PRIPARE

Privacy- and Security-by-Design Methodology Handbook

Version:	V1.00
Date:	31 December 2015
Author/s:	Alberto Crespo García (ATOS) Nicolás Notario McDonnell (ATOS) Carmela Troncoso (Gradiant) Daniel Le Métayer (Inria) Inga Kroener (Trilateral) David Wright (Trilateral) José María del Álamo (UPM) Yod Samuel Martín (UPM)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no ICT-610613

Table of Contents

LIST OF FIGURES 4

LIST OF TABLES 5

ABBREVIATIONS AND DEFINITIONS 6

FOREWORD 9

1 INTRODUCTION 10

2 REFERENCE MODEL 12

3 PHASES 14

4 ROLES 16

5 EXAMPLE DESCRIPTION 18

6 PROCESSES 20

6.1 ENVIRONMENT & INFRASTRUCTURE 20

6.1.1 Organizational Privacy Architecture 20

6.1.2 Promote privacy awareness 22

6.2 ANALYSIS 24

6.2.1 Functional Description and High-Level Privacy Analysis 26

6.2.2 Legal assessment 29

6.2.3 Privacy and security plan preparation 32

6.2.4 Detailed privacy analysis 33

6.2.5 Operationalization of Privacy Principles 38

6.2.6 Risk management 44

6.3 DESIGN 49

6.3.1 Privacy enhancing architecture design 50

6.3.2 Privacy-Enhancing Detailed Design 58

6.4 IMPLEMENTATION 63

6.4.1 Privacy implementation 63

6.5 VERIFICATION 66

6.5.1 Accountability 66

6.5.2 Security & Privacy static analysis (a priori verification) 67

6.5.3 Security & Privacy dynamic analysis 69

6.6 RELEASE 71

6.6.1 Create Incident Response Plan 71

6.6.2 Create system decommissioning plan 73

6.6.3 Final Security & Privacy review 75

6.6.4 Publish PIA report 77

6.7 MAINTENANCE 79

6.7.1 Execute incident response plan 79

6.7.2 Security & Privacy verifications 81

6.8 DECOMMISSIONING 83
6.8.1 Execute decommissioning plan 83
7 METHODOLOGY APPLICATION GUIDELINES 85
7.1 ITINERARIES 85
7.1.1 Mandatory 87
7.1.2 Lightweight 87
7.1.3 Standard 89
7.2 MERGING WITH EXISTING METHODOLOGIES 90
7.2.1 Integrating ISO 9241-210 User-Centered Design Process 90
7.2.2 Software and system engineering methodologies 94
7.2.3 Project management methodologies 107
ANNEX A: PSMA TEMPLATE 113
A.1 PURPOSE 113
A.2 PRIVACY & SECURITY TEAM 113
A.3 INTRODUCTION AND OBJECTIVE 113
A.4 ITINERARY AND ROADMAP 113
A.5 DEFINITIONS 113
A.6 FUNCTIONAL DESCRIPTION 113
A.6.1 Privacy stakeholders / actors 113
A.6.2 Domains and roles 113
A.6.3 Relevant business processes, products, systems and applications within systems 114
A.6.4 Data subject(s) associated 114
A.6.5 Data flows and touch points 114
A.7 IMPACT ASSESSMENT 115
A.7.1 Policies and regulation 115
A.7.2 Privacy principles / targets 115
A.7.3 Risk assessment 116
A.7.4 Feared events 116
A.7.5 Threats 117
A.7.6 Initial Impact Assessment 118
A.8 CONFORMANCE CRITERIA 118
A.9 DESIGN LOGBOOK 118
A.10 PRIVACY CONTROLS 118
A.11 REMAINING THREATS AND RECOMMENDATIONS 118
A.12 ACCOUNTABILITY 119
A.13 INCIDENT RESPONSE PLAN 119
A.14 SYSTEM DECOMMISSIONING PLAN 119
A.15 FINAL PIA REPORT 119
ANNEX B LIST OF PRIVACY PRINCIPLES, GUIDELINES, AND CRITERIA FOR REQUIREMENTS OPERATIONALIZATION 120

List of Figures

Figure 1: PRIPARE’s methodology reference model 12
Figure 2: PRIPARE methodology phases 15
Figure 3: PRIPARE processes and phases 20
Figure 4: Risk based vs Goal oriented approaches 24
Figure 5: Structured decomposition of privacy principles into requirements. 39
Figure 6: Privacy Control Design 49
Figure 7: Scenario components 51
Figure 8: GreenPriTech initial architecture 52
Figure 9: GreenPriTech initial billing scenario 53
Figure 10: Utility tree 53
Figure 11: Modified GreenPriTech architecture 55
Figure 12: Modified GreenPriTech scenario 55
Figure 13: Basic structure of a design technique 60
Figure 14: Itinerary selection process 85
Figure 15: PRIPARE's mandatory processes 87
Figure 16: PRIPARE's lightweight itinerary 88
Figure 17: PRIPARE's standard itinerary 89
Figure 18: ISO 9241-210 user-centered design process mapped to PRIPARE processes 90
Figure 19: User-centered UI design process 91
Figure 20: Waterfall methodology 94
Figure 21: Iterative methodology 97
Figure 22: The scrum process 103
Figure 23: PMBOK process and knowledge matrix 107

List of Tables

Table 1: Acronym table 8
Table 2: Risk Map 46
Table 3: Classification of Privacy Enhancing Techniques (Kung) 61
Table 4: Classification of Privacy Enhancing Techniques (Hoepman) 61
Table 5: Example of privacy-enhancing design techniques in GreenPriTech systems 63
Table 6: PRIPARE complementing a waterfall methodology 96
Table 7: PRIPARE complementing an iterative methodology 99
Table 8: PRIPARE complementing a prototype methodology 102
Table 9: PRIPARE complementing an agile methodology 106
Table 10: PRIPARE complementing PMBOK® 109
Table 11: PRIPARE complementing PRINCE2 112
Table 12: Privacy & Security team 113
Table 13: Data flow matrix 114
Table 14: Data flow details 115
Table 15: Privacy targets 115
Table 16: Privacy sub-targets 116
Table 17: CNIL's severity mapping 116
Table 18: Threats severity 117
Table 19: Threats 117
Table 20: Privacy controls 118
Table 21: Remaining threats 119

Abbreviations and Definitions

Abbreviation	Definition
ADD	Attribute-Driven Design
AES	Advanced Encryption Standard
ASVS	Application Security Verification Standard
ATAM	Architecture Trade-off Analysis Method
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBAM	Cost Benefit Analysis Method
CI	Contextual Integrity
CNIL	Commission nationale de l'informatique et des libertés
CPDP	Computers, Privacy & Data Protection
DPA	Data Protection Authority
DPD	Data Protection Directive
DPO	Data Protection Office
DPR	Data Protection Regulation
EC	European Commission
ECHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Network and Information Security
EUP	Enterprise Unified Process
EV	Electric Vehicle
EVID	Electric Vehicle Identification
FSPR	Final Privacy & Security review
GCM	Galois Counter Mode
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ICO	Information Commissioner’s Office
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISACA	Information Systems Audit and Control Associations
ISO	International Organization for Standardization
JRC	Jointed Research Centre
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OGC	Office of Government Commerce
OS	Operating System

OUM	Oracle Unified Method
OWASP	Open Web Application Security Project
PbD	Privacy by Design
PbD-SE	Privacy by Design Documentation for Software Engineers
PEAR	Privacy Enhancing ARchitecture
PET	Privacy Enhancing Technology
PI	Personal Information
PIA	Privacy Impact Assessment
PIAF	Privacy Impact Assessment Framework
PII	Personal Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PIR	Private Information Retrieval
PKCS	Public-Key Cryptography Standards
PLC	Power Line Communication
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMO	Project Management Office
PMRM	Privacy Management Reference Model
PRINCE2	Projects in Controlled Environments, version 2
PRIPARE	PReparing Industry to Privacy-by-design by supporting its Application in REsearch
PSbD	Privacy and Security by Design
PSMA	Privacy and Security Management Analysis
PSMO	Privacy & Security Management Officers
PWC	Price Waterhouse and Coopers
RFID	Radio Frequency IDentification
RUP	Rational Unified Process
SANS	SysAdmin Audit, Networking and Security Institute
SbD	Security by Design
SEI	Software Engineering Institute
SHA	Secure Hash Algorithm
SIMPL	SIMple Privacy Language
SIPOC	Supplier, Inputs, Process, Outputs, Customers
STIG	Secure Technical Implementation Guides
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TC	Technical Committee

TC	Technical Committee
TLS	Transport Layer Security
TOE	Target Of Evaluation
TPM	Trusted Platform Modules
TSF	TOE Security Functionality
UCA	User-Centered Design
UI	User Interface
UK	United Kingdom
UMA	User Managed Access
UML	Unified Modelling Language
UP	Unified Process
URL	Uniform Resource Locator
USA	United States of America
W3C	World Wide Web Consortium
WAI	Web Accessibility Initiative
WCAG	Web Content Accessibility Guidelines
XML	eXtensible Markup Language

Table 1: Acronym table

Foreword

PRIPARE started in October 2013 as a support action funded by the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 610613. Its mission has been twofold:

- facilitate the application of a privacy- and security-by-design methodology, support its practice by the ICT research community to prepare for industry practice; and
- foster risk management culture through educational material targeted to a diversity of stakeholders.

In December 2015, PRIPARE released the following material

- a set of documents describing the practice of privacy engineering,
- a set of educational material, and
- contribution to research.

The privacy- and security-by-design methodology handbook is the most important contribution of PRIPARE on privacy engineering. It captures and integrates the existing standards, practices and research proposals on privacy engineering.

This handbook is the result of a two-year integration effort. A first methodology specification was released in December 2014[1]. PRIPARE then focused on training and standardisation activities. There was one training workshop in March 2015, followed by smaller workshops with dedicated research projects (CRISALIS[2] on smart grids, MoveUS[3] on mobility services and RERUM[4] on the Internet of Things). Involvement on standardisation took place at OASIS[5] and at ISO[6] level. As a result of the feedback gained from these activities, a second version has been published in December 2015[7].

This handbook is an "easy-to-read" version of the methodology. We hope that it can become the reference material from which future engineers will build their privacy engineering practices.

Antonio Kung
coordinator PRIPARE
December 2015

[1] Available as deliverable D1.2 (http://pripareproject.eu/wp-content/uploads/2013/11/PRIPARE_Deliverable_D1.2_draft.pdf)

[2] http://www.crisalis-project.eu/

[3] http://www.moveus-project.eu/

[4] https://ict-rerum.eu/

[5] PRIPARE contributed to OASIS PbD-SE and PMRM committees

[6] PRIPARE contributed to the creation of an ISO working group on privacy engineering (ISO/IEC JTC1/SC27/WG5)

[7] See D1.3 in http://pripareproject.eu/research/

1 Introduction

This handbook is meant to be a complete description of PRIPARE's methodology and to be used as its reference guide. The entire document is organized in several sections:

- Introduction: presents the context that influences the methodology and its basis.
- Reference model: presents the methodology reference model, its concepts and their relationship.
- Phases: introduces and describes eight phases of the PRIPARE methodology.
- Roles: lists the main roles that are present in the description of the PRIPARE methodology.
- Example description: introduces the example used through the methodology description to demonstrate its usage.
- Processes: presents all the processes grouped in their corresponding phase.
- Methodology application guidelines: provides practical guidelines on how to select and follow some of PRIPARE's preselected itineraries and on how to merge with prevalent system engineering and project management methodologies
- Annex A: a privacy and security management analysis (PSMA) template proposed by PRIPARE team where to reflect the outputs of the processes within the methodology.

In order to provide a better reading experience, this handbook includes some styles that clearly identify the purpose of specific parts of the text:

Example

Italic text with a grey background indicates that it is related to the application of the methodology to the example provided in section 5.

Notice: text accompanied by an exclamation mark indicates text that indicates something of high importance.

Relationship with the legislation: text accompanied with an EU legislation icon, indicates that it provides references to the EU legislation (including "soft" legislation) and it is used to present the relationship of PRIPARE with the EU Data Protection Directive (DPD) and General Data Protection Regulation (GDPR), among others.

At the time when this handbook is been written the there is no definitive version of a EU GDPR. There are several drafts proposed/approved by the European Commission, the European Parliament and the Council. These three institutions are currently under trialogue discussions to jointly agree on the final text of the regulation. These discussions commenced officially on June 24, 2015, and are currently scheduled to produce the final version of the GDPR by December 2015.

When writing this document, the reference to the latest draft was always used. In the final version of this document, references to the EU GDPR will explicitly mention the draft version they were referring to.

These drafts have no legal value at the time this document was written and some provisions may change before the final approval.

Correspondence with PRIPARE's proposition of an output template (0): text accompanied with the template icon is meant to identify what sections of the template are affected by a specific process or step

- Section a.b
- Section c.d

When to apply?: text accompanied of a check mark presents the conditions that should determine the application or not of a PRIPARE processes

2 Reference model

According to OASIS, **a reference model** is “an **abstract framework** for understanding significant **relationships among the entities** of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model **is based on a small number of unifying concepts** and may be used as a basis for education and explaining standards to a non-specialist. A reference model is **not directly tied to any standards, technologies or other concrete implementation** details, but it does seek to provide a common semantics that can be used unambiguously across and between different implementations”[8].

Hence, providing a reference model, which explains the main concepts behind the PRIPARE’s methodology, will allow for a better understanding and a better communication among practitioners. Providing a reference model that clearly identifies the provenance of each of the concepts also allows one to understand how different approaches have converged within PRIPARE.

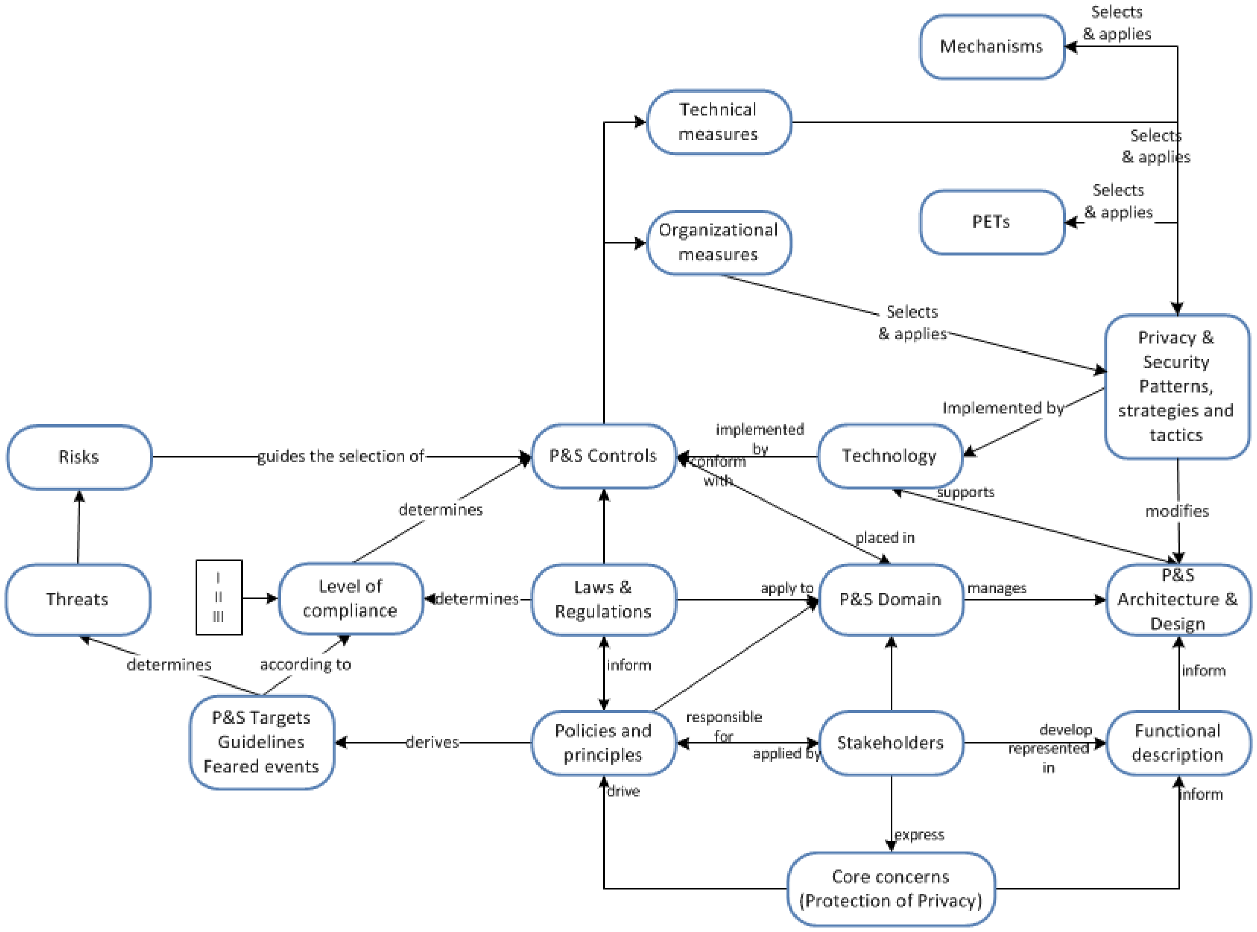


Figure 1: PRIPARE’s methodology reference model

While many concepts should already be clear for potential PRIPARE practitioners (e.g. architecture, technology, and functional description), some other concepts or relationships should be clarified:

[8] https://www.oasis-open.org/committees/soa-rm/faq.php

- The core protection of privacy concerns may be expressed by any of the stakeholders involved (e.g. data subjects, policy makers, system developers, project owners..). This concerns help to drive policies but are also essential to understand and elicit the functional requirements (functional description) that have to be designed and implemented in the various stakeholders' domains.

