given consent, due to the imbalance of power between the parties resulting from the employment contract. (ii) where employees' consent is considered freely given, it can only be provided for precisely determined purposes. (iii) it is forbidden to collect or process employee personal data for purposes not directly or indirectly involved with the employment relationship, irrespective of the employee's consent.
Italy	(i) the employee's consent is not necessary, under the legitimate interest exemption; (ii) provided the processing carried out by the employer is aimed at fulfilling the contractual employment relationship or complying with legal provisions, regulations or collective agreements.
Romania	"There are no specific rules regarding consent in the employment relationship. In practice, to data the DPA has not raised objections in respect of employers basing their personal data processing operations on (potential) employees' consent, provided that the processing complies with the general personal data rules provided by the Romanian data privacy laws. In fact, it is more likely that the DPA would object to processing operations involving the personal data of employees on the grounds that they are in breach of adequacy or non-excessiveness requirement set under the law, rather than object to the legitimacy of the processing that relies on the data subject's consent"[135].

134 Linklaters, https://clientsites.linklaters.com/Clients/dataprotected/Pages/Denmark.aspx.

[135] R. Ionescu, and O. Balaceanu, Data Protection and Privacy: Jurisdictional Comparisons, 2012, 469.

3. LEGAL AND ETHICAL CHALLENGES FOR CONDUCTING SDVAs IN ORGANISATIONAL SETTINGS

3.1. Legal framework relevant to SDVAs

In this section all the important elements relating to conducting SDVAs in organisational settings will be developed. A further detailed analysis regarding the situation where companies will use Dogana and conduct the SDVAs provided by Dogana, will be provided in D5.3 'Legal and ethical requirements for the development of Dogana: organisational context settings'. In particular, in this section, the several legal and ethical complications in performing social vulnerability assessments in the companies, taking into consideration the requirements set by European and national legislations.

3.2. Relevance for the Dogana project

The aim of Dogana is to develop a holistic instrument in order to tackle social engineering attacks against companies. While a security assessment aims at simulating attack patterns, as real as possible and before they really happen in order to measure the real vulnerability of a company, the Social Vulnerability Assessments (SDVAs) are a new type of assessment, actively using social engineering techniques in the assessment process. Since the essence of an SDVA is to understand the behaviour of the employees in the company, an interference with the private lives of the employees will be possible. For example, there will be monitoring of the employees' behaviour, for example via responses to phishing attacks, with the aim to measure how this behaviour places the company's security at risk. Since the domain presents legal lacunae, recommendations for policy makers at company level will be made in order to encounter the legal challenges. Where intervention at company level cannot be sufficient, recommendation to law makers will be made on national and / or European level, which will be further developed in D5.5 'Legal and Ethical Recommendations for policy-makers'.

Regarding the ethical challenges that companies will to encounter by implementing the Dogana solution, it is important to note that the basis for the deployment of Dogana is the concept of deception. As research[136] has demonstrated, deception is the only way for assuring that there will be no bias of the employees during the assessment of their vulnerability.

3.3. Privacy vs security

While employees are having a legitimate expectation of privacy in the workplace, this right must be balanced with the rights and interests of the employer. In particular, a balance must be found between the employer's rights to run their business efficiently and to control and organise their protection from any liability or harm an employee's actions and/or omissions may create. These rights and interests constitute legitimate grounds that may justify appropriate measures to limit the worker's right to privacy, such as where the employer is victim of a worker's criminal offence or where the employees' use of social networking sites causes damage to the employer's business reputation or releases confidential information. However, balancing different rights and interests requires taking a number of principles into account, and in particular, the principle of proportionality.

[136] T. Dimkov, W. Pieters, and P. Hartel, Two methodologies for physical penetration testing using social engineering, University of Twente, 2009, 1-11.

3.3.1. Privacy

As already analysed above, the employees have a right to privacy even in their workplace. In particular, the employees must be aware of the fact that a security mechanism affecting them is put in place in their workplace. Phishing attacks and other methods developed by Dogana will affect the employees' rights and therefore, their representatives must be consulted and/or informed accordingly before any such implementation. In this respect, the legal requirements set by national legislations must be taken into consideration on a case-by-case approach.

3.3.2. Security

The employees have the obligation to assure the security of the company's assets, including the company's data assets, IP rights, and infrastructure and at the same time to provide a safe working environment for their employees. It is also the employer's right to protect the networks against any unauthorised accesses or attacks. Therefore, adequate and appropriate measures must be implemented[137] and the employees, under their contractual engagements, must respect and follow these rules.

The selection and application of appropriate policies, standards and procedures enables companies to better secure their networks and information resources. Policies (statements of intent by the business's management to adhere to certain values and goals), procedures (methods for meeting the requirements set out in the policies), technical standards (specifications for the technology used by the company), guidelines and training materials (to provide information to employees about following the procedures established by the company), and rest category (other supporting documentation, such as device usage lifecycle etc.) can be used in order to better implement the obligation of the employees for achieving the company's security.

Key principles

The involvement of the employees,[138] and in particular the consultation and participation of the employees in the drafting of policies and in the decision-making process procedure[139] is crucial for the company to achieve an increased level of security. Therefore, during the whole organisational security management process, it is of essence for the company to create an information security company culture, to be transparent regarding managerial decisions and procedures, and in particular, to involve employees in the decision-making process.[140] In terms of the implementation of the Dogana solution to companies, it follows from the above that the employees must be appropriately informed and involved, in order to achieve greater security.

[137] For more information, see also European Network and Information Security Agency (ENISA) in relation to network and information security and recent security threats encountered, available at https://www.enisa.europa.eu/.

[138] See also, Article 27 of the Charter of Fundamental Rights of the European Union: "Workers' right to information and consultation within the undertaking: Workers or their representatives must, at the appropriate levels, be guaranteed information and consultation in good time in the cases and under the conditions provided for by Community law and national laws and practices."

[139] Articles 17 and 18 of the Community Charter of the Fundamental Social Rights for Workers of 1989.

[140] Y.S. Van Der Sype, E. Frumento, and Z. Hodaie, 'Policy Recommendations for end-user responsibility', MUSES project, D7.3, 2013, 38.

In this point, it is also important to refer to the social dialogue, which as part of the policy of promoting the engagement of the European social partners in the formulation of EU social policy, Articles 154-155 TFEU[141] provide a procedure that combines the consultation of the social partners by the Commission with the option to leave social regulation to bipartite agreement between management and labour organised at European level. The European social dialogue[142] has led to both intersectoral and sectoral European collective agreements. Its outcomes are modest if compared to national systems of collective bargaining and social dialogue. The present prospect of the EU social dialogue implies rather a tripartite process, involving the social partners and the Commission/Community as a dynamic factor. Since its creation, the social dialogue procedure[143] has produced seven agreements at intersectoral level. Three have been transformed into directives relating to Framework agreements.[144] The most striking development of European sectoral social dialogue agreements emerged in a number of transport sectors as a result of negotiations following their initial exclusion from the Working Time Directive[145]

3.4. Guidelines regarding transparency for employers

Following from the above, when implementing a security solution in the company, the employers should take into account the following recommendations.

Table 3 'Guidelines for employers'

Set out clearly to the employees the conditions under which they could be possibly attacked by phishing emails.
Specify material that cannot be viewed or copied.
Inform the employees about the systems implemented both to prevent access to certain information (and/or websites) and to detect misuse.
Inform the employees about the notification process of introducing new technologies in the company and in its implementation.
If surveillance or monitoring of communications use is to be carried out, make clear to the employees the reasons and purposes for which this will be undertaken (type of surveillance, how and when it will take place).
Include all these issues in the employer's policy and document it.
Set out enforcement procedures.

[141] Articles 154-155 of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU), 2012, C 326/01.

[142] European Commission, "A new Start for social dialogue", 2015, file:///C:/Users/u0105702/Downloads/SocialDialogue_brochure_FINAL.pdf, last visited on 12 March 2016.

[143] Articles 154-155 TFEU.

[144] Council Directive 96/34/EC of 3 June 1996 on the Framework Agreement on parental leave concluded by UNICE, CEEP and ETUC and revised in 2009; Council Directive 97/81/EC of 15 December 1997 concerning the Framework Agreement on part-time work concluded by UNICE, CEEP and ETUC; and Council Directive 1999/70/EC of 28 June 1999 concerning the Framework Agreement on fixed-term work concluded by ETUC, UNICE and CEEP.

[145] Council Directive 93/104/EC of 23 November 1993 concerning certain aspects of the organisation of working time.

