ADVANCED SOCIAL ENGINEERING AND VULNERABILITY ASSESMENT FRAMEWORK

D5.2 – Legal Requirements for Privacy by Design

Work Package:	WP5
Lead partner:	VIS
Contributing Partners:	GNS, ENG, INOV, KUL, HP, ELTA, RATB
Author(s):	Filipe Custódio
Submission date:	06/06/2016
Version number:	1.2 **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)	

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

Revision History

Revision	Date	Who	Description
0.1	15/01/2016	Filipe Custódio (VIS)	Initial template and TOC
0.2	23/03/2016	Filipe Custódio (VIS)	Document structured after analysis of D5.1
0.3	02/05/2016	Filipe Custódio (VIS)	Input from KUL
0.4	25/05/2016	Filipe Custódio (VIS)	Input from INOV
0.5	26/05/2016	Filipe Custódio (VIS)	Input from ENG and KUL
0.6	27/05/2016	Filipe Custódio (VIS)	Input from ELTA. Final draft.
1.0	31/05/2016	Filipe Custódio (VIS)	Review by CNIT.
1.1	02/06/2016	Filipe Custódio (VIS)	Review by DBI.
1.2	06/06/2016	Filipe Custódio (VIS)	Privacy and Ethics Review. Final version.

Quality Control

Role	Date	Who	Approved/Comment
Quality Control	31/05/2016	Alessio Mulas	Review by CNIT
Quality Control	01/06/2016	Dennis Hansen	Review by CNIT

Disclaimer:

Table of Contents

List of Figures

List of Tables

Definitions and acronyms

CC	CyberConnector
CyberConnector	An internal knowledge collaboration site and social network that is used to share all the information among partners. Referred to also as CC.
DOW	Description of Work
MST	Management and Support Team
PbD	Privacy By Design
PC	Project Coordinator
SC	Scientific Coordinator
SDVA	Social Driven Vulnerability Assessment
ECHR	European Convention on Human Rights
GDPR	DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL – General Data Protection Regulation

1. Executive Summary

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. Social Driven Vulnerability Assessments (SDVA) are social engineering attacks performed by request of an organization to detect if it is vulnerable to these threats. DOGANA aims to develop a toolset that can automate these assessments to maximize their effectiveness while reducing the impact on the privacy of the organizations' employees, by reducing human intervention in the process.

This document contains an analysis of personal data that has to be used by DOGANA's Use Cases, a definition of purposes and functionalities that must be achieved by the system, legal principles and requirements to be followed in order to comply with data protection regulations.

The analysis results in a set of security policies that must be implemented by an organization to implement DOGANA-based SDVA systems.

2. Introduction

From the DOW: *"This task will analyse the legal and ethical requirements to which the DOGANA system must comply. It approaches the legal and ethical aspects in DOGANA from the developers' point of view, integrating the users expertise in terms of deployment."*

Data protection controls can be divided into two groups; technical and procedural controls. Technical controls are implemented by the DOGANA system and, according to the Privacy by Design principle, must be considered since the earliest stages of system's development. Procedural controls, on the other hand, apply to human processes and are usually applicable in the deployment and usage stages of the DOGANA system.

This deliverable will focus on the technical aspects of security, such as encryption, data traceability and security by default systems, whilst D5.1 and D5.3 address the rules and procedures related to human processes, such as obtaining consent, informing users and handling the outputs of the DOGANA tools.

The goal of this document is to map the Privacy by Design principles, legal and ethical requirements and functional requirements, of the DOGANA project, to technical controls that can ensure the system's compliance during each stage of data collection, processing, storage and communication. To this end, the methodology described in chapter 3 will be followed, resulting in a set of security policies that group the technical security controls for each of the considered data sets.

3. Methodology

The aim of this report is to define security requirements to be observed in DOGANA, using as input: relevant ethical and privacy issues, legal requirements in the EU space and in the selected member states, where DOGANA pilots will be conducted and the Privacy by Design principles. The output will be a set of security controls that allow full compliance of the DOGANA project with legal, ethical, and privacy requirements.