Other definitions necessary to understand PRIPARE are:

- **Privacy and security controls** are technical and organisational measures that are incorporated into systems and organizations in order to address privacy and security issues arising from legislation and stakeholders requirements.
    - **Technical measures** are incorporated into systems at design time through technical choices. This may include **selecting and applying a specific design pattern, a specific architecture, and/or specific security**, e.g., encryption, and privacy, e.g., anonymous communications, **mechanisms**. This can also include the selection of default settings, policies or other mechanisms to ensure consent or decision support.
    - **Organizational privacy and security measures** on the other hand are management practices and operational mechanisms/ processes integrated into the organization structure. They refer to the appointment of a Data Protection Officer, drafting of internal policies and guidelines, staff training, accountability management scheme, etc.
- **Privacy & Security Domain:** "A physical or logical area within the use case that is subject to the control of a Domain Owner(s) "

Other concepts were already defined in PRIPARE's concepts and principles report[9]:

- **Threat**: Typical action used by risk sources that may cause a feared event.
- **Risk**: Scenario describing a feared event and all threats that make it possible. It is estimated in terms of severity and likelihood.

[9] Further info on these definitions can be found in http://pripareproject.eu/wp-content/uploads/2013/11/D1.1.pdf

3 Phases

PRIPARE is structured in seven different phases that match common and classic system engineering phases easing its merge with most prevalent engineering practices or to standards such as ISO 15288:

- **Analysis**: during this phase privacy and security issues or concerned must be discovered and reflected so they can be addressed during the design and implementation steps. The principal objective is to characterize the system from a security and privacy perspective.
- **Design**: define the system's architecture, components, modules, interfaces in order to satisfy specified requirements
- **Implementation**: during this phase (transform the design into a built system) technology privacy and security principles and best practices must be followed;
- **Verification**: it must be ensured that the system meets privacy and security requirements through privacy and security testing, code reviews, audits...
- **Release**: once the system is implemented and verified it is ready to be delivered or provided to the customer. During this phase it must be ensured that an action plan is present in order to respond to the discovery of privacy or security issues or breaches. Final security & privacy reviews could be required prior to the release.
- **Maintenance**: once the system is running and it is being used, responsibles must react to security & privacy incidents ensure that privacy & security processes are being enforced. Any evolution of the system during this phase must contemplate all previous steps and be incorporated into the system following the established security and data protection principles.
- **Decommission**: it must be ensured that systems are correctly dismantled and that personal data is correctly treated accordingly to the current legislation and policies.

An additional phase is contemplated to group privacy and security horizontal practices that should exist in any organization and should be independent of the engineering process itself.

- **Environment & Infrastructure**: In order to support the proper application of PRIPARE methodology for the engineering of a system, the organization developing or operating the project must have an appropriate organizational structure, besides a reasonable level of privacy and security awareness, to support the various stakeholders during the methodology application. This phase is horizontal and it is not bound to any concrete system or project.

Organizing the methodology into these phases ensures that privacy aspects are considered during the full lifecycle of the system and for any personal data which may be collected, stored or processed.

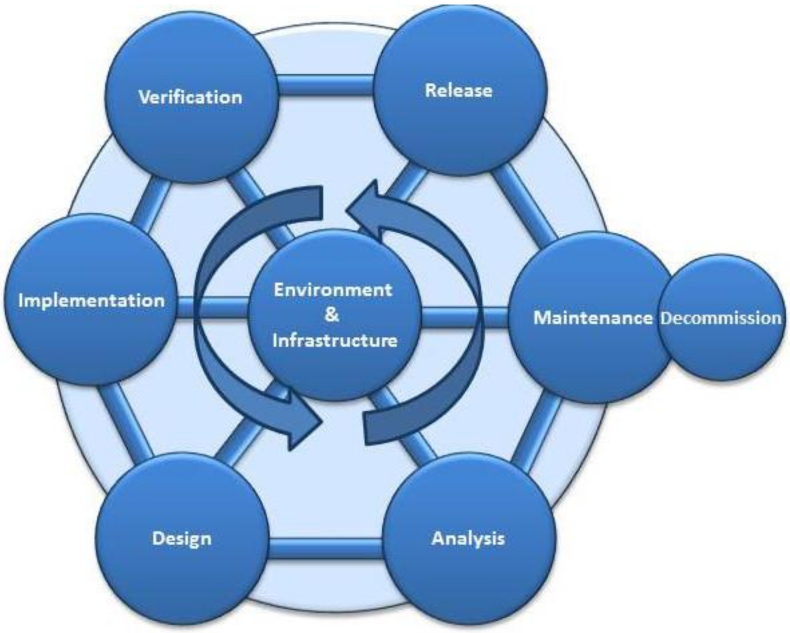


Figure 2: PRIPARE methodology phases

The representation of PRIPARE's methodology shown in Figure 2 captures several aspects of it:

- **Iterative**: the methodology can and should be applied iteratively to correctly address the dynamicity of system engineering (e.g. new requirements, design changes or iterative developments)
- **Organizational aspects are key**: organizations must foster a privacy and security environment and develop an organizational privacy & security structure which supports all the engineering processes.
- **Non-linear**: the methodology may be applied in whatever order necessary and it is possible to jump from one phase to other (e.g. from maintenance to implementation or from design to verification)

PRIPARE seven phases can be easily adapted to organisation lifecycle phases. For instance using ISO15288 would lead to the following mapping:

PRIPARE Phases	ISO 15288 System Life Cycle Processes
Environment & Infrastructure	Infrastructure management process Project privacy portfolio management process
Analysis	Stakeholder privacy requirements definition process Privacy requirements analysis process
Design	Privacy architectural design process
Implementation	Privacy implementation process
Verification	Privacy Verification process
Release	Transition process
Maintenance	Maintenance process
Decommissioning	Disposal process

4 Roles

It is important to distinguish between the roles that are inherent to the system being engineered from those that are related to the application of PRIPARE methodology. PRIPARE has identified an initial set or roles that are reflected in the processes that characterize the methodology:

- **System engineers**: are responsible for enabling the realization of successful systems; they ensure that all aspects of a project or system are considered, and integrated into a whole, during the full system's lifecycle. They can be sub-divided into:
    - Business & system analyst: its role is to liaise with the end user and to gather an understanding of the system which has to be built.
    - System designer: responsible for, based on a requirement specification, developing a comprehensive plan and instructions which can be given to the developers in order to implement a system.
    - System developer: following the design specifications, the developers build the expected system.
    - UI designer: system designers which are specifically focused on the specification of the UI aspects.
    - Tester: even each of the roles are responsible for ensuring that their outputs are complete and free from errors, there is a need for testing the system as a whole, ensuring that it meets end-user expectations. Testers are responsible for detecting errors and deviations from the requirement and design specifications.
- **Privacy & Security managers & officers (PSMOs):** the senior-level executives within organizations responsible for managing the establishment and maintenance of security and privacy procedures across the organization who address privacy and security issues and minimize their risks.
    - Privacy & security engineers: part of the privacy and security office, these engineers are IT experts in the design of systems, aware of privacy methodological practices and available PETs and techniques that lead to the development of privacy enhanced systems. Such engineers should have the knowledge and abilities to understand the legal framework in which the system will be deployed and to link this legal framework with the systems' features, privacy controls and existing risks.
    - Privacy & Security Officer: a person with expert knowledge of data protection law and practices and ability to fulfil tasks such: monitor compliance with the regulation, advise the controller and processor about their obligations (regarding the legal framework), to act as the DPA contact point, etc

While the EU Data Protection Directive talks about the controllers appointing "data protection officials" and the forthcoming Regulation about "data protection officers", PRIPARE envisions a broader role which also comprehends the data protection officers and officials' duties. The main difference is that PRIPARE believes that addressing data protection issues alone is not enough and that other types of privacy must also be considered, besides also taking into account security issues and implications.

- **Data Protection Authorities (DPAs)**: independent bodies which are in charge of:
  - monitoring the processing of personal data within their jurisdiction (country, region or international organization);
  - providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data;
  - hearing complaints lodged by citizens with regard to the protection of their data protection rights.
- **Data subjects**: people whose personal data are collected, held or processed.
- **Project managers**: the senior-level executives within organizations responsible for making project-level decisions regarding scope, costs and schedule. They can be sub-divided depending on the role the organization has in relation to the system:
  - System owners
  - System operators
  - System suppliers
- **End users**: people who make use of the engineered systems.

5 Example description

In order to exemplify the application of the PRIPARE's methodology, a use case will be followed during all the processes. The selected example is based on the use case presented in PMRM[10] and slightly adapted to a European context. It has been extended to give more importance to the related advertising program in order to maximize the demonstration of the PRIPARE's features.

This example is relevant for PRIPARE because:

- It is a real world example
- It addresses existing challenges for privacy in an emerging domain which has special relevance for the EC (smart charge and EV);

All references to the example will be enclosed in a box to clearly separate the example from the process description. The exemplification of some of the processes imported from PMRM will also be adapted and used to demonstrate the concepts.

Example description

A European utility, GreenPriTech, with a residential customer base with smart meters installed, wants to promote the increased use of electric vehicles (EV) in its service area by offering significantly reduced electricity rates for night-time recharging of vehicle battery. The system also permits the customer to use the charging station at another customer's site (such as at a friend's house and have the system bill the vehicle owner instead of the customer whose charging station is used. The system allows even charging the car in other European countries.

The customer plugs in the car and requests "charge at cheapest rates". The utility is notified of the car's presence, its ID number and the approximate charge required (provided by the car's on-board computer). The utility schedules the recharge to take place during the evening hours and at different times than other EV charging (thus putting diversity into the load).

The billing department now calculates the amount of money to charge the EV customer based on EV rates and for the measured time period.

The same EV customer drives to a friend's home (who also has an EV) and requests a quick charge to make sure that he can get back home. When he plugs his EV into his friend's EV charger, the utility identifies the fact that the EV belongs to a different customer and places the charging bill on the correct person's invoice.

As part of the programme the utility wishes to capture behavioural and movement patterns in order to adjust the electricity production peaks

An initial impact assessment reveals that this kind of system may expose customer's personal data, creating a series of privacy risks that should be carefully assessed and addressed during the engineering process:

Initial Impact Assessment

A system as the one described above presents a set of risks for privacy:

•Direct EV identification: EV may be directly linked to individuals;

[10] http://docs.oasis-open.org/pmrm/PMRM/v1.0/csprd01/PMRM-v1.0-csprd01.html

•Charging location identification: stemming from the ability to link customers and their vehicles to geo-located charging points;

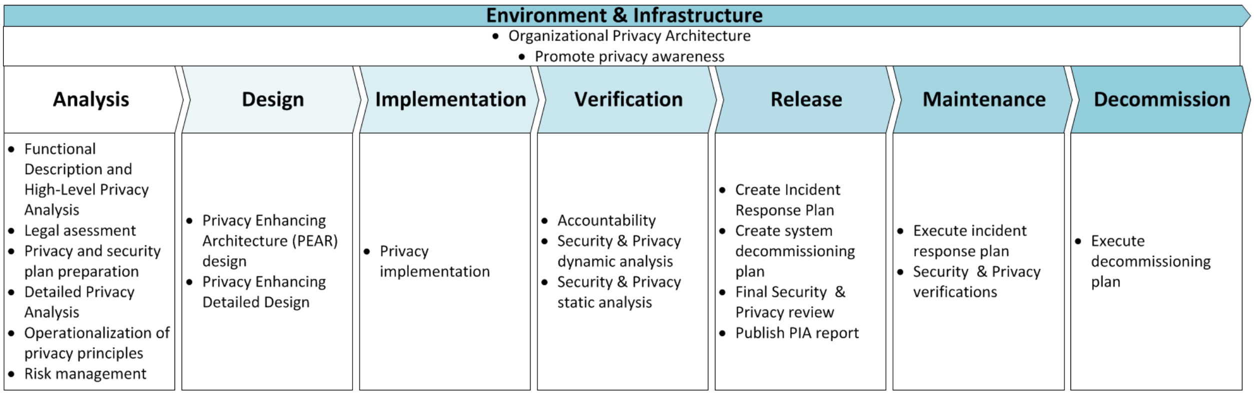
Potentially this information may be available to the utility and the advertising organization.

Also, scheduling vehicle's charging times exposes behavioural patterns to the utility, which poses privacy invasion risks: e.g. a customer that charges the vehicle every night and modifies this for one specific night reveals that the customer will not be at home that night.

While this information is key to address electricity-demand peaks, to provide electricity in a more efficient way offering customers better prices, the system must be designed to minimize or completely avoid these potential risks.

6 Processes

The complete list of all PRIPARE's processes associated to the eight methodology phases (presented in section 3) is presented in the following figure (Figure 3) and will be further described in following subsections first introducing the methodology phase and then each of its processes.



Environment & Infrastructure

- Organizational Privacy Architecture
- Promote privacy awareness

Analysis	Design	Implementation	Verification	Release	Maintenance	Decommission
• Functional Description and High-Level Privacy Analysis • Legal asessment • Privacy and security plan preparation • Detailed Privacy Analysis • Operationalization of privacy principles • Risk management	• Privacy Enhancing Architecture (PEAR) design • Privacy Enhancing Detailed Design	• Privacy implementation	• Accountability • Security & Privacy dynamic analysis • Security & Privacy static analysis	• Create Incident Response Plan • Create system decommissioning plan • Final Security & Privacy review • Publish PIA report	• Execute incident response plan • Security & Privacy verifications	• Execute decommissioning plan

Figure 3: PRIPARE processes and phases

6.1 *Environment & Infrastructure*

Privacy is not an emerging feature within organisations, privacy requires a high-level support accompanied with the fostering of a privacy culture. PRIPARE is a methodology which will be only be useful and effective if the appropriate resources and internal structure are in place within the organizations.

6.1.1 Organizational Privacy Architecture

Whenever the regulation requires a data protection office or officer to be appointed

Large organizations should establish, at least, data protection officers.

Small and medium organizations can establish informal privacy architectures and nominate a "privacy champ", which should be consulted for any privacy issue and responsible for supervising privacy aspects of the organization.

Privacy enhancing, or privacy supporting processes need to be supported by internal privacy architectures within organisations in order to support its policy objectives. This internal architecture includes an internal organisational structure and governance model, which supports a range of expertise (personnel and professional expertise) into the privacy enhancing or privacy supporting process, and a support mechanism for the implementation of results.

Organizational Privacy Architecture				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Privacy & Security Managers & Officers (PSMOs)	Privacy roles Privacy principles Accountability mechanisms Awareness of legal frameworks	Implementing internal administrative architecture to support privacy enhancing or privacy supporting process policy objectives Identifying customers & suppliers	Internal privacy architecture and governance framework	Organization's staff End users Data subjects

		for privacy architecture and processes		
Tools & Techniques	PIA methodologies, PIA standards, privacy maturity assessments and models			
Knowledge	Knowledge of privacy principles/accountability mechanisms/legal frameworks			
Responsible	Project manager advised by the PSMOs (all employees should be sensitive to privacy)			

The process outlined in the table above establishes an internal architecture through the creation of a governance framework. The privacy enhancing, or privacy supporting processes are established within a wider context of creating accountability mechanisms within organisations. For this purpose, organisations could establish a department to deal with privacy-related issues. Alternatively, the organisation could employ a privacy officer to deal with over-arching privacy-related issues across a range of projects. The privacy officer could work on a variety of projects across the organisation and in combination with the project manager to deal with privacy-related issues. All employees should be considered part of the wider privacy team, as all should be aware of privacy and data protection issues. Alongside the establishment of a privacy officer, an organisation should also establish a set of metrics (KPIs) to assess privacy and related issues, regularly measuring these against a chosen privacy maturity model.

GreenPriTech is a large organisation with over 300 employees, and with a number of potential risks and issues related to privacy. Given these considerations, a privacy department has been established, which comprises of a privacy officer, representatives from the legal department and the CTO of the organisation. This department has developed several privacy programmes oriented to: decision makers; IT employees; and support desk employees. This department is also responsible for: contacting DPAs when necessary; signing off PIA reports; security and privacy reviews prior to any system release; executing the incident response plan following a privacy breach; and following regular security and privacy verifications.