Provide opportunities for responses in cases of breaches of obligations.

4. ETHICAL AND LEGAL CHALLENGES REGARDING THE ORGANISATION OF THE DOGANA PROJECT

In the previous section, we described the implementation of Dogana in the organisational settings. In this section, the elements for the development of the Dogana project will be analysed. In particular, we will outline the concept of Privacy by Design, which will be further analysed in detail in D.5.2 'Legal requirements for Privacy by Design '. Also, the legal and ethical challenges for involving human participants in the Dogana project will be described, as a basis for further development in D.5.4. 'Legal and Ethical Requirements for the development of Dogana: human participation, trials and testing'.

4.1. The concept of Privacy by Design

This section provides a brief overview of the principles of Privacy by Design. This principle is codified in Article 23 of the GDPR. In brief, privacy and security should be taken into account by stakeholders not only at the final stages of the product or service configuration, but from its very inception.[146] Privacy and security have to be embedded, by default and design[147], from the very outset of the project and Dogana will be developed in application of these principles.

4.1.1. The principles of Privacy by Design and Privacy by Default

Privacy by Design[148] means that each new service or business process that makes use of personal data must take the protection of such data into consideration. "The concept of Privacy by Design is to integrate privacy-requirements and privacy-preserving solutions in the engineering of products and services (privacy engineering). As such, privacy becomes an essential component in the core of the delivered functionality. Privacy becomes an integral part of the system without diminishing functionality".[149] In other words, in order to mitigate privacy concerns and to achieve data protection compliance[150], privacy should be embraced from within the systems"[151]. An organisation needs to be able to show that they have adequate security in place and that compliance is monitored. In practice this means that an IT department must take privacy into account during the whole life cycle of the system or process development. Therefore, this principle will be embedded in the technology of Dogana from the early phases of its development.

Privacy by Default[152] means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must - by default - only be kept for the amount of time necessary to provide the product or service. For example, imagine signing up for a new social media service on which one can share

[146] Article 29 Working Party, Opinion 8/2014 on the on recent developments on the Internet of Things, adopted on 16 September 2014, 19.

[147] A. Cavoukian, "Privacy by design: the 7 Foundational Principles", Information and privacy commissioner of Ontario, 2009 https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf, 2.

[148] Article 23 of the GDPR.

[149] A. Cavoukian, Privacy by design: the 7 foundational principles, Information and privacy commissioner of Ontario, 2009, 2.

[150] S. Gurses, C. Troncoso, and C. Diaz, Engineering Privacy by Design, K.U. Leuven/IBBT, ESAT/SCD-COSIC, 1-25.

[151] Y.S. Van Der Sype, "On the road to privacy-friendly security technologies in the workplace", Muses RT2AE V P/DP, CPDP 2016.

[152] Article 23 of the GDPR.

personal information, life events and other content. In order to successfully publish one's profile, only the name and email address are required, yet the new service also automatically publishes age and location and makes it available to the public, rather than just to one's connections. This would be a clear breach of the privacy by default principle, since more information is disclosed to the public than is necessary, in order for this service to be provided. It is noteworthy that the regulation specifically identifies and prohibits services that by default make personal information accessible to an indefinite number of individuals.

In practical terms, these principles mean that data protection will become an integral part of both the technological development, as well as the organisational structure of a new product or service. Therefore, when embedding these principles into the technology, the focus must be based on four principles, namely the purpose limitation principle[153], the data minimisation principle[154], the transparency principle[155] and the data security principle[156].

4.1.2. Security by Design

Definitions

By "Security by Design" it is meant an approach to information security which, like Privacy by Design, is at once holistic, creative, anticipatory, interdisciplinary, robust, accountable and embedded into systems, since their inception. It stands in direct contrast to "security through obscurity," which approaches security from the standpoints of secrecy, complexity or overall unintelligibility. Within the field of engineering, the approach of Security by Design has a lot in common with the conception of "Security Engineering", i.e. seeking at making systems as free of vulnerabilities and impervious to attack as possible through measures like continuous testing, authentication safeguards and adherence to best programming practices. Malicious practices are taken for granted and care is taken to minimize impact when a security vulnerability is discovered or on invalid user input. [157]

[153] The principle of purpose limitation contains two elements, namely the purpose specification element ('specified, explicit and legitimate purpose') and the compatible use element ('not further processed in an incompatible way'). As such, the "reasons for the collection, use and disclosure of personally identifiable information should be identified to the data subject at or before the time of data collection. Personal information cannot be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as authorised by law", A. Cavoukian, Privacy and security by design: a convergence of paradigms, Information and privacy commissioner of Ontario, Canada, 2013 https://www.privacybydesign.ca/content/uploads/2013/01/pbd-convergenceofparadigms.pdf, 2.

[154] The principle of data minimisation requires that personal information shall only be used or disclosed in order to achieve the purpose of the processing (collection, storage or analysis). When the information is no longer accurate or necessary, it should be erased. This principle also implies that the processing must be carried out in the least-intrusive way, considering the risks at stake, the amount of data involved, the purpose of processing, etc.

[155] The transparency principle relates to the participation of users and specifies that "individuals should be empowered to play a participatory role in the lifecycle of their own personal data and should be made aware of the practices associated with its use and disclosure", Article 29 Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, and WP203 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 18.

[156] The data security principle highlights the need for strong security. This implies that "confidentiality, integrity and availability should be safeguarded, as appropriate to the sensitivity of the information", Article 29 Working Party, Opinion 03/2013 on purpose limitation, adopted on 2 April 2013, and WP203 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, 27.

[157] A. Cavoukian, M. Dixon, "Privacy and Security By Design: An Enterprise Architecture Approach", 2013, https://blogs.oracle.com/OracleIDM/entry/privacy_and_security_by_design.

The European Security Research and Innovation Forum (ESRIF) in its 2009 final report[158] defines the Security by Design concept as "to embed security in the technology and system development from the early stages of conceptualisation and design".

The main goal of Security by Design is to make the system complying "from scratch" with four suggested principles on which general system design, and in particular information security, should be based:

- **Confidentiality**: meaning that information is only being seen or used by people who are authorized to access it.
- **Integrity:** any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.
- **Availability**: the information is accessible when authorized users need it[159].

The design and development processes of the Dogana SDVA framework implementation must adhere to those principles, while at the same time respecting imposed standards and regulations.
Several different approaches and methods can be adopted to successfully implement Security by Design in software development, depending on the type of application and target domain.

Some scenarios and indication related to the development of the Dogana framework with the Security by Design method

We give here some initial indications, inferred from scenarios taken from various Web and literature sources, which could be of relevance to implement the DOGANA framework with the Security by Design approach

Protocols security: Typical security systems consist of several components such as people, companies, computers and card readers, which communicate by the mean of several types of channels including phones, email, radio signals, and by carrying data on physical devices such as bank cards and transport tickets. The security protocols are the rules that govern the secure communications. They are typically designed so that the system will survive malicious attacks such as people telling lies on the phone, hostile subjects jamming radio, or forgers altering the data on train tickets. Protection against all possible attacks is often too expensive, so protocols are typically designed under certain assumptions about the possible threats. For example, the logon protocol that consists of a user entering a password into a machine assumes that he can enter it into the right machine. For the Dogana framework it appears therefore essential considering the protocol aspect since the very beginning, by answering two questions:

- first, is the threat model realistic?
- second, does the protocol deal with it?

Network attacks: Attacks depend more and more on connectivity, and can manifest mainly at two levels:

[158] http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf.

[159] Sometimes in the literature it is also included to the classic triad the concept of "Non-repudiation" (one's intention to legally fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction). But often Non-repudiation is regarded as part of "Integrity", and here we prefer to adhere to this more orthodox vision.

- the connectivity level
- the application level

As an example of the connectivity level, consider an office worker clicking on an attachment in email coming from a friend (or relative). This infects his PC with malware that compromises other machines in his office by intercepting passwords that travel across the LAN. The malware had infected his friend's machine and then sent out a copy of a recent email, with itself attached, to everyone in friend's address book.
On the other hand, at the application level, a person got infected by an old friend of him who chose a common password for his ISP account. When there are many machines on a network, prowlers easily guess the password for a particular account just trying one password over and over for millions of accounts. Given a webmail account, they can send out bad email to the whole contact list.
Other network attack types exploit network protocol vulnerabilities. Often, these can be mitigated by designing the protocol secure.
Dogana, by its very nature, should take care of threats related to networking; its design and implementation should be hardened against possible network attacks at the connectivity as well as application levels.