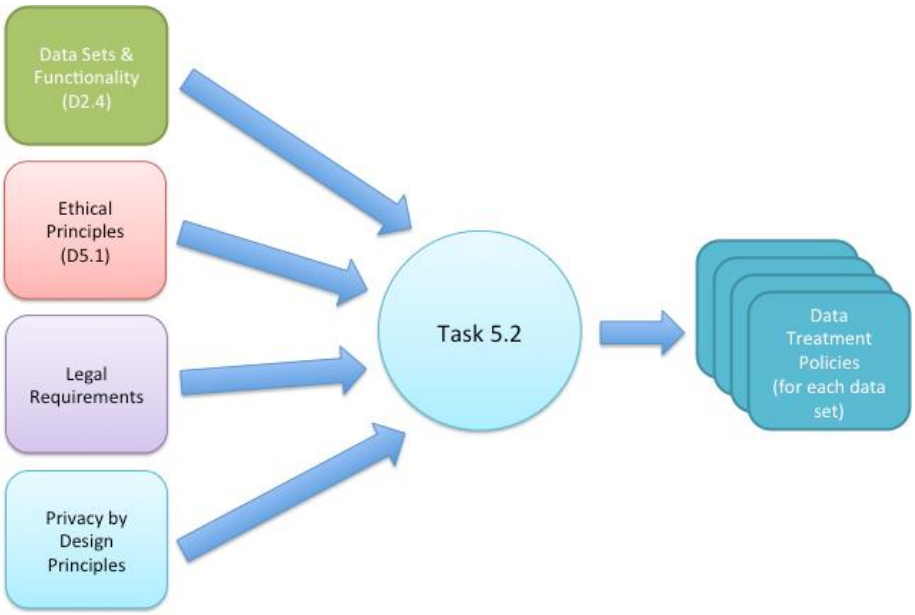

Figure 1: Methodology

Each of these inputs and outputs is described in detail in the following sections.

3.1. Data Sets & Functionality

"Data Sets" are defined as types of data that will be processed by DOGANA. This data may have different degrees of protection by law, and may have different levels of privacy implication. For the purpose of DOGANA, personal data belonging to the targets of the social engineering vulnerability assessments will be collected, processed and stored, including:

- Identification information, such as name, e-mail address, role in the organization;
- Pre-assessment of susceptibility factors, including psychological profile, hobbies and other interests;
- Social engineering attack results, which include whether or not a person successfully clicked a link in a phishing e-mail;
- Information on deception success, namely if a person divulged information as a result of a deception attempt;

- Psychological effects of attack and deception results, including the results of post-assessment questionnaires.

These major data groups may be further divided, if necessary, into smaller ones, according to the type of information collected and its privacy implications. For instance, the "susceptibility factors" may have different grades of intrusion into the subjects' personal live, and thus a finer grade of subgroup division may be necessary, such as "age, gender specific information", "health and lifestyle", "political opinion", etc.

Regarding functionality, the following major groups of data handling actions are considered for the purpose of this study:

- Data collection – actions that identify, receive and feed information into the DOGANA system;
- Data processing – any data handling function where information is processed within the DOGANA system;
- Data storage – recording of information within the DOGANA system for later processing, subject to data retention policies and access control;
- Data transfer – output of information from the DOGANA system, either in the form of reports or communications with other systems.

The data sets and functionality considered in the DOGANA system are documented in chapter 4 - Data sets and functionality of DOGANA.

3.2. Legal and Ethical Principles

This section handles the legal and ethical principles of DOGANA, with input from the D5.1 deliverable. For the purpose of this deliverable, the goal of this section is to identify rules, ethical and privacy boundaries that must be taken into account within DOGANA: both in the implementation of all required functionalities and in all general data handling activities of DOGANA.

These ethical rules will be analysed with regard to each of the types of information being handled in DOGANA, to make sure that:

a) The information being collected and processed in DOGANA does not infringe any legal and ethical principles of the project;
b) A justifiable/reasonable/righteous balance between security benefits and privacy risks is achieved.

To this end, we have to consider different legislations, including:

- International, EU and national law (for example Article 8 of the ECHR[1], Article 7 and 8 of the EU Charter[2]),
- Public law, criminal law and civil law of the countries where DOGANA will be implemented (fundamental rights, communication secrecy, privacy laws),
- Legislation focusing on substantive guarantees versus legislation on procedural requirements for processing of personal data,
- Workplace-specific collective bargaining agreements versus generic rules (not specific to the workplace).

Important is also the difference between privacy and data protection. While the protection of the private life (Article 8 ECHR and Article 7 EU Charter) guarantees the protection of private life, but justification for interference is possible when the legality-legitimacy and proportionality principle are met, data protection prescribes requirements for each processing of personal data, regardless of the professional atmosphere of the processing of the data. As the professional atmosphere merely impacts the data protection requirement on the legal ground, you need to have a reason in order to process personal information.