The privacy officer designs a strategy to develop a governance framework under which privacy awareness and control can be implemented and maintained throughout the organisation. This includes providing mechanisms for evaluation and monitoring compliance and the eventual monitoring of PIA recommendations and evaluation results from the assessment of privacy practices against KPIs and the chosen privacy maturity model. Developing a governance framework within the organisation will ensure that privacy assessments and PIA recommendations will be taken on board across the entire organisation.

The privacy officer also analyses any existing gaps in terms of the overarching internal privacy architecture and establishes linkages between PIAs and other risk mitigation tools via a range of steps detailed in the following sections.

In the European Commission proposal for the EU GDPR[11], Article 35 introduces a **mandatory data protection officer** for the public sector, and, in the private sector, for large enterprises (more than 250 persons) or where the core activities of the

[11] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

controller or processor consist of processing operations which require regular and systematic monitoring. This builds on Article 18(2) of Directive 95/46/EC[12] which provided the possibility for Member States to introduce such requirement as a surrogate of a general notification requirement.

Article 36 sets out the position of the data protection officer.

Article 37 provides the core tasks of the data protection officer.

A later draft for the EU GDPR, approved by the European Council[13] has adopted a much less strict approach and data protection officers are not 'mandatory' anymore.

! One of the tasks that a privacy and security management office could take care of is the management of a list of general repositories of privacy principles, guidelines, controls, PETs, privacy patterns, etc. that could be the baseline for new projects. This list could be part of the training programmes discussed in the privacy awareness process (section 6.1.2)

ISO 27034[14] describes the concept of organisation normative framework (ONF), defined as a framework where all application security best practices recognized by the organization are stored, or from which they will be refined or derived. The ONF can be used for application privacy best practices

6.1.2 Promote privacy awareness

✓ **Large organizations** should establish privacy awareness programs.

Small and medium organizations can establish informal privacy information repositories with links to available material on the subject which may be consulted when necessary.

Organisations are responsible for ensuring that all employees receive up-to-date privacy training and are sensitive to the privacy implications of new systems, technologies, or processes. Privacy should be incorporated across all levels of the organisation and be embedded and become a part of daily practice. Privacy awareness is promoted in order to encourage the growth and development of an internal "privacy culture" within the organisation.

Promote privacy awareness				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
PSMOs	Regulation and policies that	Creating a general level of privacy awareness within an	Training programmes,	System engineers,

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en

[13] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

[14] ISO/IEC 27034:2011 Information technology — Security techniques — Application security

	govern the organisation.	organisation, and embedding privacy into daily practice, raising the profile of PIAs within organisations through (amongst others) the establishment of codes of conduct, general e-learning, blogs, intranet, privacy screen-savers and games.	Enhanced privacy awareness within the organisation;	project managers, all staff
Tools & Techniques	Codes of conducts, blogs, privacy games (as mentioned above)			
Knowledge	Best practice in relation to privacy training, raising privacy awareness, privacy tools and techniques			
Responsible	PSMOs			

This part of the process involves embedding privacy awareness and privacy practices across all levels of the organisation. Through on-going targeted training and raising awareness of, and raising the profile of PIAs and privacy practices, utilising a range of tools and techniques, such as the establishment of codes of conduct, an enhanced awareness of privacy and PIAs is developed within an organisation. This process involves working at an organisational, rather than individual project level. However, the scope of the privacy awareness activities will depend on the size of the organisation (for example, an SME will have different resources to utilise in this regard than a larger organisation).

Some good practices guides for the security training which can be extrapolated and extended for privacy and which can be applied during this process are:

- UK ICO includes an Appendix (4) in its PIA handbook[15] which talks about privacy strategies, and how organization-broad attitudes towards privacy positively reflect upon them;
- ENISA's guide on how to raise information security awareness[16] ;
- ISACA's book "Security Awareness: Best Practices to Secure Your Enterprise";
- SANS institute paper on "Security Awareness training and privacy"[17].

In the case of GreenPriTech, the Privacy & Security Managers & Officers develop a strategy to incorporate privacy awareness across the organisation, using a range of best practice examples. Within the framework developed in the previous step (internal architecture), privacy patterns are presented and made available to system engineers. Employees are made aware of what privacy principles the organisation is following, and any risks that have been identified through the PIA process.

[15] http://ico.org.uk/pia_handbook_html_v2/html/0-advice.html

[16] http://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide/at_download/fullReport

[17] http://www.sans.org/reading-room/whitepapers/awareness/security-awareness-training-privacy-394

6.2 Analysis

Within PRIPARE two main analysis' sub-stages have been identified:

- **Preliminary stage**: it aims to identify the scope, roles and responsibilities of stakeholders involved in the application of PRIPARE's methodology. These choices must be consistent with the complexity of the project and the organization's capabilities. E.g. choose an itinerary or which processes to follow and identify the specific people who will apply the methodology.
- **Principal stage**: characterize the system, identify privacy & security requirements, controls, applicable legislation, and users' privacy expectations, conduct an initial PIA, and identify potential risks

One of the most important aspects that must be taken into account during this phase is the **involvement and consultation of internal and external stakeholders** (including data subjects and end users) in order to identify privacy and security risks based on their own expertise and particular interests.

During the analysis phase, besides the characterization of the system (requirement gathering, identifying data flows…) the central activity is to understand what privacy and security controls must be implemented in order to effectively operationalize the privacy and security principles. In order to determine which controls must be incorporated, PRIPARE proposes two complementary approaches, presented in Figure 4.

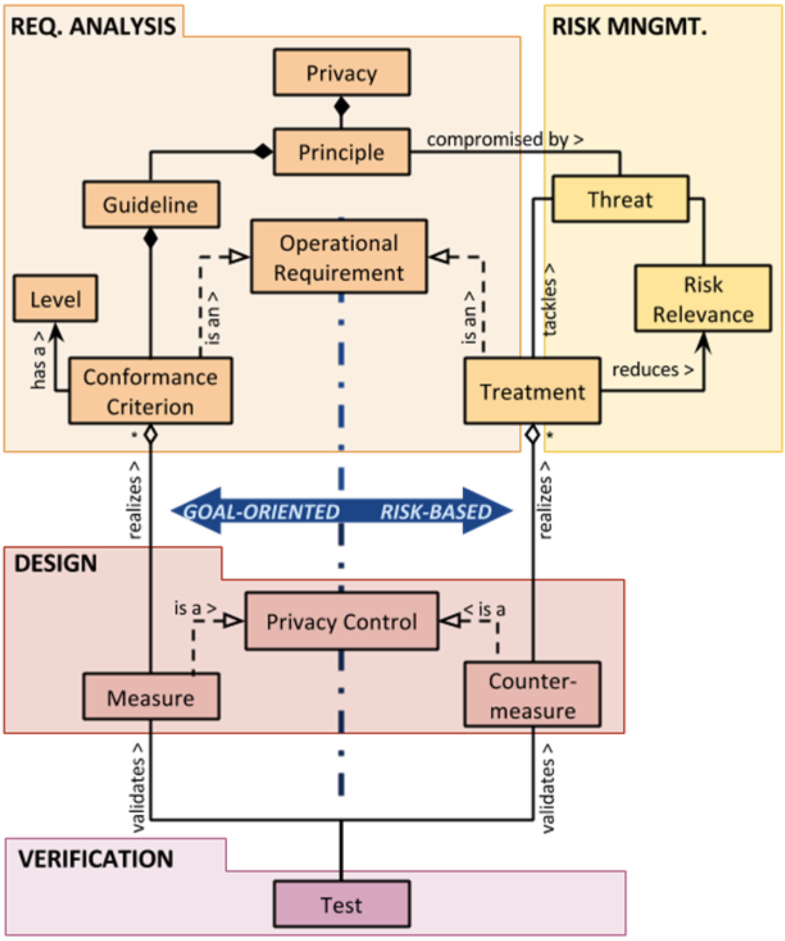


Figure 4: Risk based vs Goal oriented approaches

Risk based approach

Given an initial set of high level security and privacy principles, it consists in:

1. Determining what are the events that can prevent the system from following this principles;
2. Determining the potential impact on data subjects and/or the organization if the feared events where to happen;
3. Determining the chain of events that actually may allowed feared events to occur;
4. Determining the probability of these events;
5. Determining what measures (privacy and security controls) can be but in place in order to minimize or avoid the impact of the feared events and/or the probability of the event occurring;

Goal oriented

This approach is similar to the guidelines developed for achieving accessibility within the Web Accessibility Initiative (WAI), the Web Content Accessibility Guidelines[18] (WCAG). It consists on having, for each high level principle, a list of guidelines (operational goals) mapped to privacy criteria (according to some kind of conformance scale). The framework also provides a test suite which determines the adherence or not of a determined system to the guidelines for a specific conformance level.

Given this initial set of guidelines, tests and privacy criteria associated to high level security and privacy principles, the process consists in:

1. Determining the required level of conformance for the system. It may be self-imposed or imposed by regulations or other stakeholders;
2. Identifying the criteria according to the determined level of conformance for each guideline which determines the privacy requirements
3. Having these criteria fulfilled by the design by choosing the right controls and techniques.

Both approaches try to determine what the system has to do to ensure the system effectively responds to privacy needs, as both try to transform high-level privacy principles into something that can be actually incorporated in a development process. The goal oriented approach seems an easier approach as it removes most of the subjectivity and requires less experience as it highly depends on reliable catalogues of guidelines and privacy criteria, etc. which still have to be developed. The risk oriented approach highly depends on the risk analyst to correctly identify the risks and its subjective perception on the potential impact of a feared event or the probability of to be materialized.

[18] http://www.w3.org/WAI/intro/wcag.php

6.2.1 Functional Description and High-Level Privacy Analysis

Any project should conduct this kind of analysis at it quickly exposes potential privacy risks and the need and scope of following privacy- and security-by-design methodologies

The objective is to scope the application or business service in which personal data is associated and fully understand the environment on which it will be operated.

Functional Description and High-Level Privacy Analysis				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Project managers PSMO	Business analysis • Project details • Material collected during the project definition (e.g. interviews or workshop reports) • Business objectives • Legal framework	Provide a general description of the system or business process Provide an inventory of the capabilities, applications and policy (privacy and security) environment under review	High level privacy analysis • Definitions • Functional description • Inventory • Preliminary PIA	System engineers, Project managers, DPA.
Tools & Techniques	UML, UP, RUP, OUM, user stories, interviews, narrative…			
Knowledge	System’s domain, privacy notions			
Responsible	Business & System Analyst, Privacy engineer			

During this particular process and further ones it is key to involve all the stakeholders in order to ensure to contemplate all point of views:

- End users
- System owners, operators and suppliers
- DPAs

This process has three main activities:

Functional description: Provide a general description of the system or business process, including a glossary denoting most relevant or challenging vocabulary and business objectives. Business objectives may involve demonstrating specified privacy-preserving functionality.

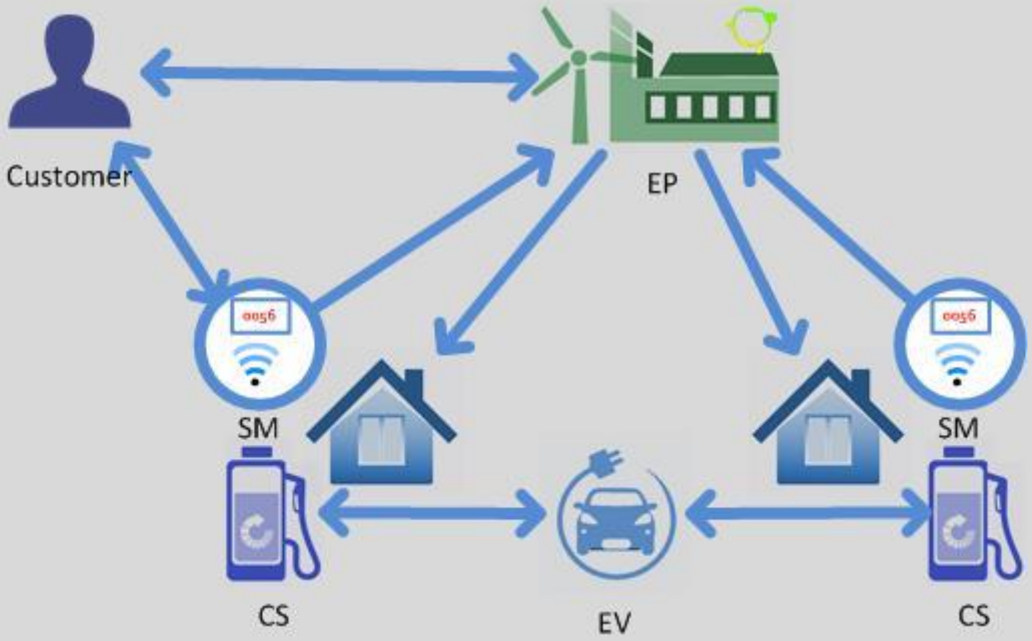
A European utility, GreenPriTech, with a residential customer base with smart meters installed, wants to promote the increased use of electric vehicles in its service area by offering significantly reduced electricity rates for night-time recharging of vehicle battery. The system also permits the customer to use the charging station at another customer's site (such as at a friend's house and have the system bill the vehicle owner instead of the customer whose charging station is used. The system allows even charging the car in other European countries.

The customer plugs in the car and requests "charge at cheapest rates". The utility is notified of the car's presence, its ID number and the approximate charge required (provided by the car's on-board computer). The utility schedules the recharge to take place during the evening hours and at different times than other EV charging (thus putting diversity into the load).

The billing department now calculates the amount of money to charge the EV customer based on EV rates and for the measured time period.

The same EV customer drives to a friend's home (who also has an EV) and requests a quick charge to make sure that he can get back home. When he plugs his EV into his friend's EV charger, the utility identifies the fact that the EV belongs to a different customer and places the charging bill on the correct person's invoice.

As part of the programme the utility wishes to capture behavioural and movement patterns in order to better schedule charging times.



Electric Vehicle (EV)

An electric vehicle (EV), also referred to as an electric drive vehicle, uses one or more electric motors or traction motors for propulsion. An electric vehicle may be powered through a collector system by electricity from off-vehicle sources, or may be self-contained with a battery or generator to convert fuel to electricity. EVs include road and rail vehicles, surface and underwater vessels, electric aircraft and electrically powered space vehicles.

Utility or Energy Provider (EP)

An electric utility is an electric power company (often a public utility) that engages in the generation, transmission, and distribution of electricity for sale generally in a regulated market. The electrical utility industry is a major provider of energy in most countries. It is indispensable to factories, commercial establishments, homes, and even most recreational facilities. Lack of electricity causes not only inconvenience, but also economic loss due to reduced industrial production.

Smart Meter (SM)

A smart meter is usually an electronic device that records consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing. Smart meters enable two-way communication between the meter and the central system. Unlike home energy monitors, smart meters can gather data for remote reporting. Such an advanced metering infrastructure (AMI) differs from traditional automatic meter reading (AMR) in that it enables two-way communications with the meter.

Charging station (CS)

An electric vehicle charging station, also called EV charging station, electric recharging point, charging point, charge point and EVSE (Electric Vehicle Supply Equipment), is an element in an infrastructure that supplies electric energy for the recharging of plug-in electric vehicles, including all-electric cars, neighbourhood electric vehicles and plug-in hybrids.

Inventory: Provide an inventory of the capabilities and applications review at the level of granularity appropriate for the analysis covered by the methodology and define a High Level Functional Specification which will guide subsequent analysis. In order to facilitate the analysis described in the “Detailed privacy and security analysis” (section 6.2.4), the components of the Inventory should align as closely as possible with the components that will be analysed in the corresponding detailed analysis.

Systems: *Electric Vehicle, GreenPriTech network, EV charging point, GreenPriTech billing and charging scheduling system…*

Policy*: “GreenPriTech has a published Privacy Policy covering the EV recharging/billing application”*

Personal data: *each EV, GreenPriTech customer and GreenPriTech charging station has its own ID that can be associated to a data subject,*

Communication: *communication between the charging stations and GreenPriTech customer billing systems relies on GreenPriTech own network based on Power Line Communication (PLC) technology.*

Customer policies: *GreenPriTech allows customer to select their privacy options via customer-facing interfaces*

Assessment Preparation: Prepare an initial privacy impact assessment, or as appropriate, a risk assessment, privacy maturity assessment, compliance review, or accountability model assessment applicable within the scope of analysis carried out during the functional description, inventory and the privacy and security policy conformance criteria establishment. Such an assessment can be deferred until a later iteration step or inherited from a previous exercise.

Assessment Preparation:

A system as the one described above presents a set of risks for privacy:

•Direct EV identification: EV may be directly linked to individuals;

•Charging location identification: stemming from the ability to link customers and their vehicles to geo-located charging points may reveal many things from one person;

Potentially this information may be available to the utility and the third party organizations.