Social media attacks: in social media the use of application levels' network attacks is pushed further into the sociological/psychological domain. The application of Social Engineering turns out to be particularly aggressive in the social media field. During the whole Dogana implementation stage, care must be taken in the use of on-line blogs and social media to gather and exchange information. Moreover, bringing the Dogana framework's implementation a series of countermeasures against social engineering techniques (among other outcomes), it could be used recursively to increase its implementation's level of security against social engineering threats.
API security: Many modern devices have some kind of application programming interface (API) that untrustworthy people and processes can access in order to get some task performed.

- A bank's server will ask an attached hardware security module "Here's a customer account number and PIN, with the PIN encrypted using the key we share with VISA. Is the PIN correct?"
- If one enables JavaScript, then a browser exposes an application programming interface which the owners of visited websites can use to perform various cyberattacks.

To mitigate such kinds of threat, a secure operating system, for instance, may limit the calls that an application program can make, using a reference monitor or other wrapper to enforce a policy such as preventing information flow from High to Low.
Wherever in the DOGANA framework the development of any API layer could result necessary, it should be securized accordingly.

Copyright and digital rights: Copyright and digital rights management have been among the most critical issues of the digital age. Copyright mechanisms exist to protect information from using by people who haven't paid for it. Software is by no way different. Software for early computers was given away free by the hardware vendors or by users who'd written it. IBM even set up a scheme in the 1960"s whereby its users could share programs they had written, therefore copyrighting software wasn't an issue. But when minicomputers arrived in the 1960's, software costs started to become significant; however software piracy really started to become a serious problem when the arrival of microcomputers in the late 1970's and early 80's created a mass market. Since then, the software-as-a-IP issue has never been fixed completely, but several countermeasures to protect against

infringements have been put on the field. To name just a few: hardware dongles, hard disk sectors manipulation, PC"s configuration storage, limited-time functioning, etc.
The DOGANA framework must plan a series of measures to counteract possible copyright infringements on the outcomes produced during its implementation.

4.2. A Security by Design recipe

Microsoft in its publication "Security Engineering Explained"[160] suggests a set of directives to develop software based on Secure by Design paradigm. It identifies four phases:

4.2.1. Security Architecture and Design Approach

The initial series of activities are relating to architecture definition and design and include:

- **Identifying security objectives**: these are goals and constraints that affect the confidentiality, integrity, and availability of data and application.
- **Applying secure design guidelines, patterns, and principles**: represent proven practices that have evolved over time to reduce risks associated with designing applications.
- **Creating threat models**: threat modeling is an engineering technique that can be used to help identify threats, attacks, vulnerabilities, and countermeasures that may be relevant to an application, and to identify when and where more resources are required to reduce risks

Security Architecture and Design Review

The three major aspects to consider while conducting an architecture and design review for security are shown in Figure 1.
To perform a security architecture and design review, **one** evaluate**s the** application architecture in relation to its target deployment environment. Next, **a design choices** review **is performed** in each of the key areas defined by the security frame. Finally, **one** conduct**s** a layer-by-layer analysis and examines the security mechanisms employed by your key components within each of the layers.

[160] Microsoft pattern & practice, Security Engineering Explained, 2005, https://www.microsoft.com/en-us/download/details.aspx?id=20528.

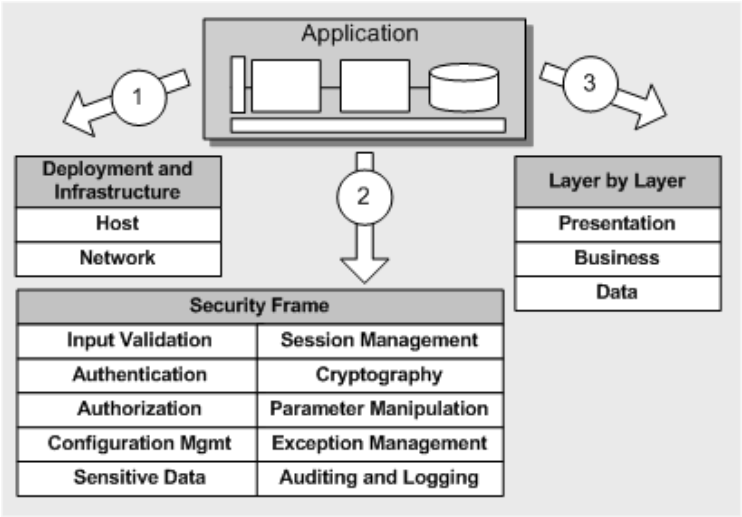


Figure 1 - Security Architecture and Design Review (source: Microsoft pattern & practice, "Security Engineering Explained", 2005, https://www.microsoft.com/en-us/download/details.aspx?id=20528).

- **Deployment and infrastructure.** Review the design of the application as it relates to the target deployment environment and the associated security policies. Consider the constraints imposed by the underlying infrastructure-layer security and the operational practices in use.
- **Security frame.** Review the security approach that was used for critical areas of the application. An effective way to do this is to focus on the set of categories that have the most impact on security, particularly at an architectural and design level, and where mistakes are most often made. The security frame describes these categories. They include authentication, authorization, input validation, exception management, and other areas. Use the security frame as a roadmap so that you can perform reviews consistently, and to make sure that you do not miss any important areas during the review.
- **Layer-by-layer analysis.** Review the logical layers of your application, and evaluate your security choices within your presentation, business, and data access logic.

Security Code Review

The purpose of a security code review is to inspect source code to discover security issues before testing and deployment begins. The four major code review steps are shown in Figure 2.

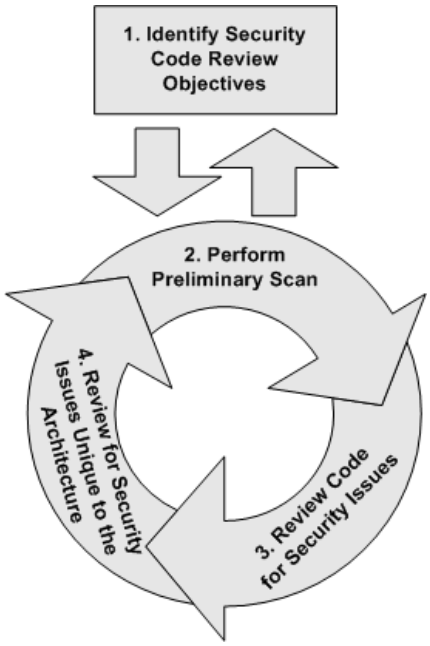


Figure 2 - Code review steps (source: Microsoft pattern & practice, "Security Engineering Explained", 2005, https://www.microsoft.com/en-us/download/details.aspx?id=20528).

- **Step 1. Identify security code review objectives**. Establish goals and constraints for the review.
- **Step 2. Perform a preliminary scan**. Use static analysis to find an initial set of security issues and improve understanding of where the security issues are most likely to be discovered through further review.
- **Step 3. Review the code for security issues**. Review the code thoroughly with the goal of finding security issues that are common to many applications. One can use the results of step two to focus your analysis.
- **Step 4. Review for security issues unique to the architecture**. Complete a final analysis looking for security issues that relate to the unique architecture of an application. This step is most important if a custom security mechanism or any feature were designed specifically to mitigate a known security threat.

Security Deployment Review

When reviewing security deployment, precautions one must take and the settings one must configure can be organized into categories. By using these configuration categories, one can systematically review the securing process or pick a particular category and complete specific steps. The categories are shown in Figure 3.

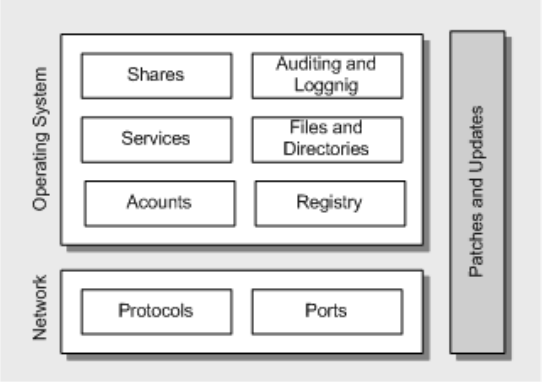


Figure 3 - Deployment configuration categories (source: Microsoft pattern & practice, "Security Engineering Explained", 2005, https://www.microsoft.com/en-us/download/details.aspx?id=20528).