Some of the data sets defined in chapter 4 - Data sets and functionality of DOGANA, might be an issue for privacy, but not for data protection. For example, the opinion of an employee on his employer is something that is typically solved by a balancing act between freedom of expression and the right to respect for private life and does not fall inside the scope of data protection.

These principles and privacy requirements are documented in chapter 5 - Legal and Ethical Principles of DOGANA. The analysis, which will result in data-set specific security policies, is documented in chapter 8 - Security Policies.

3.3. Legal Requirements

This task will identify, based on DOGANA's data sets and functionalities, what the applicable legal requirements are, taking into account EU law and member state laws in the territories where the pilots are being conducted.

The result of this analysis is documented in chapter 6 – Legal Requirements.

3.4. Privacy by Design Principles

This task will define, within the scope of the identified data sets and functionality of DOGANA, how the principles of Privacy by Design are implemented.

The result of this analysis is documented in chapter 7 – Privacy by Design Principles.

---

1 European Convention on Human Rights - https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/Convention_ENG.pdf

2 EU Charter of Fundamental Rights - http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm

3.5. Data Treatment Policies

Finally, a set of security policies are defined, that map all the requirements to actual security controls to be implemented in the system.

The data treatment policies are documented in chapter 8 – Security Policies.

4. Data sets and functionality of DOGANA

This chapter documents the information being handled by the DOGANA system.

4.1. Categories of Data

Data handled by the DOGANA system is categorized according to its relevance to the individual rights of its owner. To this end, the following categories are used:

Data Category	Description
Purely Professional	Purely professional information about employees (of which the professional nature is not questionable), regardless if the data can be considered as personal data or not. This category contains information such as data on the individual that is directly related to his or her professional life or the company they work for, such as professional e-mail and contacts, role within the organization, and other information which belongs to the company such as security codes, usernames and passwords.
Semi-Professional	Semi-professional information. This is information that, although not related to the private life of an individual, it is also not directly related to his or hers direct employer. The following elements are considered as belonging to this group: curriculum vitae, membership in professional social sites such as LinkedIn, technical discussion forums, etc.
Private Information: Publicly available	Publicly available private information - information published in social media and available to everyone.
Private Information: Semi-publicly available	Semi-publicly available private information - information published for a restricted group. This is usually information published in social media networks that is only accessible by invitation or by a restricted group of people.
Private information: Not publicly available, not sensitive	Non-published private information, which is not sensitive. Within this group is information, which is private and is not published with the consent of the owner. However, this information is not considered sensitive. Examples of such information is identification, address, interests and non-political affiliations, etc.

Data Category	Description
Private information: Not publicly available, sensitive	Non-published private information, sensitive as per the Regulation (health data, religion, political affiliation, etc.)

Table 1 - Data Categories

4.2. Data sets & Purpose

This section documents the information groups or data sets that are used withinDOGANA system and their purpose.

Data Set	Category	Purpose
DS.001 - Identification information (name, e-mail)	Purely Professional	Information on the individual, to be mapped with other sources of information for OSINT purposes.
DS.002 - Role in the target organization	Purely Professional	Information for SE targeting purposes - to identify higher value targets within the organization, or to provide context for phishing attacks.
DS.003 - Professional online presence (LinkedIn, Blogs)	Semi-Professional	To gather information that will allow a more successful SE attack, such as contextual information on the person's skills and interests.
DS.004 - Personal online presence (Facebook, LinkedIn, Blogs): Publicly available	Private Information: Publicly available	Employees often access their personal emails or social media accounts from office facilities. They also take care of personal business during working time using company resources such as phone, computers, etc.. This is a relevant SE attack surface to an organization and a main subject on an awareness evaluation framework. Thus, online private information should be gathered and used to define trustworthy pretexts for SE attacks within DOGANA vulnerability assessments tests. This information will be used to create a psychological profile based on public posts.
DS.005 - Personal online presence (Facebook, LinkedIn, Blogs): Restricted to groups (friends)	Private Information: Semi-publicly available	Not usable.