Also, scheduling vehicle's charging times expose behavioural patterns to the utility, which poses privacy invasion risks: e.g. a customer that charges the vehicle every night and modifies this for one specific night reveals that the customer will not be at home that night.

While this information is key to address electricity-demand peaks, to provide electricity in a more efficient way and providing customers with better prices, the system must be designed to minimize or completely avoid these potential risks.

Article 33 of the forthcoming EU GDPR mandates the carriage of an assessment of the envisaged processing operations on the protection of personal data whenever the processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.

In order to determine if processing operations present such impacts an initial assessment should be conducted, following best practices guidelines such as the ones developed within PIAF project[19] or to the RFID PIA framework[20].

This process is addressed in sections A.6 of the template

6.2.2 Legal assessment

The legal assessment of the system is a process which is relevant to the whole system development lifecycle and starts in the very early stage of the process. Its objective is to ensure the proposed technology, service, or programme complies with legislation. This requires a three-step approach:

- The identification of the relevant privacy principles according to the legal framework;
- The identification of legal requirements that the system will have to comply with in order to be legally compliant, taking into account the information flows and potential risks

[19] http://www.piafproject.eu/ref/PIAF_D3_final.pdf

[20] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

- Evaluate whether the final implementation of the technology, service or programme is compliant with privacy legislation. This analysis measures whether the project or technology is compliant with privacy principles in relevant data protection legislation.

Legal assessment				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Project managers, PSMOs	Project description Relevant legislation Soft Law	Analysing the project to make sure it is compliant, including 'soft law' e.g. EDPS and Article 29	Privacy principles Legal requirements Compliance analysis	Project manager, system engineers, end users
Tools & Techniques	Privacy principle checklist/table threats, vulnerabilities, risks & solutions			
Knowledge	Knowledge and understanding of relevant privacy legislation, Article 29 opinions, EDPS opinions, national legislation			
Responsible	Project manager supported by legal staff			

This process involves compiling a list of privacy principles and legal requirements according to relevant legislation and soft law (such as the Article 29 opinions), against which to measure the proposed project, technology or service. This process also involves providing a justification for those areas inscribed in law, or soft law, defined as inapplicable or irrelevant for the proposed project, technology or service (i.e. if the privacy principle is not relevant, then the organisation needs to explain why it is not relevant). The resulting compliance analysis could also include a preliminary assessment of risks and possible solutions in terms of legal compliance. An example of a legal compliance checklist is provided by the UK Information Commissioner's Office[21].

In the case of GreenPriTech, the project manager with the help of legal experts compiles a list of privacy principles, drawn from relevant legislation, such as the EU Data Protection Directive 95/46/EC and the draft GDPR, and soft law, such as the Article 29 Working Party Opinion on smart metering[22], in a checklist in order to determine whether, and to what extent, the proposed project, technology or service complies with existing legislation, including any relevant soft law. The organisation particularly seeks to comply with data protection legislation relevant to smart metering. Once the checklist has been completed, the organisation seeks to undertake a preliminary risk assessment and develop a range of solutions to mitigate any risks identified.

A list of other regulations which may affect the system is also compiled:

- EU Data Protection Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281 31).

[21] http://ico.org.uk/pia_handbook_html_v2/html/0-advice.html
[22] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp183_en.pdf

- Transpositions of the directive into national laws of EU member states (e.g. Spanish Royal Decree 1720/2007, of 21 December, which approves the regulation implementing the organic law 15/1999, of 13 December, on the protection of personal data)

- Commission Regulation (EU) No 627/2014 of 12 June 2014 amending Regulation (EU) No 582/2011 for the purposes of adapting it to technical progress as regards particulate matter monitoring by the on-board diagnostic system

- Mandate M/468 for electric vehicles - European Commission

Identified data protection principles:

Data must be:

- Fairly and lawfully processed

- Processed for limited purposes

- Adequate, relevant and not excessive

- Accurate

- Not kept for longer than necessary

- Processed in accordance with the individual's rights

- Secure

- Not transferred to countries without protection.

This process is addressed in sections A.7.1 and A.7.2 of the template

Article 33 of the EU GDPR proposal, as approved by the European Council[23], **mandates the carriage of a Data Protection Impact Assessment whenever the type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage**s. Such assessment "shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

[23] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

There are some guides which can help to identify the aspects that should be considered during a legal check:

- The PACT project (D5.1) lists criteria that should be included in a legal compliance checklist. These criteria[24] include reference to: assets/rights to be respected; EU regulatory acts on specific sectors; national legislation on specific sectors; notification' binding specific rules; and potential implications/sanctions.
- ENISA's cloud computing information assurance framework[25] includes in its section 6.10 key legal questions that organizations should ask their cloud providers in order to identify potential legal issues.

6.2.3 Privacy and security plan preparation

Projects taking into account privacy from the onset must consider the resources needed for such purpose as well as planning necessary actions, and how they interact with organizations practices, to achieve privacy and business goals

An organisation should carry out a threshold analysis based on previously collected information in order to determine whether, what and with what scope PRIPARE processes are necessary. Once following privacy- and security-by-design methodologies has been deemed as necessary, the organisation should determine the appropriate scale of the process to be undertaken. An organisation also needs to determine the roles and responsibilities for staff working within the organisation with regard to the process, including who should carry it out and who should approve it. A privacy and security team should be assembled, including people with a range of expertise, such as: information security experts, lawyers, ethicists, audit personnel, communications professionals, and so on.

It can be assumed that most organisations use project management techniques or risk management techniques. Section 7 provides a guide on how to merge PRIPARE with existing engineering and project management practices.

Privacy and security plan preparation				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Project manager, PSMOs	Project information/information flows	Identify itineraries or processes, and their scope. Assess PRIPARE's processes with the organisation's own standards and practices. Distribution of roles and responsibilities/assembling the security and privacy team	Results of threshold analysis, determining the privacy and security roadmap. Privacy and	System engineers, internal & external stakeholders

[24] http://www.projectpact.eu/deliverables/wp5-new-conceptualization-and-framework/d5.1/D5.1.pdf

[25] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport

			security team	
Tools & Techniques	Threshold analysis			
Knowledge	PRIPARE methodology and processes and itineraries. Business domain of the project, privacy and security risks			
Responsible	Project manager, PSMO			

The itinerary or processes selected will be developed in accordance to the initial impact assessment which includes: the potential privacy and security risks; the amount of personal data collected or processed; the sensitivity of such data; the size of the organisation and its capabilities; and the organisation's commitment to protect personal data. These issues will determine the scope and scale of the itinerary of processes.

GreenPriTech has chosen to follow a 'full heavyweight itinerary' due to the range and number of potential privacy impacts that could arise in relation to the project. GreenPriTech must comply with EU legislation and has a strong commitment to the protection of personal data. GreenPriTech follows will follow an iterative methodology with three monthly iterations.

This process is addressed in sections A.2 and A.4 of the template.

6.2.4 Detailed privacy analysis

Any project with potential privacy and security issues should conduct a detailed privacy analysis in order to provide an inventory of personal data, sub-systems, etc. that may be subject to privacy or security risks

The objective of this process is to document and detail the application or business service in which personal data is associated and fully understand the environment on which it will be operated and its constraints.

Detailed Privacy Analysis				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Project Manager, PSMOs, Business & System Analyst	• High level privacy analysis • Business analysis • Legal framework	• Identify stakeholders, systems, domains and domain owners, roles and responsibilities, touch Points and data flows • Identify personal data in Privacy Domains and	Detailed privacy analysis: • Stakeholders , Systems, Domains and Domain Owners, Roles and Responsibilities, Touch Points and Data Flows • Personal data • Privacy Controls	System engineer, DPAs PSMOs

		Systems - Specify Required Privacy Controls Associated with personal data		
Tools & Techniques	UML, UP, RUP, OUM, user stories, narrative…			
Knowledge	System's domain, applicable legislation and good practices			
Responsible	Business & System Analyst			

As in the high level analysis, it is important to reflect all stakeholders' points of view in this analysis.

This process has three main activities:

1. Identify stakeholders, systems, domains and domain owners, roles and responsibilities, touch Points and data flows

"**Stakeholders** are all those who are creating, managing, interacting with, or otherwise subject to, personal data managed by a system within a privacy domain."

Stakeholders: *registered customers, registered customer host (temporary host for EV charging), registered customer guest, GreenPriTech and advertiser.*

"**System** is a collection of components organized to accomplish a specific function or set of functions having a relationship to operational privacy management."

Systems: *EV ID provider, EV on board system, customer's communication portal, mobile device, customer's EV charging system, customer's metering system, advertising system, billing system, EV load scheduler system, EV program information system, pattern analysis system.*

"A **domain** covers both physical areas (such as a customer site or home) and logical areas (such as a wide-area network or cloud computing environment) that are subject to the control of a particular domain owner."

GreenPriTech's domain: *includes the physical premises of GreenPriTech's, the network used to transport electricity and data, the logical systems which the enable the ubiquitous smart charging (e.g. billing system and EV load scheduler system), the communication portal and the charging and metering systems located in customer's physical premises. It also includes the on-board system which is installed in the EV.*

Customer's domain: *its physical premises, the electric vehicle and its mobile device.*

Advertiser's domain: *includes the advertiser's physical premises and its advertising systems.*

EV manufacturer's domain: *the EV id provider*

ISP: the network used to transmit adds to the user

"For any given use case, identify the **roles and responsibilities** assigned to specific Participants and Systems within a specific privacy domain"

EV Manufacturer Privacy Officer: Ensure that all personal data flows from EV On-Board System conform to contractual obligations associated with the Utility and vehicle owner as well as the data protection principles such as data minimisation.

"Identify the **touch points** at which the data flows intersect with Privacy Domains or Systems within Privacy Domains."

The Customer Communication Portal provides an interface through which the Customer communicates a charge order to the Utility. This interface is a touch point.

When the customer plugs into the charging station, the EV On-Board System embeds communication functionality to send EV ID and EV Charge Requirements to the Customer Communication Portal. This functionality provides a further touch point.

"Identify **the data flows** carrying personal data and privacy constraints among domains in the system or business process."

When a charging request event occurs, the Customer Communication Portal sends Customer information, EV identification, and Customer Communication Portal location information to the EV Program Information System managed by the Utility.

This application uses metadata tags to indicate whether or not customer' identification and location data may be shared with authorized third parties, and to prohibit the sharing of data that provides customers' movement history, if derived from an aggregation of transactions.

2. Identify personal data in privacy domains and systems

"Specify the personal data collected, created, communicated, processed or stored within Privacy Domains or Systems in three categories:

- Incoming personal data: flowing into a Privacy Domain, or a system within a Privacy Domain.
- Internally generated personal data: created within the Privacy Domain or System itself.
- Outgoing personal data: flowing out of one system to another system within a Privacy Domain or to another Privacy Domain".

Incoming personal data: "Customer ID received by Customer Communications Portal."

Internally generated personal data: "Current EV location associated with customer information, and time/location information logged by EV On-Board system".

Outgoing personal data: "Current EV ID and location information transmitted to Utility Load Scheduler System".

It is very important to identify and classify personal data in terms of its identifiability and sensitivity. The HIPAA Privacy Rule[26] provides a list of identifiers that should be removed in order to avoid identifiability. ISO 29100 also provides a method (and examples) to determine what personal data can lead to identification of data subjects and should be especially avoided.

Current EU DPD[27] state in its Article 8 that “Member States **shall prohibit** the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life”.

The version of Article 9 of the EU GDPR draft, as adopted by the European Parliament[28], clearly states that “The processing of personal data, revealing race or ethnic origin, political opinions, religion or philosophical beliefs, sexual orientation or gender identity, trade-union membership and activities , and the processing of genetic or biometric data or data concerning health or sex life, administrative sanctions, judgments, criminal or suspected offences, convictions or related security measures **shall be prohibited**“

The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. Article 29 Data Protection Working Party has issued an Opinion with its view in Anonymisation Techniques[29] which describes that “anonymity requires that data should be such as not to allow the data subject to be identified via ‘all’ ‘likely’ and ‘reasonable’ means. It also includes most common anonymisation techniques with its strengths and weaknesses.

3. Specify required privacy and security controls associated with personal data

“For Incoming, Internally Generated and Outgoing personal data, specify the privacy and security controls required to enforce the privacy and security policies associated with the personal data. Privacy and security controls may be pre-defined or may be derived. In either case, privacy and security controls are typically associated with specific data protection and security principles that apply to the personal data. Privacy and security controls can be classified into:

- Inherited: those which are inherited from Privacy Domains or Systems within privacy domains;
- Internal: those which are mandated by internal Privacy Domain policies;
- External: those which must be exported to other privacy domains or to systems within privacy domains;”

[26] http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/

[27] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=en

[28] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN

[29] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

Inherited privacy controls

"The utility inherits a privacy control associated with the Electric Vehicle's ID (EVID) from the vehicle manufacturer's privacy policies.

The utility inherits the consumer's operational privacy control requirements, expressed as privacy preferences, via a link with the customer communications portal when she plugs her EV into the customers' host charging station.

The utility must apply customer's privacy preferences to the current transaction. The Utility accesses customer's privacy preferences and learns that the customer does not want her association with customer's hosts exported to the Utility's third party partners. Even though customer host's privacy settings differ around his personal data, customer's non-consent to the association being transmitted out of the Utility's privacy domain is sufficient to prevent commutative association. Thus if the customer host were to charge his car's batteries at customer's place, the association between them would also not be shared with third parties."

Internal privacy controls

The Utility complies with the Spanish Royal Decree 1720/2007, of 21 December, which approves the regulation implementing the organic law 15/1999, of 13 December, on the protection of personal data.

It complies with Article 8 of the ECHR, a right to protection against the collection and use of personal data forms part of the right to respect for private and family life, home and correspondence.

It implements CEN-CENELEC-ETSI Smart Grid Coordination Group's Smart Grid Information Security recommendations[30]*.*

Further, it adopts NIST 800-53 Appendix J's "Control Family" on Use Limitation – e.g. it evaluates any proposed new instances of sharing personal data with third parties to assess whether they are authorized and whether additional or new public notice is required.

External privacy controls

The Utility exports customer's privacy preferences associated with her personal data to its third party partner, whose systems are capable of understanding and enforcing these preferences. One of her privacy control requirements is to not share her EVID with marketing aggregators or advertisers.

This process expects to reflect the identified stakeholders, systems, domains and domain owners, roles and responsibilities, touch Points, data flows and personal data flows in sections A.6.1 through A.6.5 of the template.

Identified privacy controls should be directly included in section A.10.

Article 33 of the EU GDPR, as approved by the European Council[31], **mandates the carriage of a Data Protection Impact Assessment whenever the type of processing, in particular using new technologies, and taking into account the**

[30] http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_security.pdf

[31] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, [breach of (…) pseudonymity], loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantages. Such assessment "shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.

6.2.5 Operationalization of Privacy Principles

Any project aiming to embed privacy and security principles should follow this operationalizing process

The goal of operationalizing privacy principles is to identify the specific privacy requirements the system should meet, by mapping high-level, legal and user concerns onto engineering requirements. The operationalization replaces the abstract privacy principles with the effects that result from applying them, which must be well defined, empirically observable and objectively measurable. Privacy specification thus becomes a set of operational requirements.[32]

PRIPARE requirement operationalization process departs from a standardized **catalogue of privacy requirements**, which are stakeholder-neutral, structured, hierarchized, and prioritized; together with the system specification, architecture and privacy impact analysis; to reach a specific set of requirements applicable to the system under development. Requirements are organized into a five-layer, successively refined model (see Figure 5), from abstract principles and guidelines, to objective and operable definitions for privacy conformance criteria, and to design techniques and test procedures.

[32] An extended guide on operationalizing Privacy by Design principles by the Information and Privacy Commissioner of Ontario may be found at http://www.ipc.on.ca/images/Resources/operationalizing-pbd-guide.pdf

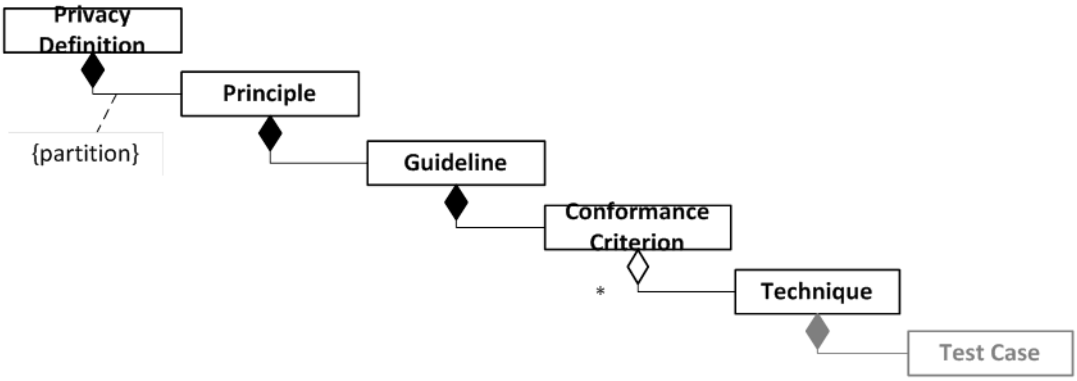


Figure 5: Structured decomposition of privacy principles into requirements.