4.3. Data Handling

The second topic treated in the present discussion is how **data storage, transfer, retrieval and recovery** could raise ethical and legal issues in the Dogana project's implementation. Fairly data handling in the Dogana project is a most sensitive subject: Dogana's main goal is to develop a framework delivering an Advanced Social Engineering and Vulnerability Assessment (SDVA), the implementation of which involves investigations touching the heart of the psychological, social and ethical implications of the human sphere. The problem of personal data protection was already touched in section 2.2.2 of this document in the framework of the ethical and legal challenges. The relevant regulation identified there was the EU Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. This regulation also discusses the movement of personal data, in Article 47 and from Article 57 to Article 66.[161]. Nigel Stanley summarizes the requirements for handling personal data, following the aforementioned directive, in the following seven principles[162]:

- **The Principle of Openness:** policies and procedures about information handling should be made readily available; nevertheless, data must not be allowed to leave the Member States unless the destination countries have similar legislation
- **The Principle of Individual Participation**: data must be processed in line with a person's rights
- **The Principle of Collection Limitation**: data must be processed fairly and lawfully and collected with the knowledge or consent of the data subject
- **The Principle of Data Quality**: data must be accurate and up to date, adequate, relevant and not excessive

[161] 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.

[162] N. Stanley, EU compliance and regulations for the IT security professional, White Paper b< Bloor Research, March 2009, p. 7, https://www.qualys.com/docs/EU_Compliance.pdf.

- **The Principle of Finality**: data must be processed for limited purposes and kept for as long as necessary
- **The Principle of Security**: data must be secured against such risks as loss or unauthorised access, destruction, use, modification or disclosure
- **The Principle of Accountability**: a specialist in the role of "data controller" should be accounted in order for the adopted measures to comply with the established data protection directives. The points above aim at being fully compliant with the foundational principles of data management, which are secure storage, confidentiality and selective availability[163]. The Dogana implementation will try to operate in full respect of these principles.

4.3.1. The Dogana case in relation to Security by Design's ethical and legal challenges

The aim of the Dogana project is to build the SDVA framework from the ground up within the context of the Security by Design paradigm. From an organizational perspective, actions have to be undertaken in order to allow for checking the respect of all applicable laws and standards. A specific committee shall be appointed, this committee has to be selected in a way to cover all aspects and skill required by the complexity of the project, from hardware selection and/or development, to software supply chain developing and the whole testing, field trials and validation activities.

These tasks cannot be covered in parallel and cannot be closed during the project development, these activities and monitoring shall flow all along the project and constantly check that the SbD prerequisite defined at the beginning are constantly respected.

The development of the Dogana SDVA framework with the Security by Design approach must consider at least the following technical topics:

a) System engineering methodology
b) Security policy and requirements engineering
c) Requirements evolution management, change management
d) Project requirements management
e) Process parallelization

We examine the above points in the light of the ethical and legal challenges that the Dogana project must face.

System engineering methodology

System engineering was initially conceived in the effort to produce technological systems that are economical, reliable and work efficiently in real situations. This must be achieved by managing two kinds of complexity: contingent complexity, involved in developing using inadequate tools, and intrinsic complexity when dealing with large and complex systems. The first kind of complexity can often be avoided by accurately choose technical tools during the design stage, whereas intrinsic complexity usually requires methodological tools that help subdivide the system into smaller manageable

[163] P. White, The Principles of Good Data Management, IGGI, UK, 2005 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/14867/Good_dataMan.pdf.

components (divide et impera) and limit the extent to which these subsystems can interact. Basically there are two widespread methodologies, which are adopted in mitigating intrinsic complexity:

- **Top-down design.** The classical approach in top-down design is the Waterfall model[164], in which one starts from a concise statement of the system's requirements and elaborate this into a specification; then implement and test the system's components, followed by integrating them together and testing them as a whole system; then unwind the system for live operation. At the first two phases in this chain there is a feedback on whether the engineer is building the right system (validation) and at the next two on whether he/she is building it right (verification). There may be more than four steps: a common variant is to have a sequence of refinement stages as the requirements are developed into ever more detailed specifications The strengths of the waterfall model are: it forces early clarification of system goals, architecture, and interfaces; it makes the project manager's task easier by providing clear milestones; it may increase cost transparency by allowing separate charges to be made for each step, and for any late specification changes; and it is compatible with a big range of tools. The critical aspect about the waterfall model is that development flows unavoidably downwards from the first statement of the requirements to the deployment of the system, without any system-level feedback from system testing to the requirements. With the today systems complexity constantly increasing, and the consequent necessity in the improvement of maintenance requirements, this can result in an important drawback. Based on those considerations, alternative top-down methods, like the agile model[165], are not adequate for a SbD approach.
- **Iterative design.** In case of necessity to consolidate the specifications, a common approach is Barry Boehm's spiral model in which the development line proceeds through a predetermined number of iterations. A prototype is built and tested, and managers being able to evaluate the risk at each stage can decide whether to proceed with the next iteration or rethink the objectives; on the other hand, when the deal is to manage the complexity or enhancing an already existing large system, the standard model is evolutionary development. Earlier investigated by Harlan Mills, in the evolutionary model it is taught that one should build the smallest system that effectively works, try it out on a real environment, and then add functionality in small increments.[166] In this view, products aren't the result of a project but of a process requiring to continually update previous versions. The critical point of the evolutionary approach is that, as each generation of a biological species has to be viable for the species to continue, so each generation of an evolving technological product must be viable. Therefore, regression testing, by which assessment verifications are continually conducted on all or parts of the evolving subsystems, are an essential ingredient of this methodology. But automated testing is not that useful for the security engineer, because security properties are more diverse, and security engineers are fewer in number, so there hasn't been as much investment in tools and the available tools are much more fragmentary and primitive than those available to the usual engineering community. Many of the flaws that system engineers seek and fix tend to appear in new features rather than to reappear in old ones. Specific types of attack are also often easier to fix using targeted remedies. And many

[164] The Waterfall Model was first described in WW Royce, ''Managing the development of Large Software Systems: Concepts and Techniques'', in Proceedings IEEE WESCON (1970).

[165] See the Agile Manifesto, http://agilemanifesto.org/.

[166] S. Maguire, Debugging the Development Process, Microsoft Press, ISBN 1-55615-650-2 p 50 (1994).

> security flaws cross all of the system's levels of abstraction, such as when specification errors interact with user interface features— the sort of problem for which it's difficult to devise automated tests. But regression testing is still a really important tool. It often detects functionalities that have been affected by changes, but not fully understood (by the way much the same applies to safety critical systems, which are similar in many respects to secure systems).

Both approaches, the top-down model and the iterative design, could be successfully implemented in the Dogana framework. Nevertheless, the waterfall method could unveil all its weaknesses in particular as far as the ethical and legal aspects is concerned: as described before, within that method there is no feedback at the system-level as a whole, i.e. from system testing to the requirements. If a system is particularly complex, composed of many different subsystems, evolving and long lasting in time (such as Dogana is supposed to be), it may become very difficult for the designer to discover ethical or, even worst, legal nonconformities: a change in legislation touching a past stage of the development (for instance during the specification phase) could be totally ignored and never ever considered.

An iterative design, in particular the evolutionary model, should therefore be more suitable for the development of the Dogana SDVA framework in the SbD perspective. The constant monitoring of changes in ethical/legal boundary conditions can be directly integrated in the methodology and modifications can be promptly considered in the system evolution, averting the danger of omission of important regulations and directives.

Security policy and requirements engineering

The process of developing a security policy and obtaining agreement on it from the system owner is called requirements engineering. Usually it starts by investigating and defining a threat model setting out the attacks and failures with which the system must be able to cope, and which in turn drives the definition of a security policy model to be a concise statement of the protection properties that a system must guarantee. Security requirements engineering is often the most critical task of managing secure system development, and can also be the hardest. It's at the intersection of the most difficult technical issues, the most acute bureaucratic power struggles, and the most determined efforts at blame avoidance, reason why frequently it can closely involve ethical considerations and sometimes even bump into legal barriers: if the policies are unclear, ambiguous or incomplete, the subject can be unaware of law infringement. Also, particular care should be put in the management of risk, and have the risk assessment drive the development or evolution of the security policy: ethical/legal issues becoming a relevant part of risk assessment. Moreover, risk management must also continue once the system is deployed (this can often be more an ethical issue than an obligation requirement).

Requirements evolution management, change management

In general security requirements have to be re-tuned for one out of four reasons. First, there might be the need to fix a defect. Second, the system must be improved. Third, the environment itself could be evolving thus creating the necessity to adapt the system. Fourth, there may be a change in the organization (firms are continually undergoing mergers, management buyouts or business process reengineering).