Data Set	Category	Purpose
DS.006 - User accounts & Passwords (credential harvesting)	Private information: Not publicly available, sensitive	Credential harvesting is a main threat from SE attacks and it should be included in the DOGANA vulnerability assessment tests. The goal of this data set is to allow impersonation attacks, and to access company IT Systems.
DS.007 - Hobbies and special interests - published information	Private Information: Publicly available	The same as pointed out for DS.004. Also, this kind of information is valuable when a Social Engineer is trying to establish a relationship with the employee, as it can be used as a pretext to a cold contact or to increase the likeability and empathy. Used for psychological profiling.
DS.008 - Hobbies and special interests - non-published information	Private Information: Semi-publicly available	Not usable.
DS.009 - Affiliations (political causes)	Private Information: Publicly available	Not usable.
DS.010 - Online relationships	Private Information: Semi-publicly available	This is valuable information as it significantly increases the trustworthiness from online contacts and phishing suggestions (spoofing the origin of the contacts - e.g. e-mail address) Used to gather information concerning groups, contacts relationship to help in attacks, which require connection and relationship.
DS.011 - User rights & roles (who has access to what)	Purely Professional	To focus the attacks on key people. To assess the awareness to SE per role.
DS.012 - Access codes for safety systems	Purely Professional	To assess the security of the systems.
DS.013 - Knowledge (professional CV)	Semi-Professional	Profile and background.
DS.014 - Sensitive Information (religion, health, etc.) that may allow employees to be blackmailed	Private information: Not publicly available, sensitive	Not usable.

Data Set	Category	Purpose
DS.015 - Opinion on their employer (to be able to identify potential disgruntled employees)	Private Information: Semi-publicly available	To assess the security of the systems.
DS.016 – Location of offices	Purely Professional	Location of target's offices can be used for a more successful spear phishing attempt by using this information as part of the message to the target.
DS.017 – Location of target	Private Information: Not publicly available, not sensitive	Real time target location can be used for a more successful spear phishing attempt either by using this information as part of the message to the target or by designing the message based on location.
DS.018 - Photos of the personal life of the target	Private Information: Publicly available	Photos obtained from social networks may contain information on names of friends and family (via tags) as well as events attended by the victim.
DS.019 – Analysis Results	Purely Professional	Results of the SDVA study.

Table 2 - DOGANA Data Sets

4.3. Mitigation Actions

This section identifies actions and rules that can be used to limit the impact on the individual during collection, processing and storage of the data.

During data collection, the following mitigation actions will be used:

Mitigation Action	Data Sets	Related policies (chapter 8)
When collecting e-mails, restrict the collection to professional e-mails, meaning only the official employer's e-mail domain should be considered.	DS.001	SP.014 – Professional contacts
Don't collect multimedia contents	DS.004 DS.007	SP.013 – Data Minimization
Don't collect the credentials. Instead get the time stamp and some information to be shown as evidence. If we adopt this mitigation measure, it will be impossible to use the result of this attack in a following stage.	DS.006	SP.017 – Collection of credentials
When collecting mobile numbers, restrict the collection to professional mobile numbers, meaning only the official employer's mobile numbers domain should be considered. The company could provide this data set.	DS.001	SP.014 – Professional contacts
When collecting information from online presence, collect only publicly available professional and semi-professional related information, if sensitive information is available do not collect it.	DS.003 DS.004 DS.007	SP.015 – Publicly Available Information SP.013 – Data minimization
When collecting information regarding online relationships, only use this information if it is accessible to the public, without resorting to "fake profiles".	DS.010	SP.015 – Publicly Available Information
Collection of photos is only done from publicly available information.	DS.018	SP.015 – Publicly Available Information

Table 3 – Mitigation Actions – collection

During data processing, the following mitigation actions will be used:

Mitigation Action	Data Sets	Related policies (chapter 8)
Anonymised processing and use of pseudonyms; aggregate at the lowest possible level	All	SP.016 – Data Anonymisation
The aggregation level in the report should be specific enough to have interesting insights on one hand and general enough to ensure employees security on the other.	DS.019	SP.018 – Anonymisation of results

Table 4 – Mitigation Actions - processing

During data storage, the following mitigation actions will be used:

Mitigation Action	Data Sets	Related policies (chapter 8)
Staff from the organisation under test should not have access to this information.	All	SP.011 - Authorization
Separation of data, to support limitation and unlinkability (e.g. peer to peer networks); Assure Security safegards principle.	All	SP.007 – Data Security

Table 5 – Mitigation Actions - storage

5. Legal and Ethical Principles of DOGANA

This chapter documents the legal and ethical principles of DOGANA, which apply to all personal data to be handled by DOGANA system. Within the scope of this deliverable, we are only considering principles that apply to the data handling activities of DOGANA, from collection to processing, storage and communication activities.