The process presented here deals with the four top layers (from the definition of privacy to conformance criteria), and is typically performed by a system analyst who has the expertise to specify non-functional requirements and the knowledge of the system drawn from having defined its functional specification. This process will later be complemented with the Privacy-Enhancing Detailed Design (see section 6.3.2), which deals with the bottom layers, and will be introduced later (Operationalization of Privacy Principles deals with requirements –i.e. the 'what'–, while Privacy-Enhancing Techniques deal with design –the 'how'–).

<table>
<tr><th colspan="5">Privacy Requirements Operationalization</th></tr>
<tr><th>Suppliers</th><th>Inputs</th><th>Process</th><th>Outputs</th><th>Consumers</th></tr>
<tr><td>- Business & System analysts
- Data Protection Authority
- Privacy Managers & Officers</td><td>-Functional description of the system
- Stakeholders , Systems, Domains and Domain Owners, Roles and Responsibilities, Touch Points and Data Flows
- Privacy principles</td><td>- Identify principles and guidelines
- Determine applicability of privacy conformance criteria</td><td>- Privacy requirements as a set of applicable conformance criteria</td><td>System designer
Project managers</td></tr>
<tr><td><b>Tools &amp; Techniques</b></td><td colspan="4">Family of guidelines and privacy conformance criteria.</td></tr>
<tr><td><b>Knowledge</b></td><td colspan="4">Guidelines, privacy conformance criteria, and mapping from principles to those.</td></tr>
<tr><td><b>Responsible</b></td><td colspan="4">Business & System analysts</td></tr>
</table>

The overall process selects, from a given set of heuristically-predefined privacy requirements, those that should be designed and implemented, starting from the set of privacy principles to be applied and successively refining them; while considering the functional description of the system, its boundaries, data flows and the privacy roles involved. This includes two steps:

1. Identify externally defined principles (quality attributes) and guidelines employed to define privacy requirements.

2. Determine the applicability of privacy criteria according to: the functional specification, other competing quality attributes, and the level of conformance desired.

Step 1: Identify principles and guidelines

Starting from the quality attributes yielded by the high-level privacy analysis, the first step in the path to operationalize privacy into concrete requirements is the definition of the category of privacy as a set of privacy principles which delimit its scope.

A **privacy principle** is both an essential consequence of privacy that defines its foundations and a feature that a system must compulsorily exhibit to respect the user's privacy. That is, a system is privacy-friendly if and only if it abides by the privacy principles designated as such. Privacy principles are usually defined together with one another within a family of principles: a family represents a partition of the concept of privacy into a set of principles which are pairwise disjoint and collectively exhaustive. Several conceptualizations for privacy exist, and consequently several families of principles have been developed from different legal, industrial and academic origins[33].

While PRIPARE has been designed to work with different sets of principles, the process itself was developed to be compliant and is fully compatible with EU GDPR data protection principles. However and given the engineering focus of ISO's privacy framework, ISO 29100[34] privacy principles will be used to illustrate the operationalization process. These are, namely:

1. Consent and choice
2. Purpose legitimacy and specification
3. Collection limitation
4. Data minimization
5. Use retention and disclosure limitation
6. Accuracy and quality
7. Openness, transparency and notice
8. Individual participation and access
9. Accountability
10. Information Security
11. Privacy compliance

Principles are then specified into **guidelines**. A guideline provides specific goals that organizations must work towards so as to meet a principle. Each principle is decomposed into a fixed, mandatory set of guidelines, which refine them with specific objectives, and serve as a framework for the lower layers. Based on different sources, we have compiled a set of privacy

[33] Different families of privacy principles have been compiled and compared by the American Institute of CPAs (http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/InternationalPrivacyConcepts.aspx) and the International Security, Trust and Privacy Alliance (http://xml.coverpages.org/ISTPA-AnalysisOfPrivacyPrinciplesV2.pdf).

[34] The 11 privacy principles of ISO 29100 – Privacy Framework, http://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip

guidelines that develop ISO 29100 privacy principles, but other families of guidelines might also be applied[37].

Annex B provide a list of privacy principles, guidelines and criteria of requirements.

In an initial version of the methodology, PRIPARE identified 14 principles: (1) data quality, (2) data minimization and proportionality, (3) purpose specification and limitation (finality or legitimacy), (4) purpose specification and limitation for sensitive data, (5) transparency and openness, (6) right of access, (7) right to object, (8) confidentiality and security, (9) compliance with notification requirements, (10) limited conservation and retention, (11) accountability, (12) right to erasure, (13) privacy and data protection-by-design, (14) privacy and data protection-by-default. The PRIPARE set of privacy principles were directly extracted from the study of the GDPR. We have decided to adopt ISO29100 for the following reasons:

- ISO29100 is the international privacy framework standard,
- It is a reference document that can be used by privacy engineers (rather than a legal document).

Nonetheless, if the regulatory or the corporate context required abiding by any other family of principles, then the operationalization process we present here might be easily re-adapted.

Directive 95/46/EC (**"Data Protection Directive")** established a set of general rules for lawful processing of personal data in its Chapter II: data quality[39] (which includes fairness and lawfulness of processing; purpose specification, explication and legitimacy; adequacy, relevance and moderation to purpose; and expiration), rules for special categories of personal data, information to the data subject, right of access, right to object, confidentiality and security, and notification (contents, prior checking and publicizing).

The **proposal for a General Data Protection Regulation** reorganizes these existing principles, adding some new ones and reformulating existing ones, reinforcing them:

- Chapter II establishes the **principles for personal data processing**: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage minimisation; and securitySpecial consideration is given to lawfulness, consent, children's data and special categories of data and criminal data.
- Chapter III establishes the **principles for the rights of the data subject**: transparent information and communication, notification requirement, information policies, information to the data subject, right to access and to obtain data, right to rectification, right to erasure and "to be forgotten",

[37] For instance, https://cloudsecurityalliance.org/research/ccm/

[39] https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/74#data_quality

right to restriction of processing, right to object, and right to not to be subject to automated individual decision.

- Chapter IV establishes the **obligations for the data controllers and processors**: responsibility and accountability, data protection by design and by default, documentation, cooperation with the supervisory authority, security of processing, notification and communication of breaches, risk analysis, impact assessment, compliance review, and prior consultation.

Principles and guidelines are compulsory: a system can only respect user privacy if it abides by all of them.

Nonetheless, the process itself does not mandate the family of principles and guidelines to be applied. The first step consists indeed in determining which of the principles should be applied, as established by the legal, regulatory and policy context, which ultimately set the definition of privacy which the organization abides by. PRIPARE uses ISO 29100 Privacy Framework principles; other principles can be used by projects in need to comply with the respective regulations.

Note that the proposed operationalisation process takes into account the three privacy protection objectives defined by ULD[40]

Unlinkability	Ensures that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended.
Transparency	Ensures that all privacy-relevant data processing including the legal, technical and organizational setting can be understood and reconstructed.
Intervenability	Ensures that data subjects, operators and supervisory authorities can intervene in all privacy-relevant data processing.

Step 2 - Determine the applicable privacy criteria

Once the principles and guidelines to be applied have been chosen, the next step consists in determining the applicable privacy requirements that characterize the system's behaviour from the privacy perspective. Their applicability depends on the functional description of the specific system under development, the data flows and related concepts (stakeholders, system boundaries, domain and domain owners, roles and responsibilities, processes, touch points) and the level of conformance this system will abide by.

Guidelines are not yet directly testable as is; hence each of them needs to be refined into a set of detailed criteria whose success can be objectivized. **Privacy conformance criteria** define technical and organisational requirements that systems and organizations need to meet in order to address privacy issues. Privacy criteria are defined by technology-neutral statements, which the system user might observe, and which can be objectively tested and/or measured. Being objective does not imply being automatable. Rather, the criteria can be regarded as a list of check-points to be met, which can be checked against and assessed to determine the system compliance —human judgment will be needed in order to validate many of them, although

[1] [40] Marit Hansen, Meiko Jensen, Martin Rost: "Protection Goals for Engineering Privacy"; in 2015 International Workshop on Privacy Engineering (IWPE). http://ieee-security.org/TC/SPW2015/IWPE/2.pdf

automatic software tools may help determine conformance. The assessment of the system compliance regarding these check-points will occur during the system verification phase (see section 6.5).

Following the same process shown above for guidelines, PRIPARE has compiled a list of privacy criteria applicable to different situations. Next we show **some example criteria** corresponding to ISO 29100 privacy principle 4 (data minimization)[41].

4. Data minimization

G-4.1. Avoid and minimise the use of personal data along its whole lifecycle:

C-4.1.1. Keep only the strict minimum data necessary for the strictly specific, consented, minimal purposes.

C-4.1.2. Periodically evaluate that all the personal data held by the organization is identified in the privacy notice and necessary for the specified purposes.

C-4.1.3. When some personal data is no longer needed for the specified purpose, delete or anonymise it.

C.4.1.4. When some personal data is no longer needed for the specified purpose, delete or anonymise all the back-up data corresponding to that personal data.

C-4.1.5. When retention rules prevent unnecessary personal data from being deleted, exclude it from regular processing of personal data.

C-4.1.6. - When doing testing, training and research: Apply procedures to minimise personal data.

G-4.2. - Limit the ability of external parties from inferring personal data from sources coming from different controllers.

C-4.2.1. - Keep data from different services or different parties separated, and avoid combining them.

C-4.2.2. - Reliably separate personal data on the same device which belongs to different issuers or owners.

C-4.2.3. - Prevent unauthorized parties from tracking personal data.

C-4.2.4. Restrict the parties (either legal entities or natural persons, including employers and contractors) that may gain access to personal data, and keep the data they can access to the minimum they need to know in order to fulfil their legitimate purposes.

G-4.3. Minimize the traces left by transactions and interactions with a system or service:

C-4.3.1. When the data subjects perform a transaction or otherwise interact with the system, ensure that any information associated to that event does not disclose the identity of the data subjects, and allows them to remain anonymous.

C-4.3.2. When the data subjects perform a transaction or otherwise interact with the system, ensure that no two transactions by the same data subject can be linked with each other.

C-4.3.3. When the data subjects perform a transaction or otherwise interact with the system, ensure that no other party can ascertain or observe whether the transaction has happened.

[41] See annex B

The definition of a privacy criterion may only be applicable to specific system functions: those systems which do not exhibit these functions are deemed to have met the respective criterion. Consequently, before imposing each criterion, it must be **determined whether it applies** to the system under development (e.g. if the system does not include the functionalities a criterion refers to, then there is no need to apply it). This depends on which domain's perspective we are studying the system: some criteria may pertain to one subsystem but not the others, some to all the subsystems, and yet some others may pertain to none.

Each criterion has a **level** of relevance assigned: "I" (most relevant and essential), "II", and "III" (not so relevant). Accordingly, a system may hold one of three levels of conformance: Level I (minimum) implies fulfilling all the Level I privacy criteria, Level II (medium) implies fulfilling both Level I and Level II criteria, and Level III implies fulfilling all the criteria. Thus, if some part of a system fails a privacy conformance criterion for some level X, then the system as a whole does not meet that level X. That is, conformance can only be measured at an ordinal scale (none, level I, level II, or level III), while statements such as "60% privacy-friendly" do not make sense in this framework. Levels of conformance can be reused by privacy certification seals, computer-automated privacy level negotiations, etc. Privacy criteria are usually independent of one another, but it may also be sometimes the case that two privacy criteria are similar in content, one of them being more stringent than the other, and having a tighter level associated.

The concept of different levels of privacy protection is adopted by different legislations and regulations, which usually attach it to different degrees of sensitivity of personal data: tighter requirements are established for the treatment of sensitive personal data. In the EU, Article 8 of the Data Protection Directive 95/46 establishes the categories of sensitive data, to be extended by the final version of Article 9 of the EU GDPR.

PRIPARE levels may be determined from examining the applicable legislation, together with internal policies or regulations.

6.2.6 Risk management

Any project with potential privacy and security issues should follow a risk management process in order to determine the assets to protect, the threats and risks that may pose, and the measure to address the discovered risks.

The main goal of this process is to identify the privacy risks associated with the system and to suggest treatments to address these risks. This process is instrumental in establishing a link between the high-level functional description and actual operational requirements of the system.

Risk Management				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**

Project managers **PSMO**	Functional requirements (external) Context (external) Assets at stake (external)	Step 1. Identify feared events Step 2. Identify threats Step 3. Identify risks Step 4. Identify treatments	Feared events Feared threats Initial risks Privacy & Security requirements Remaining risks	PSMO System engineers
Tools & Techniques	CNIL's PIA Manual[42], LINDDUN[43]			
Knowledge	Risk analysis methodologies, privacy threats			
Responsible	Privacy expert			

The main goal of this process is to help decision makers assess the risks and address them. It is also useful to enhance the communication about risks within a company and outside.
The main steps are the following:

Definition of "feared events" (events against which the system must be protected)

Amounts to define precisely for each asset the expected privacy guarantees (confidentiality, anonymity, unlinkability, etc.) and the impact of any breach of these guarantees (on the individual). These feared events are closely related and basically stem from the principles which govern the organization and the system.

All identified events must be categorized in terms of its potential impact, estimating the impact on the data subject and/or the organization if this event was to happen. This potential impact is heavily linked to the amount, the sensibility and identifiability characteristics of the leaked data. PRIPARE proposes two different approaches to estimate this potential impact (severity), the one proposed by CNIL in its privacy risk assessment manual or a second one which is proposed by the BSI in their Privacy Impact Assessment guidelines[44].

Definition of the threat scenarios (scenarios which can give rise to a feared event)

All threats, which are related to specific feared events, are characterized by two parameters: their source ("attacker") and the vulnerabilities of the system that they exploit. Each of these parameters can be estimated and, combined, links each of the threats to an estimation of it happening probability (likelihood).

Risk assessment based on the feared events and the threat scenarios

This step also defines the methodology to assess the risks based on their likelihood and the severity of their potential impact. It is proposed to map severity and likelihood to an overall risk value by following Table 2:

[42] http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf

[43] https://distrinet.cs.kuleuven.be/software/linddun/

[44]https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/PIA/Privacy_Impact_Assessment_Guideline_Kurzfasssung.pdf?__blob=publicationFile

Severity

Maximum	🟧	🟧	🟥	🟥
Significant	🟧	🟧	🟥	🟥
Limited	🟩	🟩	🟨	🟨
Negligible	🟩	🟩	🟨	🟨
	Negligible	Limited	Significant	Maximum

Likelihood

Table 2: Risk Map

Objectives may be set based on where risks are located on the map:

- **Maximum:** Risks with a high severity and likelihood must absolutely be avoided or reduced by implementing measures that reduce both, their severity and their likelihood;
- **Significant:** Risks with a high severity but a low likelihood must be avoided or reduced by implementing measures that reduce both, either their severity or their likelihood;
- **Limited**: Risks with a low severity but a high likelihood must be reduced by implementing measures that reduce their likelihood;
- **Negligible**: Risks with a low severity and likelihood may be taken;

Measure definition

The last step is to identify appropriate treatments, which help to achieve the objectives set in the previous step for the already mapped risks. In traditional risk management there are four different strategies to follow when facing risks:

- Avoid the risk by changing the activity/project to circumvent the problem;
- Accept risk whenever this one is acceptable (under certain levels);
- Transfer the risk to a third party;
- Mitigate the risk by identifying specific requirements.

PRIPARE, in order to avoid trade-offs, focuses on the mitigation treatments by selecting requirements which then must be met by specific privacy controls. Elicited requirements must be linked to the risks they address and how they modify their severity and likelihood parameters. This process should continue until all risks reach a level considered acceptable.

Addressed privacy risks should not disappear from the sight of project managers, PSMOs or privacy engineers; this could cause to dismiss potential risks because they were already perceived as resolved. Even if a risk has been mitigated, this does not mean that it does not exist nor that it was mitigated using the most effective control. Hence the need of having risks (addressed and non-addressed) always accessible and considered.