The third reason, changes in environment, could also result in the change of ethical/legal conditions: times evolve and persons" ethical sensibility change accordingly, and with time this inevitably reflects in legal adjustments. Finally, changes can intervene not only in time but also in space: a product's market could move to another country where ethical or legal conditions are different substantially or in part.

Projects requirements management

This section lays at the core (and the "hardest part") of the business, since it is dealing with how to do security requirements engineering for such a far reaching project as Dogana. Some related examples can include building an e-commerce portal from scratch, or an established application going online as critical components acquire the ability to communicate (such as postage meters, or developing burglar alarms and door locks). Building things from scratch is an accident-prone business; many large development projects have failed. The problems appear to be very much the same whether the disaster is a matter of safety, of security or of the software simply never working at all. According to Herb Simon's classic mode of engineering design, one starts from a goal, a utility function and budget constraints, then work through a design tree of decisions until one finds a design that's "good enough", then iterate the search until one finds the best design or run out of time[167]. As many important guidelines on "how to do it" are in fact warnings about how not to. The classic study of large software project disasters was written by Bill Curtis, Herb Krasner, and Neil Iscoe[168]: they found that failure to understand the requirements was to avoid as much as possible: a thin spread of application domain knowledge typically led to erratic and conflicting requirements which in turn caused a breakdown in communication. They suggested that the solution was to find an "exceptional designer" with a strong understanding of the problem who would assume main responsibility. Therefore the requirements engineer needs to acquire a deep knowledge of the application as well as of the people who might attack it and the kind of tools they might use. The more likely the domain experts are available, the better.

A recent influential publication is a book on threat modeling by F. Swiderski and W. Snyder[169]. This publication describes the methodology adopted by Microsoft following its big security push. The basic idea is that one lists the assets is trying to protect (ability to do transactions, access to classified data) and also the assets available to an attacker (perhaps the ability to subscribe to your system, or to manipulate inputs to the smartcard). One then traces through the system, from one module to another, trying to figure out what the trust levels are and where the attack paths might be; where the barriers are; and what techniques, such as spoofing, tampering, repudiation, information disclosure, service denial and elevation of privilege, might be used to overcome particular barriers. The threat model can be used for various purposes at different points in the security development lifecycle, from architecture reviews through targeting code reviews and penetration tests. What one is likely to find is that in order to make the complexity manageable, one has to impose a security policy — as an abstraction, or even just a rule of thumb that enables to focus on the exceptions. Possibly the subject can result even harder if one takes into account the ethical and legal domains. Very stringent constraints can be imposed by such barriers, resulting in the impossibility for some parts or subsystems

[167] H. Simon, The Sciences of the Artificial,MIT Press, 1996, 241.

[168] W. Curtis, H. Krasner, N. Iscoe, ''A Field Study of the Software Design Process for Large Systems'', 1268–87.

[169] F Swiderski, W Snyder, threat Modeling, Microsoft Press 2004, 65-68.

of the project to be implemented. In the worst case, the entire project is so excruciated that its destiny is the abandonment.

Therefore, particular care must be taken by the Dogana project on the ethical/legal aspects in relation to its requirements management.

4.3.2. Comparison with the Privacy by Design paradigm

Finally, the Security by Design (SbD) approach can be put in strict comparison with Privacy by Design. The following table attempts to give such a categorization by inspiring to seven Privacy by Design general measures that are relevant to the Dogana framework implementation. Furthermore it tries to identify and respond to possible ethical and/or legal problems implied.

SbD characteristic	Description	Security aspects	Ethical/legal issues
1. Proactive not Reactive; Preventative not Remedial	Defining and designing company's security strategy in advance.	Begin with the end in mind. Leverage enterprise architecture methods to guide the proactive implementation of security.	Ethical and legal issues are taken into consideration from the start. Ethical/legal policies are identified and established in this phase.

2. Default Setting	Secure by Default is a concept that covers policies for implementing security controls and specific methods for installing and configuring software. In both cases, the goal is to make sure information systems are configured to be as secure as possible by default, rather than having users do it one by one or, worse, tightening down security after the fact.	Implement "Secure by Default" policies, including least privilege, need-to-know, least trust, mandatory access control and separation of duties.	Secure by Default policies have to be implemented with respect of users" ethical requirements. Also, legal regulations have to be observed, if necessary.
3. Embedded into Design	In order to produce secure systems, security must be embedded into the design of such systems. Embedding security into the design of secure systems, nevertheless, can happen in two ways: through the software and through the hardware of a system.	Apply Software Security Assurance practices. Use hardware solutions such as Trusted Platform Module.	
4. Positive-Sum, not Zero-Sum	Security by Design as with Privacy by Design seeks to achieve a positive-sum result where one can have both privacy and security. All too often privacy is forfeited for security. In addition to privacy, there are other objectives and interests that may appear to be in conflict with security.	Accommodate all stakeholders. Resolve conflicts to seek win-win.	Personal privacy as stated in regulations (e.g. Directive 95/46/EC, see section 2.2.2 of the present document) must be reverenced first.

5. End-to-End Security	The objective of enterprise security is to ensure confidentiality, integrity and availability of all information for all stakeholders in the enterprise. In order for it to really enable privacy, security must address and compensate for potential vulnerabilities throughout the enterprise, not just at the perimeter or in part of the enterprise. Experience has shown that old methods of protecting just the perimeter of the enterprise are woefully inadequate. Only when the security strategy addresses the enterprise end-to-end can privacy be protected and enterprise activities and assets be enabled and protected.	Ensure confidentiality, integrity and availability of all information for all stakeholders.	ibidem, personal privacy must be respected first.
6. Visibility and Transparency	Visibility and transparency are well-known security principles that strengthen customer and vendor confidence in the security of information systems.	Strengthen security through open standards, well-known processes and external validation.	Visibility and Transparency must be applied whenever not in contrast with users" ethical requirements or existing laws

7. Respect for the User	A basic principle of Privacy by Design is to focus on the individual and have respect for individual privacy rights. Security, however, addresses a broader constituency. It must respect and protect the interests of all information owners, accommodating both individual and enterprise interests. For example, economic espionage, where the primary target is intellectual property, not personally identifiable information (PII), is rampant in today's business environment.	Respect and protect the interests of all information owners. Security must accommodate both individual and enterprise interests.	Personal ethical requirements, as well as personal privacy as stated in regulations (e.g. Directive 95/46/EC, see section 2.2.2 of the present document) must be reverenced first.

4.4. Guidelines for developers

All of the above mentioned elements relating to privacy and data protection by design and by default, will be analysed in depth in D 5.2 'Legal and Ethical Requirements for the development of Dogana: Privacy by Design ', with the aim of integrating the user's experience in terms of deployment. The complexity of this engineering task demands caution against reducing methodologies to Privacy by Design into simple check-lists that can easily be ticked away for compliance reasons, while not mitigating some of the risks that Privacy by Design is meant to address.

Therefore, in this subsection, we will outline the main guidelines, to be taken into consideration when developing Dogana. In order to illustrate an example of how to embed techniques in order to develop systems according to the foundational engineering principle of Privacy by Design, which is data minimization, we refer to the Paper "Engineering Privacy by Design"[170]. In this paper, the researchers have tried to find a solution to the complex matter of implementing the principle of Privacy by Design , emphasizing on the fact that "the interpretation of Privacy by Design principles requires specific engineering expertise, contextual analysis, and a balancing of multilateral security and privacy interests" and proposed the following five steps, namely:

(1) Functional Requirements Analysis: The first step in the design of a system with privacy embedded at the core is to clearly describe its functionality. That is, the goal has to be well defined and feasible. Vague or implausible descriptions have a high risk of forcing engineers into a design that would collect more data, as massive data collection is needed in order to

[170] S. Gurses, C. Troncoso, and C. Diaz, Engineering Privacy by Design, K.U. Leuven/IBBT, ESAT/SCD-COSIC, 1-25.

guarantee that any more specific realization of the system can be accommodated by the design.

(2) Data Minimization: For a given functionality, the data that is absolutely necessary to fulfill the functionality needs to be analyzed. This activity includes a survey of state-of-the-art research to explore which data can be further minimized, as well as an evaluation of alternative architectures, e.g., distributed, centralized, that could contribute to data minimization. In most cases, the solutions rely on advanced privacy-preserving cryptographic techniques like the anonymous credentials or cryptographic commitments used in our case studies.