Legal Principle[3]	Description	How these principles apply to DOGANA
Collection Limitation Principle	There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	DOGANA has policies regarding consent and collection limitation – see SP.001 and SP.006 in chapter 8.
Data Quality Principle	Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.	The data quality principle does not apply to social vulnerability assessments, as the collected information is only used for the development of social engineering attacks, and is not maintained after the end of the study.
Purpose Specification Principle	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	DOGANA has policies regarding consent and collection limitation – see SP.001 and SP.006 in chapter 8.
Use Limitation Principle	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with applicable data protection law except: a) with the consent of the data subject; or b) by the authority of law.	DOGANA has policies regarding consent and collection limitation – see SP.001 and SP.006 in chapter 8. These policies specify that data can only be used with the consent of the data subject.
Security Safeguards Principle	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.	DOGANA has a policy regarding the security requirements of the systems responsible for data storage and processing – see SP.007 in chapter 8.

3 Source: http://oecdprivacy.org

Legal Principle[3]	Description	How these principles apply to DOGANA
Openness Principle	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.	Policies supporting the openness principle are SP.002 and SP.008, which define that all data must be traceable within the system and that the data repositories must identify a person within the organization with the role of data controller. These policies are documented in chapter 8.
Individual Participation Principle	An individual should have the right: a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) To have communicated to him, data relating to him i) Within a reasonable time; ii) At a charge, if any, that is not excessive; iii) In a reasonable manner; and iv) In a form that is readily intelligible to him; c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.	The traceability policy (SP.002) ensures that the technical implementation of the system allows for data related to any individual can be traced within the system. The data controller nominated within the DOGANA system implementing organization as per policy SP.008 will ensure the individual participation principle is correctly implemented (SP.009) These policies are documented in chapter 8.
Accountability Principle	A data controller should be accountable for complying with measures, which give effect to the principles stated above.	The accountability principle is implemented in DOGANA through policies SP.008 (Data controller), SP.010 (Authentication), SP.011 (Authorization) and SP.012 (Accountability). These are documented in chapter 8.

Table 6 - Legal Principles of DOGANA

6. Legal Requirements

In this chapter, we analyse the legal requirements applicable to the data handling activities of DOGANA. The scope is functionality and data sets described in chapter 4 – Data sets and functionality of DOGANA, relevant to computer processing of information. These rules apply only to the social engineering vulnerability tests, within the scope of DOGANA.

The requirements stated in this document are general at this stage, and will have to be subject to a more detailed analysis during the pilot phases of the project, based on the specific legislation applicable to each of the pilots.

Stage	Legal Requirements	Security Policies (chapter 8)
Data Collection	Information given by the company contracting a DOGANA SDVA assessment must not include sensitive personal data.	SP.019 – Sensitive personal data
Data Collection	Information given by the company contracting a DOGANA SDVA assessment must not contain personal data that is not needed for the assessment.	SP.013 – Data Minimization
Data Collection	Information collected by phishing or deception must not include sensitive personal data.	SP.019 – Sensitive personal data
Data Collection	Any personal data collected that is not relevant for the assessment – based on the purpose of the processing – must be deleted.	SP.013 – Data Minimization
Data Collection	Keep anonymised logs from all actions.	SP.003 – Data processing logs
Data Collection	Take security measures to ensure the protection of the collected data.	SP.007 – Data security
Data Collection	Do not collect information from not publicly available sources.	SP.015 – Publicly Available Information
Data Processing	Do not process more information than necessary to achieve the purpose of the processing.	SP.013 – Data Minimization
Data Processing	Process the data in a secure way	SP.007 – Data security
Data Processing	Keep a log from the processing actions	SP.003 – Data processing logs
Data Processing	Anonymise the personal data	SP.016 – Data Anonymisation
Data Processing	Make sure that no automated decisions are based on the processing of personal data.	SP.020 – Automated decisions

Stage	Legal Requirements	Security Policies (chapter 8)
Data Storage	Do not keep personal data for longer than necessary.	SP.005 – Data retention
Data Storage	Keep the personal data in an anonymised, or at least pseudonymised form.	SP.016 – Data Anonymisation
Data Storage	Security measures.	SP.007 – Data security
Data Storage	Keep a log.	SP.003 – Data processing logs
Data Storage	Erase the data once they are not necessary for the processing anymore.	SP.006 – Collection Limitation

Table 7 - Legal requirements of DOGANA

7. Privacy by Design Principles

In this chapter, the Privacy by Design (PbD) principles are analysed with regards to the DOGANA scope, the considered data sets and functionality.