Several sources can and should be consulted in order to guide practitioners in the discovery of feared events and their impact, threats and their probability or measures which mitigate risks. Examples of this sources are:

- OWASP Top 10 Privacy Risks Project[45]: list of the top 10 privacy risks in web applications and possible counter-measures covering technological and organizational aspects like missing data encryption or the lack of transparency;
- CNIL Privacy Impact Assessment methodology[46] which includes a catalogue of generic threats;
- CNIL catalogue of measures for the privacy risk treatment[47];
- LINDDUN provides a threat modelling approach[48] that is based on a categorization of threats (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, Noncompliance) associated with a system description based on data flow diagrams (LINDDUN methodology therefore spans over the analysis and the design process).
- JRC's report on RFID Tags Privacy threats and countermeasures[49]: which presents a list of potential threats and measures for RFID Tags technology
- ENISA's cloud computing information assurance framework[50] includes in its section 6 key questions that will help practitioners to discover risks for systems operating in the cloud.
- Cloud Security Alliance provides a controls framework[51] in 16 domains mapped to other initiatives and standards (e.g. PCI DSS, ISO27001 or European Union Data Protection Directive 95/36/EC) and which might guide practitioners to identify relevant privacy controls.
- ISO 29134 includes a list of generic threats to personal data.
- WP29's Statement on the role of a risk-based approach in data protection legal frameworks[52]. It identifies a set of objective criteria that should be considered during the risk assessment: nature of personal data, category, number of data

[45] https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project#tab=Top_10_Privacy_Risks
[46] http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-1-Methodology.pdf
[47] http://www.cnil.fr/fileadmin/documents/en/CNIL-PIA-3-GoodPractices.pdf
[48] https://lirias.kuleuven.be/bitstream/123456789/472921/1/wuyts2014_thesis_online.pdf
[49] https://ec.europa.eu/jrc/sites/default/files/jrc78156_report_rfid_en.pdf
[50] https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport
[51] https://cloudsecurityalliance.org/research/ccm/
[52] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

subjects affected, the purpose of the processing, along with the severity and likelihood of the impact. The same reference remarks that Data Protection rules still apply to pseudonymised and encrypted data and should be considered during the risk assessment

- IAB's Privacy Considerations for Internet Protocols[53] , which offers guidance for developing privacy considerations for inclusion in protocol specifications.

Feared event: *an example of feared event for the GreenPriTech project is the profiling of the car owners by the electricity supplier and the use of such profiles in targeted advertising. The impact for the driver can be considered as high because the profiles could involve sensitive information (such as health condition, sexual preferences or religion).*

Threat scenario: *the electricity provider could store the location of the places where the driver recharges the battery of his vehicle and sell these traces to an ad broker. The broker can analyse these locations using maps with the points of interest in the nearby and build a profile of the driver based on this information. The likelihood of the risk can be considered as high because the benefit can be significant for the electricity provider and the attack is easy to conduct if no countermeasure is implemented.*

Risk assessment: *the risk is maximum because both the potential damage and the likelihood are high.*

Mitigation measures: *the risk must be mitigated. Potential measures include the use of protocols minimizing the disclosure of personal information, anonymous credentials, anonymous communication channels as suggested in the POPCORN protocol*[54]

Article 30 of the EU GDPR, as it appears in the draft approved by the European Council[55], clearly state that "Having regard to available technology and the costs of implementation and taking into account the nature, scope, context and purposes of the processing as well as **the likelihood and severity of the risk** for the rights and freedoms of individuals, the controller and the processor shall implement appropriate technical and organisational measures (…) to ensure a level of security appropriate to the risk.
In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by data processing (…), in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed "

This process is addressed in sections A.7.3, A.7.4 and A.7.5 of the template.

Any relevant decisions regarding the remaining risk or the selected mitigation measures should be addressed in the design logbook (section A.9 of the template).

[53] https://tools.ietf.org/html/rfc6973
[54] https://www.pvib.nl/download/?id=17691267
[55] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

6.3 Design

While the analysis phase focuses on what has to be built, the design phase focuses on how it has to be built. The design of a system is the "process of defining the hardware and software architecture, components, modules, interfaces, and data for a system to satisfy specified requirements"[56].

Figure 6 highlights design applied to privacy. The analysis phase provides operational requirements on privacy controls. The design phase involves technical decisions that will lead to the specification of privacy enhancing techniques. The specification of these techniques will involve architecture decisions or privacy enhancing architectures (PEARs).

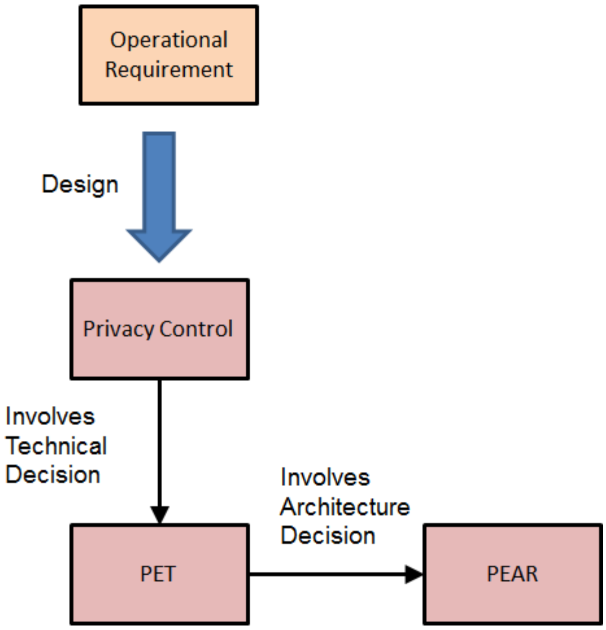


Figure 6: Privacy Control Design

The design of a system provides an abstract representation of a solution to meet its requirements previously specified. It defines the system structure and behaviour so as to enable its functionalities and satisfy other requirement categories (e.g. privacy). This implies defining:

- the system components, their organization, their internal and external interfaces, and the relations among them;
- the structure, representation and semantics of the data processed by the system (including personal data) and by each component;
- the flow of that data through the different components and processes involved in the system (e.g. input, validation, storage, movement, transformation, processing and output), and when it interacts with the human users (acquisition and presentation).

PRIPARE embraces this vision and hence proposes two processes, one for the architectural aspects of the system (privacy enhancing architecture design) and one for the detailed design (privacy enhancing detailed design). However, the two processes are inherently entangled and

[56] http://www.its.bldrdoc.gov/fs-1037/fs-1037c.htm

have some overlaps. Both processes are oriented to taking the right choices about the organization of the system, the selection of its structural elements, their interfaces and their behaviours that will help to build the desired system while maximizing its privacy respectfulness.

While there is no inherent order among PRIPARE's processed, PRIPARE's practical experience suggests the following approach would achieve best results:

- First, the privacy enhancing detailed design would pre-select a set of techniques that could be potentially useful for the devised system, according to the desired level of privacy conformance, the underlying technologies, functional description…
- Second, the architectural approach, will provide a final overall specification, integrating subsets of the previously identified techniques and detailing its application (e.g. specific protocols) into the final system design

The design decisions taken during this phase are addressed in the design logbook section of the template (section A.9). The final design should be documented according to the organizations' standards.

PRIPARE strongly suggests using privacy enhanced documentation standards such as those proposed by OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) TC.[57]

6.3.1 Privacy enhancing architecture design

The main objective of this process is to develop a privacy enhancing architecture (PEAR), i.e. an architecture which is capable of achieving the system's business objectives but ensuring that privacy and security quality requirements are also fulfilled.

Any project with potential privacy and security issues should evaluate several architectural approaches, taking into account privacy patterns and strategies to provide the most privacy-friendly possible design.

[57] https://www.oasis-open.org/committees/pbd-se/

Privacy enhancing architecture				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Project manager	Functional and technical requirements	- CMU-based approach - Formal approach (Top down, Bottom up)	Privacy Enhanced Architecture	System engineers
PSMO	Privacy requirements			
Tools & Techniques	Formal frameworks for the definition of privacy properties Cost Benefit Analysis Methods, Architecture Trade-off Analysis Methods, utility trees			
Knowledge	Formal modelling and verification, Architecture security and privacy approaches			
Responsible	System designer, Privacy engineer			

There are many different approaches to develop PEARs. PRIPARE does not impose one particular method. There are many. We describe here the CMU based approach which relies on the highly influential work on software system architecture from Carnegie-Mellon[58]. We also describe formal approaches (i.e. top-down and bottom-up approaches) are formal approaches which are not suitable to all types of projects but do fit, for example, with projects where ulterior modifications are almost impossible or would imply very high costs (e.g. an Internet protocol).

6.3.1.1 Approach based on CMU architectural analysis methods

Starting from an initial architecture and following an iterative process where the architecture is refined in order to address architectural significant requirements (ASR) while still complying with the desired business objectives Changes in the architecture are measured under different scenarios in order to determine if the change provides a positive or negative impact.

The CMU-based iterative approach is mostly based in the usage of scenarios, which are "structured means to state attribute requirements". The elements of a scenario are six (see): the source of a stimulus, the stimulus, the environment of the artifact being stimulated, the artifact itself, the response of the artifact and the measure of such response.

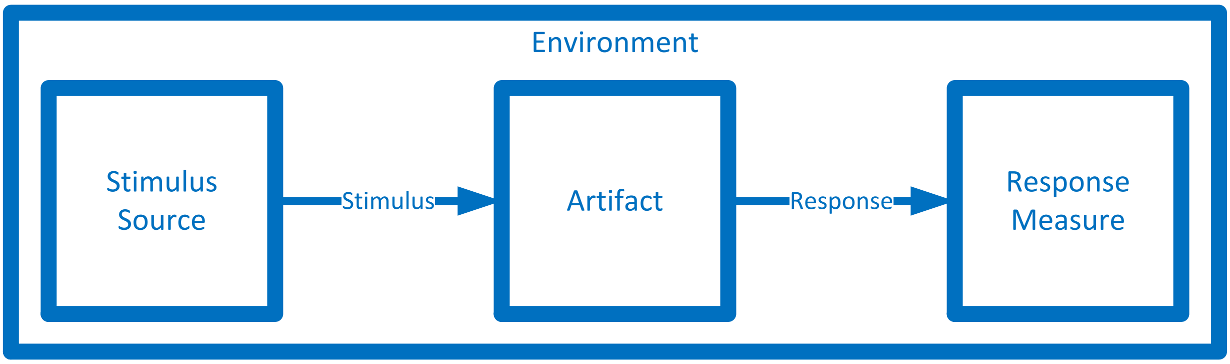


Figure 7: Scenario components

[58] Software Architecture in Practice (3rd Edition) (SEI Series in Software Engineering). Addison Wesley. by Len Bass, Paul Clements, Rick Kazman.

CMU-based iterative approach is an iterative process and has the following steps:

1. Present an initial architecture

System architects should present an initial architecture that should address the functional requirement of the system (may also refer to specific elements of the system):

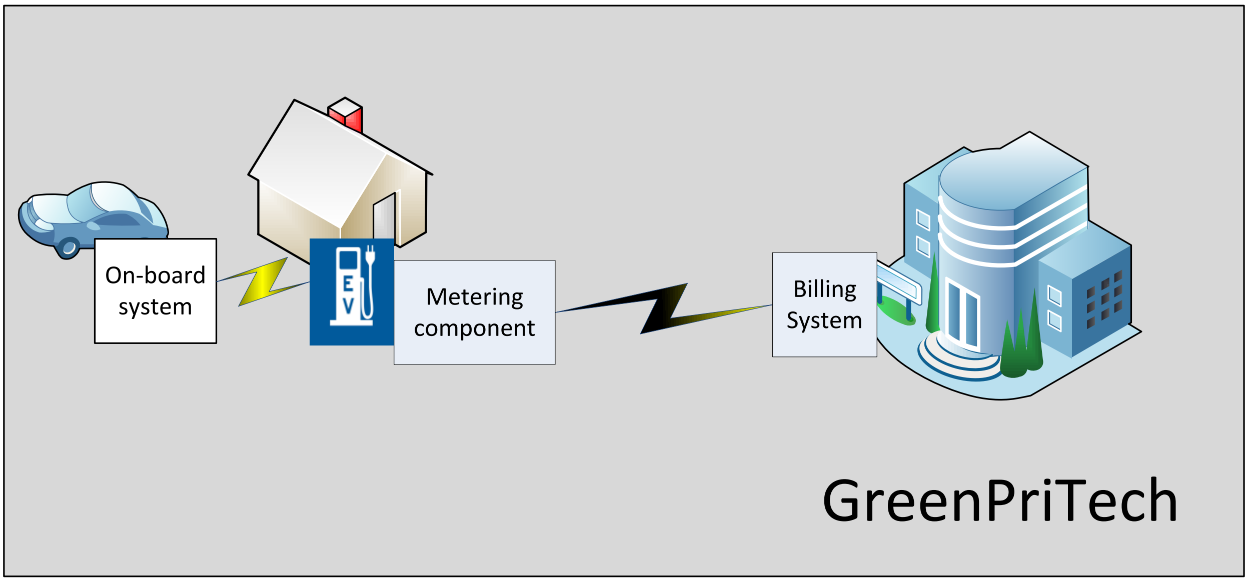


Figure 8: GreenPriTech initial architecture

2. Identify and prioritize scenarios and quality attributes

All stakeholders involved must identify and analyse the different scenarios that represent the system. This analysis should be based on available functional requirements, use cases or user stories.

The scenarios must be linked to quality attributes that comprise the system (e.g. performance, availability, security, modifiability, usability, security, privacy, etc…)

The following sequence diagrams represent electricity consumption – billing scenario that can be linked to efficiency and privacy quality attributes. For this scenario the performance can be measured as the overall costs of over-dimensioning the network capacity:

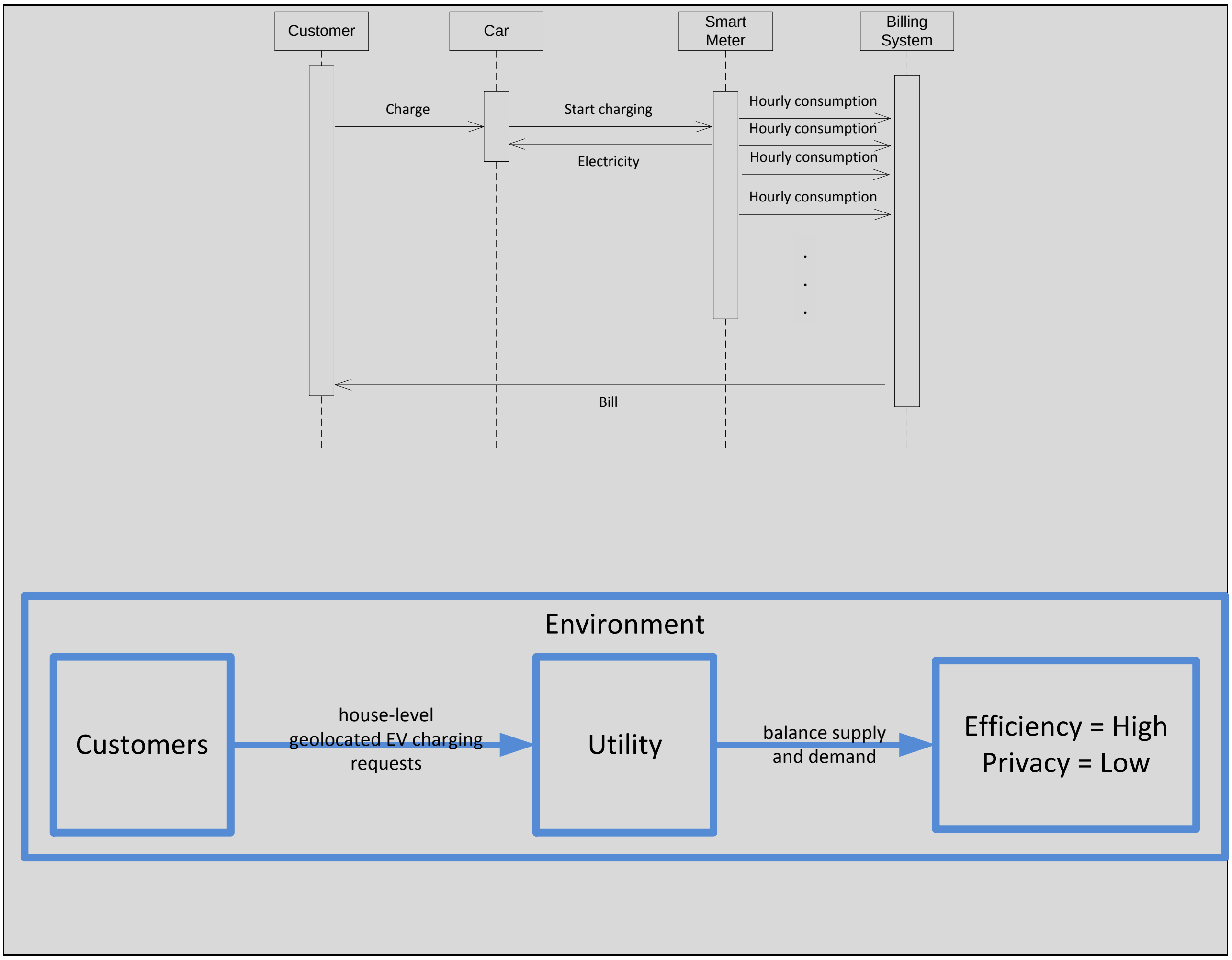


Figure 9: GreenPriTech initial billing scenario

As highlighted by Kung[59] and ATAM[60], utility trees are a very useful approach to identify, document and prioritize quality attributes and scenario. An example of a utility tree is found in .