(3) Modeling Attackers, Threats and Risks: Once the desired functionality is settled and the data that will be collected is specified, it is possible to start developing models of potential attackers, e.g., curious third parties, the service provider; the types of threats these attackers could realize, e.g., public exposure, linking, profiling.

(4) Multilateral Security Requirements Analysis: Besides the system's purpose itself, an engineer must account for other constraints that ensure the security and correct behavior of the entities in the system, as expected by the different stakeholders of the system. The inclusion, analysis and resolution of these conflicting security requirements are also known as multilateral security. The objective of this analysis is to find a design in which privacy measures cannot be detrimental to other important security objectives such as integrity, availability, etc. and vice versa.

(5) Implementation and Testing of the Design: The final step in the design of the system is to implement the solution that fulfills the integrity requirements revealing the minimal amount of personal data. Further, the potential vulnerabilities have to be scrutinized, and the functioning of the system according to the articulated functional requirements has to be validated.

Another example of embedding the Privacy by Design principle can be drawn from the Paper "An innovative and comprehensive framework for Social Vulnerability[171]", which is about evaluating risks through a specific type of vulnerability assessments.

(1) According to this paper, the first operation is the "setup phase" of SDVAs, with the purpose "to involve only the strictly required stakeholders, explain the threat, share the objectives, define the scope of the assessment, obtain agreement and retrieve the needed information". The most important output of this phase is to share the objectives and the scope of the activity, in particular the boundaries of the assessment and regarding the spear phishing attack simulation phase, usually performed by email, the level of contextualization of the hooks and the definition of the employees' sample.

(2) The next phase is the "Passive Social Information mining", where there is a simulation of an attacker seeking information about the employees of a company, published mainly on Social Media in order to gain knowledge of potential victims for creating an effective attack. In order to respect the employees involved in the SDVA and to avoid legal problems, only passive

[171] An innovative and comprehensive framework for Social Vulnerability Assessment, E. Frumento & R. Puricelli, »In Depth Security – Proceedings of the DeepSec Conferences«, edited by Stefan Schumacher and René Pfeiffer, Gegründet 2011 | ISSN: 2192-4260.

scanning at the level of the company's brand is used. Due to legal constraints, the employer cannot know the identities of whom illicitly shared information on the Social Media, hence the results collected were properly anonymised.

(3) In the next phase of "Spear Phishing attack simulation", and since it was necessary to track the user behaviour, each email managed by the system was completely anonymous, in compliance with the most important requirement of the assessment methodology, namely to prevent the identification of the employees who fall victim of the hook and therefore, only statistically anonymized results are allowed. In conclusion, this paper demonstrates how the Privacy by Design principle was considered from the very outset of the development of the project, as well as during all its phases.

Therefore taking into account the above mentioned elements, when developing Dogana, the following recommendations should be taken into consideration[172]:

Table 4 'Guidelines for the development team'

Collect laws, regulations and applicable standards that the Dogana implementation has to cope with, including correct versioning and documentation policies.
Know the Threats Model applicable to Dogana.
Establish secure and reliable software development procedures, possibly adopting an iterative design method along, adopting a secure design pattern.
Provide secure and reliable changes management and review procedures.
Establish a secure and reliable software acceptance and deployment procedures.
Ensure reliable Dogana project's data and information handling.
Ensure physical security of data and assets, including data access control and data backup/lifetime management.
Describe the purposes aimed and the functions delivered (e.g. company information security) for all elements included in Dogana.
Use anonymisation and pseudonymisation techniques, as well as decentralised storage of personal information.
Provide data protection as a default setting (e.g. without any actions by individual users, but in automatic means), if possible.
Ensure the security, confidentiality, and integrity of personal data throughout the lifecycle of the processing activities (e.g. via encryption).
Ensure that the system informs the users about the collection and processing of their data, the further use, disclosure, etc. before the data are collected.
Ensure that the system remains reasonably transparent and subject to independent verification.

[172] Y.S. Van Der Sype, E. Frumento, and Z. Hodaie, "Legal Privacy and Data Security Requirements for the MUSES Platform", MUSES project, 59.

5. LEGAL AND ETHICAL CHALLENGES FOR INVOLVING HUMAN PARTICIPANTS IN THE DOGANA PROJECT

5.1. Relevance for the project

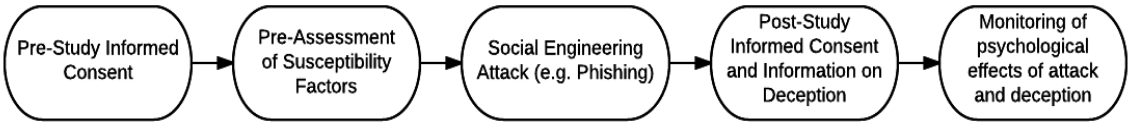
As it is essential for Innovation Actions (Horizon 2020) to have large and close to real-life tests, real humans will participate in the trials. This results in multiple ethical and legal concerns, regarding especially the privacy and data protection rights of the participants. Dogana will be developed in respect of the ethics requirements, as foreseen in the European Commission's guidelines regarding FP7 projects[173].

The analysis of the legal and ethical challenges, as well as specific guidelines for the involvement of human participants in trials and testing for the project of Dogana, will be provided in D 5.4 'Legal and ethical requirements for the development of Dogana, human participation, trials and testing'. In this section, a general description of the legal and ethical challenges will be outlined.

5.2. Legal and ethical issues related to trials and testings

5.2.1. Use-cases and user-studies:

AIT will perform several user studies, in which companies will be attacked, with the aim to determine which factors contribute to the susceptibility to fall for social engineering attacks. Participants in the studies will be the partners of Dogana, as well as external companies recruited by AIT. The user studies will be performed according to the following scheme:[174]



Therefore, the legal and ethical issues related to the use cases and user studies are the following:

- Pre-Study Informed Consent: Participants will receive a pre-study informed consent form, in which they will consent to participate in studies about "ICT at the workplace", covering diverse aspects such as health, wellbeing, safety, security, culture. The pre-study informed consent will not disclose information about the real intention of the study, which is to attack people with social engineering methods and to assess their susceptibility to these attacks and the factors that determine this susceptibility.

- Pre-Assessment of Susceptibility Factors: Participants will receive a link to an online questionnaire, in which the factors potentially contributing to the susceptibility to fall for social engineering attacks will be assessed. Since characteristics, such as age, sex, gender organizational/social position and country-specific factors, which constitute sensitive personal data will be assessed; therefore, stricter data protection requirements have to be considered, especially regarding to consent. Also, the procedures

[173] In accordance with the guidelines for ethics of the European Commission regarding FP7 projects http://ec.europa.eu/research/participants/portal/desktop/en/funding/reference_docs.html#fp7.

[174] M. Busch, 'Psychological SE framework', D 4.2, Dogana, 2016.

and the criteria that will be used to identify and recruit participants, as well as the prevention measures to avoid recruiting potential vulnerable individuals must be further specified.

- Post-Study Informed Consent: Participants will receive a written explanation of the actual goal and procedure of the study and will have the right to withdraw their data from the study.

In this point, it is important to remind the basic legal requirements regarding the legal notions of use of personal data. Firstly, one must specify if it is about "normal" personal data or "special categories"[175] of personal data. In practice, the difference between dealing with personal data and special categories of personal data concerns the legal grounds based on which the personal data may be processed. Also, the different formulation of Article 8 (1) of the Data Protection Directive and Article 7 of the Data Protection Directive, "Member States shall prohibit the processing of […] data concerning health […]" versus "Member States shall provide that personal data may be processed only if", indicates that the interpretation of the data processing principles need to be more restrictive with regard to the special categories of data opposed to "normal" personal data. This restrictive interpretation is also in accordance with Article 6 of Convention 108, which stipulates that "personal data concerning health may not be processed automatically unless domestic law provides appropriate safeguards".

Regarding the use of primary data for research, meaning when personal data relating to health are originally collected for research purposes, one will often have to rely on the consent of the patient[176]. As stated above, participants will receive a pre-study informed consent form, in which they will consent to participate in studies about "ICT at the workplace", covering diverse aspects such as health, wellbeing, safety, security, culture. Since "special categories of data" will be included, therefore, informed consent is required.