PbD Principle	How this principle applies to DOGANA	Resulting policies (chapter 8)
Proactive not reactive, Preventative, not Remedial – "The PbD approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events. It does not wait for risks to materialize, nor does it offer remedies for resolving infractions once they have occurred – it aims to prevent them from occurring. In short, PbD comes before, not after the fact."[4]	In DOGANA, several security policies aim to have preventative privacy controls embedded into the design	SP.005 – Data Retention SP.006 – Collection Limitation SP.007 – Data Security SP.013 – Data Minimization SP.014 – Professional Contacts SP.015 – Publicly Available Information SP.016 – Data Anonymisation SP.017 – Collection of Credentials SP.018 – Anonymisation of results SP.019 – Sensitive Personal Data
Privacy as the default – *"PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy remains intact! No action is required on the part of the individual to protect his or her privacy – it is built into the system, automatically, by default."*[5]	In DOGANA, personal data is anonymised as soon as it is possible and it is not retained after the end of the SDVA study. If nothing is done, information is automatically erased after a retention period.	SP.005 – Data Retention SP.006 – Collection Limitation SP.007 – Data Security SP.013 – Data Minimization SP.016 – Data Anonymisation

4 *Cavoukian, Ann - Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, page 37*

5 *Cavoukian, Ann - Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, page 38*

PbD Principle	How this principle applies to DOGANA	Resulting policies (chapter 8)
Privacy Embedded into Design – *"Privacy should be embedded into the design and architecture of IT systems and business practices. It should not be bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy becomes integral to the system, without diminishing functionality."*[6]	Security policies are defined in the early stages of DOGANA development and are validated throughout the implementation tasks until the final pilots.	SP.007 – Data Security SP.021 – Privacy Embedded into Design SP.022 – Privacy Impact Assessment
Full functionality - Positive Sum not Zero Sum – *"PbD seeks to accommodate all legitimate interests and objectives in a positive- sum, or doubly enabling "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. It avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is indeed possible to have multiple functionalities."*[7]	The DOGANA project aims at developing an SDVA system that works with the most advanced technology and functionality (beyond "state-of-the-art"), while ensuring the compliance with data protection legislation.	All security policies.

6 *Cavoukian, Ann - Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, page 39*

7 *Cavoukian, Ann - Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, page 40*

PbD Principle	How this principle applies to DOGANA	Resulting policies (chapter 8)
End-to-end security - Lifecycle Protection – ***"Privacy, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, and in a timely fashion. Thus, PbD ensures cradle-to-grave lifecycle management of personal information, end-to-end."***[8]	DOGANA protects personal data from collection to analysis and reporting, making sure privacy rights such as consent, individual participation, right of erasure and accountability are respected.	SP.001 – Consent SP.002 – Traceability of Data SP.004 – Data Erasure SP.008 – Data Controller SP.009 – Individual Participation SP.012 – Accountability SP.019 – Sensitive Personal Data
Visibility and Transparency – ***"PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember – trust but verify."***[9]	DOGANA implements controls to ensure user participation and transparency.	SP.001 – Consent SP.002 – Traceability of Data SP.004 – Data Erasure SP.008 – Data Controller SP.009 – Individual Participation SP.012 – Accountability

8 *Cavoukian, Ann - Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, page 41*

9 *Cavoukian, Ann - Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, page 42*

PbD Principle	How this principle applies to DOGANA	Resulting policies (chapter 8)
Respect for User Privacy – ***"At its core, respecting the user means that, when designing or deploying an information system, the individual's privacy rights and interests are accommodated, right from the outset. User-centricity is designing for the user, anticipating his or her privacy perceptions, needs, requirements, and default settings."***[10]	In DOGANA user rights are respected throughout the SDVA process, including the right to objection and erasure of information.	SP.001 – Consent SP.002 – Traceability of Data SP.004 – Data Erasure SP.006 – Collection Limitation SP.008 – Data Controller SP.009 – Individual Participation SP.012 – Accountability SP.015 – Publicly Available Information

Table 8 - Mapping of PbD principles

10 *Cavoukian, Ann - Privacy by Design and the Emerging Personal Data Ecosystem, October 2012, page 42*

8. Security Policies

In this chapter we document the resulting security policies identified in the previous chapters, grouped by the functionality of DOGANA and the respective data sets they apply to.