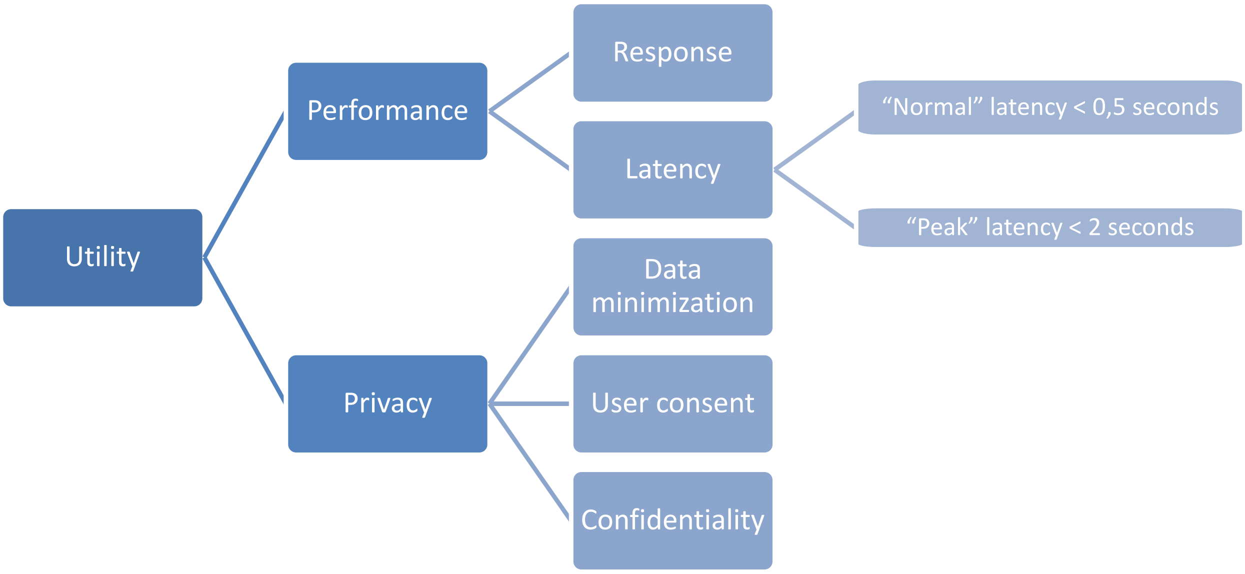


Figure 10: Utility tree

[59] http://link.springer.com/chapter/10.1007%2F978-3-319-06749-0_2

[60] http://www.sei.cmu.edu/architecture/tools/evaluate/atam.cfm

Architectural decisions based on the scenario approach should be included in the design log of the PSMA template (section A.9)

3. Identify potential architectural security and privacy enhancements

System architects must identify available privacy and security patterns, tactics, strategies, mechanisms, procedures and PETs applicable to the architecture.

The user confinement pattern as described in PEAR's paper [61]*:*

"The objective is to collect and process personal data in a location that is physically controlled by the user. It necessitates the availability of security mechanisms (PET) to control what is revealed to other stakeholders involved in the operation of the application."

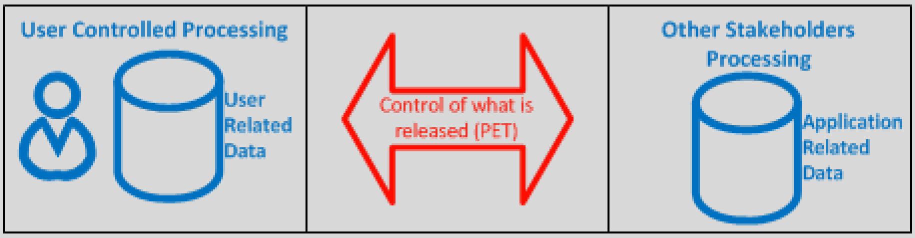

User Controlled Processing
User Related Data
Control of what is released (PET)
Other Stakeholders Processing
Application Related Data

Figure 15: The user confinement pattern

Location granularity pattern[62] *may also be applied to this use case to avoid data subject identification.*

4. Select and apply privacy and security architectural approaches to the scenario

Apply to the identified scenarios the different architecture approaches. Evaluate the differences between response measures before and after applying the architectural approach. Identify benefits and drawbacks of the approach and evaluate its applicability along with involved stakeholders.

Some quality attribute are hard to measure. While there is no standard, there are many privacy measuring frameworks which have been developed by researchers (e.g. Kosa et al[63]), **PRIPARE suggests leveraging these frameworks and the knowledge of privacy experts in order to provide useful privacy estimations**.

In order to determine the right architectural approaches, it is suggested to follow a cost-benefit analysis method such as Carnegie Mellon's CBAM[64]. This kind of approach "guides system engineers and other stakeholders to determine the costs and benefits associated with the architectural decisions that result in the system's qualities".

As a result of applying the user confinement and location granularity pattern to the scenario, the following results are achieved:

[61] https://books.google.es/books?id=RX25BQAAQBAJ&pg=PA24&lpg=PA24&dq=user+confinement+privacy+pattern&source=bl&ots=BNaJyc5KJZ&sig=-PJbmN-8r3avlE5l14ni2uuKsBc&hl=es&sa=X&ei=bFr0VI-FPInJPJPsgeAG&redir_esc=y#v=onepage&q=user%20confinement%20privacy%20pattern&f=false

[62] https://privacypatterns.eu/#/patterns/location-granularity

[63] http://isyou.info/jisis/vol1/no4/jisis-2011-vol1-no4-04.pdf

[64] http://www.sei.cmu.edu/architecture/tools/evaluate/cbam.cfm

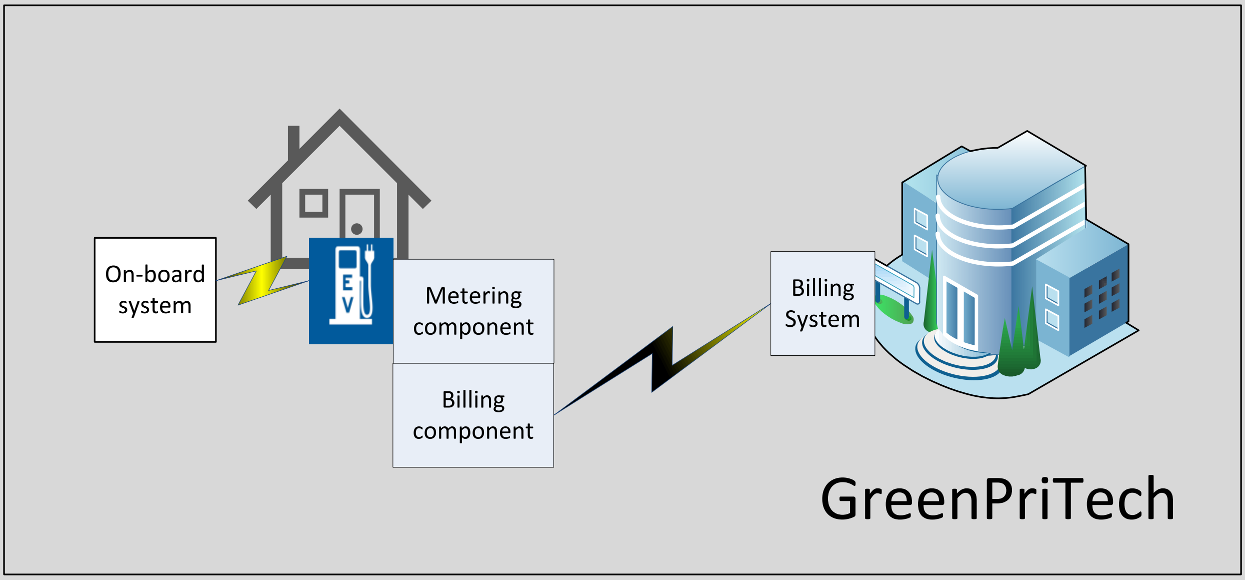


Figure 11: Modified GreenPriTech architecture

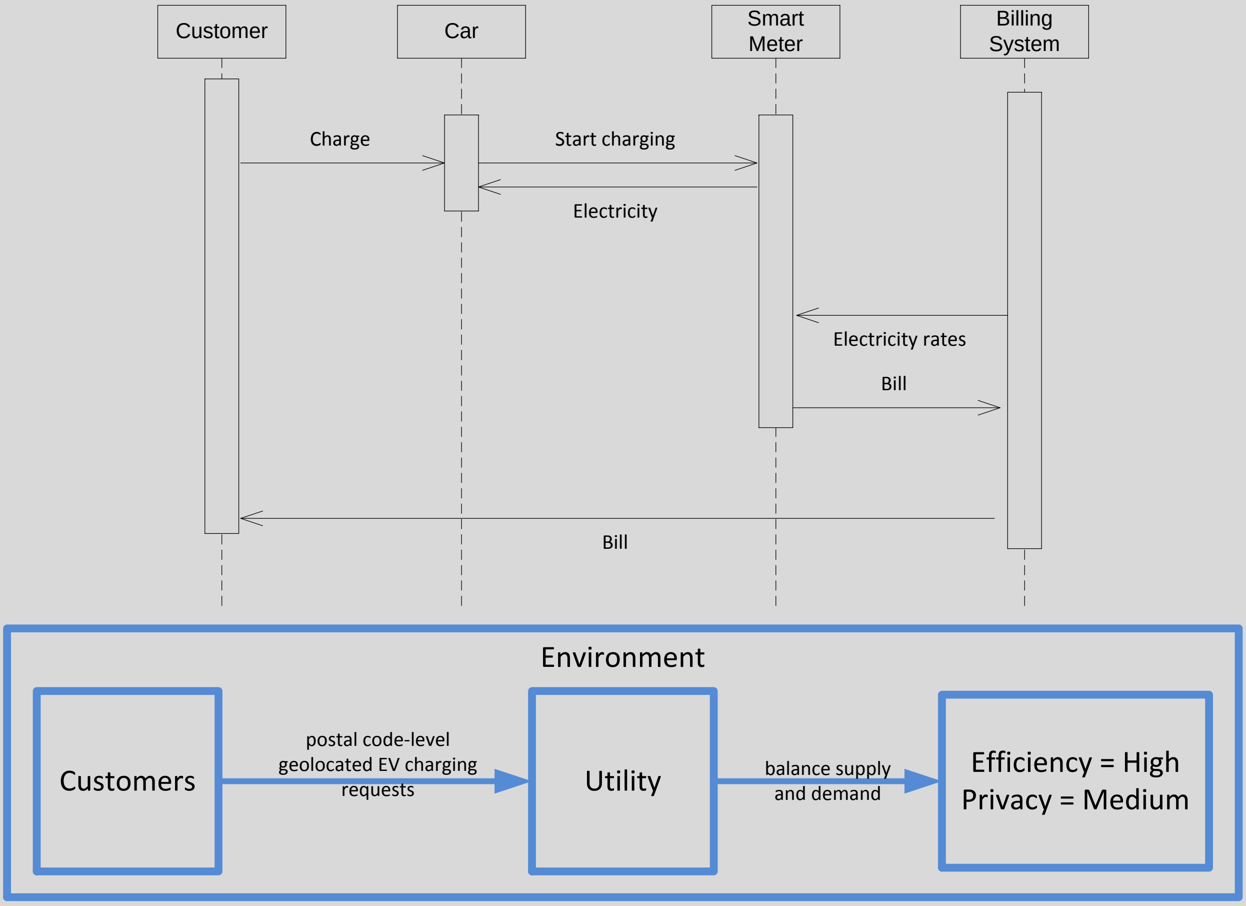


Figure 12: Modified GreenPriTech scenario

Applying the user confinement pattern to the initial architecture has several impacts:

- Increased cost as it includes a new component that must be deployed in the customer's premises;

- New risks that stem from threats of manipulating the billing components, the list of potential risks should be updated

- Decreased performance, not having information of hour-consumption means that the network has to be over-dimensioned in order to avoid shortages.

- Increased privacy for the customer: without tampering the devices or accessing customer's premises on no one can elicit customer's habits or routines.

Applying the location granularity pattern, the overall privacy provided by the system increases without any trade-off in terms of efficiency

6.3.1.2 Formal approaches

Architectures are often described in a pictorial way, using different kinds of graphs, or semi-formal representations such as UML diagrams (class diagrams, use case diagrams, sequence diagrams, communication diagrams, etc.). Even though such pictorial representations can be very useful, reasoning about privacy requirements is such a subtle and complex issue that the architecture language used for this purpose must be defined in a formal way. By formal, we mean that the properties of the architectures must be defined in a mathematical logic and reasoning about these properties must be supported by a formal proof or verification system. A source of complexity in the context of privacy is the fact that it often seems to conflict with other requirements such as functional requirements, integrity requirements, performances, usability, etc. Formal methods both make it possible to define precisely the concepts at hand (requirements, assumptions, guarantees, etc.) and to help designers to explore the design space and to reason about the possible choices. In the top-down approach the requirements are expressed in a formal language and different choices of architectures can be proposed to the designer based on the trust assumptions between the stakeholders. Different types of trust can be distinguished such as *blind trust* (assumption that an agent always behaves as expected), *verifiable trust* (a posteriori verification) or *verified trust* (a priori verification).

Top-down architecture design: CAPRIV (Computer Assisted Privacy Engineering)

The top-down approach is illustrated by the CAPRIV Computer Assisted Privacy Engineering framework[65]. It consists in deriving compliant architectures starting from the set of requirements (privacy, functional, technical, etc.) resulting from the privacy risk analysis. The process can be carried out in a semi-formal framework or in a formal framework (based on specifications of the individual components used in the architecture). The steps for this approach consist on:

- Expressing the requirements (either informally or in a formal framework)
- Checking the consistency of the requirements (either formally or informally) or detect inconsistencies
- Derive architectures from the requirements

An example of privacy requirement for the GreenPriTech project is the fact that the identity of the vehicles should remain secret as well as the identities of the mobility operator and the energy provider communicating with a specific vehicle. This property can be expressed as "weak

[65] https://hal.inria.fr/hal-01112856/document

secrecy" when active adversaries cannot deduce the complete secret from their interactions with the communicating parties or "strong secrecy" where adversaries cannot even distinguish if the secret changes. Strong secrecy provides stronger guarantees on the confidentiality of the secret, excluding any partial knowledge of the secret. In contrast, weak secrecy is not breached as long as the adversary cannot deduce the complete secret. Strong secrecy can be expressed formally as an observational equivalence property in a language such as the applied Pi-Calculus: P{M/secret} ≈ P{M'/secret}[66]. This property states that it is possible to replace secrets by different values in the protocol without active adversaries being able to distinguish these situations. Typically, the designer could use verified trust option to ensure that, by construction, the identities are not revealed.

Top-down architecture design: CAPRIV (Computer Assisted Privacy Engineering)

The top-down approach is illustrated by the CAPRIV Computer Assisted Privacy Engineering framework[67]. It consists in deriving compliant architectures starting from the set of requirements (privacy, functional, technical, etc.) resulting from the privacy risk analysis. The process can be carried out in a semi-formal framework or in a formal framework (based on specifications of the individual components used in the architecture). The steps for this approach consist on:

- Expressing the requirements (either informally or in a formal framework)
- Checking the consistency of the requirements (either formally or informally) or detect inconsistencies
- Derive architectures from the requirements

Bottom-up architecture design

In contrast with the top-down approach, the bottom-up approach requires the designer to propose a first version of the architecture that must be expressed in the formal framework before it can be verified. The goal of this process is to try to prove that this architecture complies with the requirements. The process should be carried out in a formal framework and rely on specifications of the individual components used in the architecture.Formal frameworks such as CAPRIV can be used either in a top-down manner or in a bottom-up manner depending on the initial knowledge of the designer: if the designer has a precise idea of the architecture (or very strong constraints on its design), he can follow the bottom-up approach; otherwise he may want to explore the design space more systematically through the top-down approach. The steps for this approach consist on:

- Expressing the requirements in a formal framework
- Checking the consistency of the requirements or detect inconsistencies
- Express the architecture in a formal framework and verify that the architecture meets the requirements

[66] Formal Verification of Privacy Properties in Electric Vehicle Charging, Marouane Fazouane, Henning Kopp, Rens W. van der Heijden, Daniel Le Métayer, Frank Kargl, ESSOS 2015.

[67] https://hal.inria.fr/hal-01112856/document

An application of the bottom-up approach for the GreenPriTech project consists in starting with a formal definition of the protocol (for example in the applied Pi Calculus) and a specification of the required privacy property (for example the unobservability property $P\{M/secret\} \approx P\{M'/secret\}$ *introduced in Section 6.3.1 and to apply a verification tool to prove this property. An example of tool that can be used to achieve this goal is ProVerif*[68].

6.3.2 Privacy-Enhancing Detailed Design

Any project with potential privacy and security issues should evaluate several designs, taking into existing guidelines and techniques which allow incorporating privacy controls in the system or process.