Regarding secondary use of data for research, meaning the use of data which are already available for the data controller or for a third party, personal data originally collected for a specific purpose can be re-used / further used for another purpose without needing a new legal ground, such as a new informed consent, under the condition that this secondary purpose is compatible with and coherent to the original purpose of the data processing.[177] With regard to the further processing of data for research the Data Protection Directive already assumes further processing for historical, scientific and statistical research is not incompatible with the original purpose. Nevertheless, the Article 29 Working Party warned that this provision "should not be read as providing an overall exception from the requirement of compatibility, and it is not intended as a general authorisation to further process

[175] Recital 26 of the 2015 Proposal for General Data Protection Regulation specifies a number of categories that they should be protected as sensitive data: Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject; including information about the individual collected in the course of the registration for and the provision of health care services as referred to in Directive 2011/24/EU to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; information derived from the testing or examination of a body part or bodily substance, including genetic data and biological samples; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

[176] Article 8 (1) of the Data Protection Directive.

[177] Article 6 (1) b) of the Data Protection Directive states that With regard to research data protection law specifies that research for scientific, historical or statistical purposes shall not be regarded incompatible provided that the necessary safeguards are imposed by Member State law.

personal data in all cases for historical, statistical or scientific purposes"[178]. However, this remains a case-by-case appreciation. Additionally, the Directive clarifies that further use for scientific, historical or statistical research can only be considered compatible if compliant with Member States" specific safeguards.

Compared to the Data Protection Directive, the GDPR mentions that further processing for scientific, historical and research purposes shall not be considered incompatible with the initial purposes. Furthermore, Article 83 makes explicit the conditions for the assessment of the compatible use, introducing the following tiered system.

Table 5 'Tiered system'

When the purpose of the research can be fulfilled by further processing, data which do not permit or do not any longer permit the identification of data subjects, the research should be fulfilled in this manner.
In respect of the data minimisation principle, pseudonymisation can be included as a technical measure, as long as it allows the purpose of the research to be met.
If pseudonymisation does not allow the purpose of the research to be met, other appropriate safeguards – technical and organisational measures - should be put in place to protect the rights and freedoms of data subject, which is for the Member States to define what exactly these appropriate safeguards should be.
Under the national regime for research, Member State law may also foresee derogations to the right of the data subject to access data processed on him, the right of the data subject to request rectification, the right of the data subject to restrict processing, and the right of the data subject to object unless the research is of significant public interest.[179]

5.2.2. Field trials with end-users

Dogana will implement field-trials with six users. The four users, as partners are Gabinete Nacional de Segurança (GNS), Regia Autonoma de Transport Bucuresti (RATB), Hellenic Ministry of Defence (HMOD), and Danish Institute of Fire and Security Technology (DBI). The two additional supporting users providing a link to the financial world will be ENI and Poste Italiane. The delivery of the framework at the end of the project will be the means of verification. WP7. 'Field-trials' will assess and demonstrate the effectiveness of the released framework in real-life conditions against a group of selected end-users. Dogana will only include participants from the users in the field trials. The individual volunteers will be identified by the human resource departments from the above mentioned partners. Consequently, no external participants will be involved, while minors and members of vulnerable groups will be explicitly excluded from recruitment.

[178] Article 29Working Party, Opinion 03/2013 on purpose limitation, WP203, adopted on 2 April 2013, 28.

[179] Regarding the margin of appreciation, Member States are allowed to foresee diverging, specific procedures for the exercise of data subjects' rights. They may foresee technical and organizational measures aimed at minimizing the processing of personal data in pursuance of the proportionality and necessity principles. They may set conditions for research based on the coupling of information from different registries. And finally Member States should set specific conditions to the publications or otherwise disclosure of personal data in the context of scientific research.

As part of D7.2 'Set-up of the field trial plan', before the beginning of trials, each user involved in the execution of SDVAs will document the general criteria that will guide their assessments, including the criteria for recruitment/involving that they will use. According to WP7. 'Field-trials', there will be pairs of partners closely working together that will be created in D7.1. 'Assembling of the Dogana framework'. This is also documented in the description of D7.3 "Field trial execution', where the SDVA tests will be executed and tracked by the couples' tech partner – end-user which have been created in D7.1. The execution of the SDVA tests and the recruitment of individuals will be handled by each couple, using the general Dogana results. This is an additional security measure added by Dogana to ensure that only trusted partner(s) will have access to the systems of the user.

The legal and ethical concerns regarding user involvement in field trials is often related to the evaluation of the assets each employee handles. Therefore, according to the specificities of an employee's job position, there are different types of vulnerabilities. The category and the number of the employees chosen to take part in the field trials is a direct consequence of the perception of risk and the weakness of the asset. Therefore, measures have to be implemented to avoid a possible profiling of the employees. Moreover, after the SDVA has taken place, the release of the results raises new potential vulnerabilities. In other words, the relation of trust among employees and employers will be jeopardised. In order to tackle this challenge, specific guidelines will be provided in D 5.4. 'Legal and Ethical Requirements for the development of Dogana: human participation, trials and testing', taking into account the criteria as provided by the legal framework outlined in the present deliverable, such as prohibition of profiling, special categories of data etc.

5.3. The concept of deception in research

The essential aim of the social engineering attacks risks targeted by Dogana, is to trick employees and to force them to violate a company policy. The Dogana research involves the development of technologies or the creation of information that could have severe negative impacts on human rights standards (e.g. privacy, discrimination, etc.), if misapplied. Research with severe negative impact on human rights could relate to research on surveillance technologies, new data-gathering and data-merging technologies.

It is important to emphasise on the fact that Dogana is based on the concept of deception, which could generate ethical concerns. Nevertheless, deception is the only way for assuring that there will be no bias of the employees during the assessment of their vulnerability.

According to the research paper of Finn and Jacobson,[180] digital penetration tests have an indirect interaction between the penetration tester and the employees, therefore reducing the ethical impact to a minimal level, by comparison to a physical penetration. Also, in social research, the Bellman report[181] defines the ethical guidelines for the protection of humans in testing. In addition, the table below shows the four justifications that need to be satisfied in order to use deception in research:[182]

Table 6 'Deception in research'

[180] P. Finn and M. Jacobson, Designing ethical phishing experiments, Technology and Society Magazine, 2007, 46-58.

[181] The National Commission for the Protection of Human Subjects of Biomedical and Behavioral research, "The Belmont report: Ethical principles and guidelines for the protection of human subjects of research", 1978, 18.

[182] P. Finn, "The ethics of deception in research", Indiana University Press, 1995, 87-118.

The assessment cannot be performed without the use of deception. **The knowledge obtained from the assessment has important value.** **The test involves no more than minimal risk[183] and does not violate the rights and the welfare of the individual.** **Where appropriate, the subjects are provided with relevant information about the assessment after participating in the test.**

5.4. Risk mitigation actions

In order to be compliant with the ethics requirements, risk mitigation actions are required. For example, in the development of the project the following can be foreseen, namely, the undertaking of a human rights impact assessment, the involvement of human rights experts in the research, training of personnel and/or technological safeguards, and cautiousness when publishing or otherwise disseminating those results, e.g. through Privacy by Design. If applicable, also documentation of copies of ethics approvals.

The outcome of the Dogana project could be of high-importance for potential hackers or criminals. Specifically in the context of social network-based attacks, the project results may have a high risk to be abused by terrorists or criminals. For this reason, the Dogana consortium foresees additional protection measures for the end-users being part of the consortium, whose data will be assessed during the trials. Therefore, copies of personnel security clearance documents should be obtained, when the project research has potential for malevolent, terrorist or criminal abuse and details on the measures to prevent abuse should be documented. Also, an ethics advisor/ethics advisory board should be appointed.

These risks can be minimised through a detailed set of actions, based on two main approaches: (a) sanitisation of what is published, considering the three different levels of sharing, and (b) technological protection of the tools for a controlled distribution of developed tools and the protection of data during the tests.

Table 7 'Actions for the partners of the Dogana project'

Action 1: Users and technical partners will be defined in the early phases of the tasks in order to create access restrictions. This ensures that no important data assets are shared outside the security zone. **Action 2:** Each user will review the trials reports closely in order to agree on the type of information reported. This ensures that the user retains full control on what information can be shared beyond the user security zone.

[183] Code of Federal Regulation states that: "minimal risk is defined as the probability and magnitude of physical or psychological harm that is normally encountered in the daily lives", 2005, 1–12.

Action 3: Each user will evaluate the data and information collected during the trials within WP7 with the corresponding partner and properly anonymise it considering three different sharing levels: inside the consortium, with the European community, public documents.

Action 4: Dogana will study a proper code distribution methodology to control the threat of a developed SDVA technical framework becoming an abused way of performing socially enabled attacks'.