Security Policy	Policy Text
SP.001 – Consent	Subjects of the SDVA must give their informed consent for the usage of their personal data, which is one of the legal grounds for the implementation of SDVA tests. To ensure the informed consent does not disturb the results of the assessment, consent is given through the acceptance of the corporate security policies of the organizations using DOGANA. These policies must explicitly mention the possibility of conducting SDVA tests.
SP.002 – Traceability of data	All data must be traceable at any given moment, by owner. It must be possible to identify in a human-readable report: (i) all data concerning an individual, and (ii) the identity of the owner of any piece of data stored within the system.
SP.003 – Data processing logs	A log must be kept that allows for the independent verification of all actions performed on a unit of personal data, through all the processing stages, from collection to destruction. These logs must not contain any personal data.
SP.004 – Data Erasure	The system must allow for the deletion of all data pertaining to an individual upon his or her request. This deletion action must be logged.
SP.005 – Data retention	All items of data stored in the system must have a validity date, after which they cannot be used and should be erased. Data retention times should be configured to match the legal requirements of the country the SDVA is being conducted in. If it is not configured, validity time should default to 30 days.
SP.006 – Collection Limitation	Data that is collected but not used for the SDVA study must be immediately deleted. This action must be logged.
SP.007 – Data Security	Any systems used for the storage and processing of personal data within the DOGANA project must demonstrate a good level of security readiness, which can be done by (a) inclusion of the system within the scope of an ISO 27001 certified Information Security Management System or (b) independent verification by a third-party audit.
SP.008 – Data Controller	Each repository of personal data used by DOGANA must identify the person responsible for the information, who will assume the data controller role within the organization managing or deploying a DOGANA-based SDVA system.
SP.009 – Individual Participation	The data controller nominated within the organization implementing a DOGANA-based system must implement a service desk using reasonable means to allow individuals to query about their information.
SP.010 – Authentication	All access to personal data within DOGANA is subject to user authentication.

Security Policy	Policy Text
SP.011 – Authorization	Access levels should be implemented to allow only authorized individuals to view, modify or delete information within DOGANA.
SP.012 – Accountability	All accesses and operations must be logged with detailed information on the date, time, location, system, user and action performed on which data. Read-only accesses to personal data must also be logged.
SP.013 – Data Minimization	Unused or unnecessary data that is collected must be deleted as early as possible. The collection process must be designed to identify and discard any sensitive information that is gathered on a subject. When collecting information from social media sites, do not collect multimedia contents (such as photos, video or audio).
SP.014 – Professional contacts	Only professional contacts (e-mail and mobile numbers) should be collected. Any personal contacts that may be collected must be discarded as soon as they are identified as non-professional.
SP.015 – Publicly Available Information	Restrict data collection to publicly available information.
SP.016 – Data Anonymisation	Personal data must be anonymised as early as possible in the data collection and processing.
SP.017 – Collection of credentials	When performing credential harvesting, usernames and passwords should immediately be discarded after they are longer necessary. The system should retain proof that the vulnerability exists (access to sensitive information) but should not keep the username and password information.
SP.018 – Anonymisation of results	Analysis results must not identify individual subjects of the study, either directly or by inference.
SP.019 – Sensitive personal data	Sensitive personal data as defined in Article 10 of the General Data Protection Regulation[11] shall not be processed by DOGANA. This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
SP.020 – Automated decisions	No automated decision should be done when processing personal data.
SP.021 – Privacy Embedded into Design	The implementation of the DOGANA system must follow the policies documented in this deliverable in all development stages, from conceptual design to final rollout.
SP.022 – Privacy Impact Assessment	Before each deployment of a DOGANA-based system, a privacy impact assessment must be conducted by an independent auditor to ensure compliance with these policies and the legal requirements of the deployment country.

11 DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL – General Data Protection Regulation

Security Policy	Policy Text
SP.023 – Reuse of Personal Data	Personal data collected for a SDVA study shall not be reused after the completion of the study. All collected data shall be anonymised as soon as possible and deleted as soon as the study is complete. See SP.018 and SP.005.

Table 9 – Security policies