Action 5: The SDVA platform will be also actively protected by a potential intrusion or defacing during the execution of the tests, in order to avoid stealing of data during the execution of tests and before their destruction.

5.5. Criteria for the development of guidelines

In this sub-section the relevant elements to be taken into consideration for the creation of specific guidelines will be briefly outlined, since this work will be in depth carried out in D.5.4. 'Legal and Ethical Requirements for the development of Dogana: human participation, trials and testing', where legal guidelines for Dogana partners involved in the testing stages will be provided.

In particular, within the project, volunteers will be involved for social sciences studies. Therefore, the details on recruitment, inclusion and exclusion criteria, as well as informed consent procedures must be provided. It is important to note that for the purposes of the development of Dogana, persons unable to give informed consent[184], vulnerable individuals, children or patients will not be recruited and that therefore, no additional approvals should be obtained.

Also, the used research methods will not result in discriminatory practices or unfair treatment.[185] In addition, the ethical implications of the chosen methodologies must be clarified (e.g. on surveys, questionnaires, interviews, standardized tests, direct observation, ethnography, recordings, etc.). Moreover all activities relating to the processing of personal data, will be taken in compliance with all above mentioned legal requirements (consent, purpose, duration of storage, anonymisation methods etc.).

Therefore, in case personal data are processed in the project, according to the ethics issues table[186] the following information will be provided to human participants[187].

Table 8 'Information to human participants'

[184] The EU Framework Programme for Research and Innovation HORIZON 2020 of July 11, 2014, "How to complete your ethics Self-Assessment" http://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-fetopen-2014-2015-ria/1660136-1645175-h2020_-_guidance_ethics_self_assess_en.pdf, 9, last visited on 11 March 2016.

[185] The EU Framework Programme for Research and Innovation HORIZON 2020 of July 11, 2014, "How to complete your ethics Self-Assessment" http://ec.europa.eu/research/participants/portal/doc/call/h2020/h2020-fetopen-2014-2015-ria/1660136-1645175-h2020_-_guidance_ethics_self_assess_en.pdf, 10, last visited on 11 March 2016.

[186] The EU Framework Programme for Research and Innovation HORIZON 2020 of January 10, 2013.

[187] Y.S. Van Der Sype, Internal legal and ethical compliance check, D 1.3, Dogana, 2016.

Description on the procedures for data collection, storage, protection, retention, transfer, destruction, or re-use (including collection methodology (digital recording, picture, etc.), methods of storage and exchange (LAN, cloud, etc.), data structure and preservation (encryption, anonymisation, etc.), data-merging or exchange plan, commercial exploitation of data sets, etc.).

Description of the data safety procedures (protective measures to avoid unforeseen, usage or disclosure, including mosaic effect, i.e. obtaining identification by merging multiple sources).

Confirmation that informed consent has been obtained.

Description of (any) data transfers to third countries (type of data transferred and recipient country).

Copies of notifications/authorisations for the collection and/or processing of the personal data (if required), e.g. authorisation for (any) data transfer from the competent data protection authority.

Informed consent forms, information sheets and other consent documents (opt in processes, etc.).

If the research involves the collection or processing of sensitive personal data (e.g. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction), a copy of notification/authorisation for processing of sensitive data should be obtained.

If the research involves tracking or observation of participations (e.g. surveillance or localisation data), the details on methods used for tracking or observing participants must be documented and a copy of notification/authorisation for tracking observation should be obtained, if required.

6. CONCLUSION

This deliverable provided an overview of the legal and ethical implications of Dogana. In particular, the applicable legal framework for the project of Dogana was provided, with the aim to guide the consortium for the development of Dogana, as well as for the implementation of Dogana in the companies.

Legal and ethical compliance is crucial for the development of the Dogana project. The ethical and legal considerations are not only an aspect to be assessed during the project, but they constitute part of the research results, legal and ethical guidance. Therefore, they are included in the workflow from within the early stages of the project. The main challenge regarding the set-up of the Dogana project is how to ensure the legal compliance of the tests, while guarantying that no abuses to the employees will take place, Since traditional methods for consent gathering complicate the execution of SDVAs, due to the fact that a prior consent would insert a bias in the testing process, therefore, one of the main challenges of the Dogana is to establish a balance between realistic attack simulation and respect of legal and ethical requirements.

Moreover, legal and ethical challenges are also entailed regarding the implementation of the Dogana solution in the organisational settings. An example of this challenge can be demonstrated in the case when the investigation addresses how employees behave and how this behaviour places the company's security at risk, in order to assess the resilience of the employees against socially engineered attacks. Therefore, a certain level of interference with the private lives of employees will be unavoidable. As a result, the problem in legal terms is how to reconcile two equally important obligations, namely the employer's obligation to secure its companies data, in respect of the security principle on one hand, and the obligation to respect of privacy and of its employees, on the other.

This deliverable contributed at identifying the legal and ethical hurdles and provided the initial elements for a further and in-depth analysis of these issues in the future deliverables, namely in D 5.2 'Legal and Ethical Requirements for the development of Dogana: Privacy by Design', the ethical and legal challenges for conducting SDVAs in organisational settings will be provided, while in D 5.3 'Legal and Ethical Requirements for the development of Dogana: organisational context setting', the legal challenges for developing a privacy-friendly Dogana framework will be described and in D 5.4 'Legal and Ethical Requirements for the development of Dogana: human participation, trials and testing', the legal challenges for involving human participants in the Dogana project will be analysed. The output from this task will be further applied and specified from the different viewpoints of the relevant stakeholders during the lifetime of the project.

7. REFERENCES

Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, WP48, 4; Working document on the surveillance of electronic communications in the workplace, adopted on 29 May 2002, WP55, 7; Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, WP187, 1-38.

A. Cavoukian, Privacy and security by design: a convergence of paradigms, 2013, 2.

B. Schneier, The Human side of Heart Bleed, The Mark News, 2014, https://www.schneier.com/blog/archives/2014/06/the_human_side_.html.

European Data Protection Supervisor, Comments on selected issues that arise from the IMCO Report on the review of Directive 2002/22/EC and Directive 2002/58/EC (ePrivacy), 2008, 1-13.

E. Frumento, R. Puricelli, An innovative and comprehensive framework for Social Vulnerability Assessment, In Depth Security – Proceedings of the DeepSec Conferences, 2011, 2192-4260.

F. Swiderski, W. Snyder, Threat Modeling, Microsoft Press, 2004, 65-68.

F. Dorssemont, K. Lörcher, I. Schömann, The European Convention on Human Rights and the Employment Relation, Bloomsbury Publishing, 482, 2013.

H. Simon, The Sciences of the Artificial, MIT Press, 1996, 241.

L. Tam, M. Glassman, M. Vandenwauver, The psychology of password management: a trade-off between security and convenience, Behav Inf. Technol, 2010, 233–244.

M. Huber, S. Kowalski, M. Nohlberg and S. Tjoa, Towards Automating Social Engineering Using Social Networking Sites, International Conference on Computational Science and Engineering, 2009, 1-8.

M. Warkentin, and R. Willison, Behavioral and policy issues in information security systems: the insider threat, European Journal of Information Systems, 2009, 90-101.

N. Stanley, EU compliance and regulations for the IT security professional, White Paper Bloor Research, 2009, 7.

P. De Hert and H. Lammerant, Study, Protection of Personal Data in Work-related Relations, 2013, 1-77.

P. Finn and M. Jacobson, Designing ethical phishing experiments, Technology and Society Magazine, 46–58, 2007.

P. Finn, The ethics of deception in research, Indiana University Press, 1995, 87–118.

R. Gowtham, I. Krishnamurthi, A comprehensive and efficacious architecture for detecting phishing websites, 2014, 23–37.

S. Furnell, Still on the hook: The persistent problem of phishing, 2013, 7–12.

S. Gurses, C. Troncoso, and C. Diaz, Engineering Privacy by Design, K.U. Leuven/IBBT, ESAT/SCD-COSIC, 1-25.

S. Maguire, Debugging the Development Process, Microsoft Press, 1994, 50.

T. Dimkov, W. Pieters, and P. Hartel, Two methodologies for physical penetration testing using social engineering, University of Twente, 2009, 1-11.

W. Curtis, H. Krasner, N. Iscoe, A Field Study of the Software Design Process for Large Systems, 1988, 1268–87.

W. Royce, Managing the development of Large Software Systems: Concepts and Techniques, 1970, Proceedings IEEE WESCON.

Y.S. Van Der Sype, On the road to privacy-friendly security technologies in the workplace, Muses RT2AE V P/DP, CPDP 2016.