When system designers need to provide a solution to satisfy specific requirements in specific systems, they do not come up with a new solution each and every time they are developing a new system. Instead, they resort to **reusable design solutions** that guide the design with proven recipes based on previous experience and knowledge, which reduce uncertainty and cost in the design. This process provides and makes use of such reusable solutions, which define any of the three design facets above mentioned (components, data and flows), in order to meet privacy requirements.

Privacy-Enhancing Detailed Design				
Suppliers	**Inputs**	**Process**	**Outputs**	**Customers**
- Business & System analysts - System designer - Project managers - Privacy engineer	- Detailed Privacy Requirements. - System Architecture - Functional description - System boundaries, data flows and privacy roles	- Select most suitable techniques. - Instantiate techniques as system design.	- Detailed system design as a set of instantiated techniques.	Software developer
Tools & Techniques	Catalogue of design techniques			
Knowledge	Techniques and mappings to requirements			
Responsible	System designer, Privacy engineer			

The process identifies and instantiates the design techniques that need to be implemented by the system in order to meet the privacy requirements that were specified in previous processes (e.g. the Requirement Operationalization or the Risk Management processes; see sections 6.2.4 and 6.2.6), taking into account the specifics of the system under design. This process is typically

[68] Blanchet, B., Smyth, B.: Proverif 1.85: Automatic cryptographic protocol verifier user manual and tutorial (2011).

applied by the system engineer, who is responsible for the system design. It complements the process of architectural design (in section 6.3.1).

This process relies on a **catalogue of privacy-enhancing design techniques** that (heuristically) satisfy privacy requirements (principles, guidelines, criteria), to which they are in turn mapped. Designers select techniques from that catalogue, and apply then to refine the design of a privacy-friendly system. This catalogue acts as sort of a cookbook where designers might find the most suitable recipes to meet different requirements in different scenarios.

A **technique** is a reliable, implementable way to meet the definitions of one or more privacy criteria. Innumerable techniques may be created and hundreds have been defined by different sources (sometimes under the names of mechanisms, heuristics, controls, patterns, etc.), which cover a broad variety of cases. Techniques provide **informative guidance** to meet privacy requirements following best practice. They are not compulsory, nor are they necessarily the only or the best way to meet those requirements –yet they are well known and heuristically proven to work. They are deemed as informative (optional), instead of normative (mandatory) because there may be different ways (different techniques) to satisfy the same privacy criterion; thus, in general, a specific technique is not necessary to satisfy a given privacy criterion. Moreover, new techniques may appear in the future which do not yet exist and may perfectly help satisfy a privacy criterion. Hence the catalogue of techniques used by an organization should be kept up to date, so that they are applicable to novel technologies or just to keep up with current developments.

The process of Privacy-Enhancing Detailed Design can be split into two steps:

1. First, the most suitable **techniques are selected**, according to the system specifics. Some techniques will not suit just because they refer to privacy criteria that do not apply to the system. Besides, their suitability is constrained as well by the specifics of each system: its functions, the actors involved (domains and roles), its architecture, the technologies employed to implement it, and even the development team expertise. For instance, a technique to minimize location information does not make sense to a system which does not deal with that kind of information. Or, a technique to preserve privacy specifically in RFID systems does not apply to a system which uses an alternative technology. That is, each technique has a specific scope or context of application. Sometimes, the system designer will find that more than one technique can be applied in order to satisfy a privacy criterion in their system, and then they will need to choose one, depending on other constraints (expertise, cost, impact on other requirements such as usability, performance, etc.).
2. Second, the **techniques previously selected need to be instantiated**. That is, they are mapped to the specific system characteristics and architecture. For instance, a technique might establish that location coordinates are to be replaced by region names. Instantiating this technique means analysing the specific uses of location information in the system, and making the replacement in those places. This relies on the data flows and touch points previously analysed. Note that the application of these techniques may even result in redefining some of the data flows that were initially considered when the system analysis was performed (e.g. a subsystem may no longer use an item of personal data that was initially deemed as necessary).

As techniques represent the most refined level in the process to move from generic requirements to design, they contain a **lot of details** (see Figure 13) which allows determining when (its applicability scope or context), how (the detailed description of its process, plus optional application examples and tests), what for (correspondence with the requirements they allow meeting), who (responsible role) applies the technique, whether it is possible (readiness level and support by third parties), with(out) which other techniques it can be applied (and the relations between them)[69].

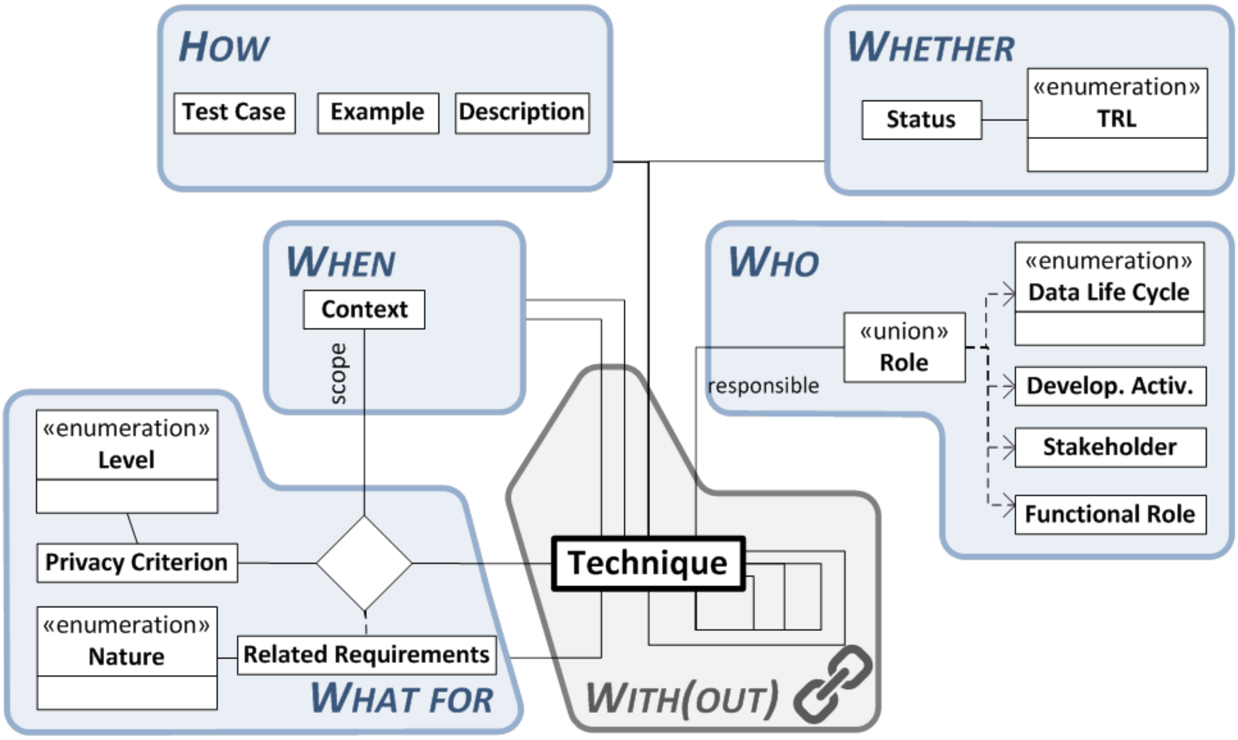


Figure 13: Basic structure of a design technique

At the moment no complete catalogue of privacy enhancing techniques is available. There are a number of classifications that have been proposed as showed in Table 3 and in Table 4. It is suggested to rely on such external sources, adapted to specific domains, and enriched by organizations. Techniques can also be based on the PRIPARE initiative to create a repository of privacy patterns[70]. Note as well that some PRIPARE patterns are architecture patterns and thus do not directly correspond to any technique.

Strategy		Techniques
Minimization	Collection of personal information should be kept to a strict minimum	Anonymize credentials (e.g. Direct anonymous attestation) Limit processing perimeter (e.g. client processing, P2P processing)
Enforcement	Provide maximum protection of personal data during operation	Enforce data protection policies (collection, access and usage, collection, retention)

[69] A more detailed description of the structure of techniques can be found on Annex B of D1.3. See http://pripareproject.eu/research/

[70] http://pripareproject.eu/wp-content/uploads/2013/11/D2.1.pdf

		Protect processing (e.g. storage, communication, execution, resources)
Transparency and accountability	Maximum transparency provided to stakeholders on the way privacy preservation is ensured	Log data transaction Log modifications (policies, crypto, protection) Protect log data
Modifiability	Cope with evolution needs	Change Policy Change Crypto Strength and method Change Protection Strength

Table 3: Classification of Privacy Enhancing Techniques (Kung[71])

Strategy		Techniques
Minimization	Amount of processed personal data restricted to the minimal amount possible	Select before you collect Anonymisation / pseudonyms
Hide	Personal data, and their interrelationships, hidden from plain view	Storage and transit encryption of data Mix networks Hide traffic patterns Attribute based credentials Anonymisation / pseudonyms
Separate	Personal data processed in a distributed fashion, in separate compartments whenever possible	Not known
Aggregate	Personal data processed at highest level of aggregation and with least possible detail in which it is (still) useful	Aggregation over time (used in smart metering) Dynamic location granularity (used in location based services) k-anonymity Differential privacy
Inform	Transparency	Platform for privacy preferrences Data breach notification
Control	Data subjects provided agency over the processing of their personal data	User centric identity management End-to-end encryption support control
Enforce	Privacy policy compatible with legal requirements to be enforced	Access control Sticky policies and privacy rights management
Demonstrate	Demonstrate compliance with privacy policy and any applicable legal requirements	Privacy management systems Use of logging and auditing

Table 4: Classification of Privacy Enhancing Techniques (Hoepman[72])

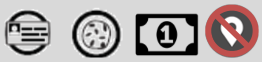
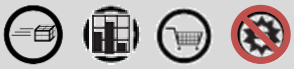
Examples of selected techniques and their instantiation

[71] Antonio Kung. PEARs: Privacy Enhancing ARchitectures. In Privacy Technologies and Policy – Second Annual Privacy Forum, APF 2014, Athens, Greece, May 20-21, 2014. Proceedings, pages 18–29, 2014

[72] Jaap-Henk Hoepman. Privacy design strategies. In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings, pages 446–459, 2014

Next we exemplify some of the techniques that can be applied to the GreenPriTech scenario. *In particular, we will emphasize those related to either of two groups: a first set of techniques regarding consent, choice, openness, transparency, notice, participation and access (ISO 29100 principles 1, 7 and 8); and another one regarding collection limitation, minimization, and confidentiality as part of information security (ISO 29100 principles 3, 4 and 10).*

Instead of presenting the whole content of each technique, we have summarized them into a table with a few fields: title (including references to the associated conformance criteria), summary (of problem, goal, procedure and rationale), and instantiation in the particular scenario we are dealing with. Note that some of the data flows may change after these techniques are applied (e.g. because some personal data has been minimized and is not sent anymore between two subsystems involved). Note also that we are not distinguishing here how techniques are instantiated by different domains: in a whole analysis of the scenario, the system designer from each domain would perform this activity independently and instantiate the design of their own (sub-)system.

Title of the Technique **plus Privacy Criteria Addressed**	**Summary**	**Instantiation**
Privacy Icons **Suf.: 1.2.3, *(1.3.3)*, 7.7.3, 7.7.4** **Part.: 7.7.1.**	Many organizations provide privacy policies which are too lengthy and hard to understand by the general audience. Users should understand, at first glance, what are the potential consequences of consenting of a privacy policy. Standardized icon sets may be added to the privacy policy. They are a great complement to written text, as they convey much information at a glance through a different modality (images).	GreenPriTech would add standard icons to its privacy policy stating that: 1) It may process contact and other personally identifiable information, cookies, consumption records, and payment data. It will not process location information.  2) The data subject personal data may be used for service delivery, internal operations optimization and billing purposes, but not sold to third parties. 
Added-noise measurement obfuscation **Rec.: 3.1.1.**	The provision of a service may require repeated, detailed measurements of a service attribute linked to a data subject to e.g. properly bill them for the service usage, or adapt the service according to the demand load. However, these measurements may reveal further information (e.g. personal habits, etc.) when repeated over time. If a noise value that abides by a previously known distribution is added to the true, measured value before it is transmitted to the service provider, the effective measurement will be obfuscated, but the result of aggregating several measurements can be still estimated.	GreenPriTech wants to employ consumption records to both adapt the power distribution in a dynamic fashion, according to the instantaneous demand, and bill the each client periodically, according to his or her aggregated consumption over the billing period. However, when trusted meters provide detailed records, they do not provide the real, measured data, but they add some noise, with a distribution depending on e.g. the power supply contract. GreenPriTech can still deduce the aggregated consumption requirements for an area, so as to schedule power distribution, optimize trading, etc., without being able to individually distinguish the consumption profiles of each individual customer.
Trustworthy	To apply variable billing tariffs, repeated, detailed consumption measurements are	A Privacy Plugin, hosted at the Consumer's EV receives the signed rates from the utility and

Privacy Plug-in	needed. However, these measurements may reveal further information (e.g. personal habits, etc.) when repeated over time. Instead of computing the bill at the Service Provider's side, the consumer may host a Privacy Plugin, in between the meter and the service provider. This plugin computes the aggregated bill and sends it to the service provider. Cryptographic techniques (homomorphic commitments, zero-knowledge proofs of knowledge, digital signatures) are used to ensure trustworthiness of the generated invoices without requiring tamper-proof hardware.	the detailed records from the meter, and periodically (e.g. monthly) generates a trusted invoice and sends it to GreenPriTech.

Table 5: Example of privacy-enhancing design techniques in GreenPriTech systems

6.4 Implementation

This phase relates to the implementation of the system described in the design phase (i.e., following the architecture and the detailed privacy-enhancing design).

Its scope is to:

- Select concrete security, privacy and functional mechanisms that instantiate the choices taken in the design phase.
- Implement these concrete mechanisms. This includes:
  - Selecting the hardware platform in which the mechanisms will be developed.
  - Developing the software components that implement the functionalities and protections devised in the design phase.
- Analyse the security and privacy properties of the implementation.

As in any other computer IT system, developers will use knowledge of software engineering principles and patterns. Additionally, they will use knowledge of secure programming and secure implementation of cryptographic primitives or, when possible secure use of cryptographic libraries. In order to perform the security and privacy analysis, developers and testers will use available evaluation methodologies (e.g., STRIDE[73]) and ad-hoc studies based on knowledge of state of the art attacks. The result of this evaluation shall be revised by the PSMOs of the organization

6.4.1 Privacy implementation

Any project collecting, storing or processing personal data or posing any significant threat to data subject's privacy should follow available best practices and techniques during the development of any system or business process

[73] S. Hernan et al., "Uncover Security Design Flaws Using the STRIDE Approach," http://msdn.microsoft.com/en-gb/magazine/cc163519.aspx, 2006.

This process deals with the implementation of the system in a privacy-preserving manner. It includes the selection and implementation of hardware platforms and software mechanisms that implement the functionality, architecture and protection mechanisms defined at the design phase.

<table>
<tr><th colspan="5">Privacy implementation</th></tr>
<tr><th>Suppliers</th><th>Inputs</th><th>Process</th><th>Outputs</th><th>Consumers</th></tr>
<tr><td><b>PSMOs</b>
<b>Project Managers</b>
<b>System engineers (designer)</b>
<b>Privacy engineer</b></td><td>- Functional requirements
- Privacy requirements
- Technical requirements
- System design
- Architecture</td><td>-Select Hardware platforms
-Select concrete mechanisms following the privacy enhancing design (tailor it if necessary to implementation constraints but keeping patterns privacy principles)
- Select concrete implementation of mechanisms
- Follow target OS, development languages and products' security and privacy best practices guidelines</td><td>Implementation of System</td><td>Project Managers (owners, operator, supplier) and End users</td></tr>
<tr><td><b>Tools &amp; Techniques</b></td><td colspan="4">Software libraries, Cryptographic libraries, hardware platforms (Microcontrollers, desktop, laptop, server, smart card...)</td></tr>
<tr><td><b>Knowledge</b></td><td colspan="4">Software Engineering, Secure programming, state of the art in privacy-preserving technologies</td></tr>
<tr><td><b>Responsible</b></td><td colspan="4">System engineers (developers, and testers)</td></tr>
</table>

Process description:

1) The first step in the process is to select concrete hardware platforms on which the different entities in the architecture will be implemented. This platform may be uniquely determined by the technical requirements that constrain the design.
2) The second step is to select functional, privacy and security concrete mechanisms that implement the functionalities and protections devised at design stage. For instance, if at design it is devised that communication shall be protected using symmetric encryption, the implementation will decide which encryption algorithm to use (AES, Blowfish...). This decision may be uniquely defined by the design decisions, if these select a privacy control mechanism that only has one implementation.
3) The third step is to decide the concrete implementation of the mechanisms selected in the second step. This includes selecting the programming language and the particular software architecture of each of the modules. Note that both elements may be uniquely determined by the hardware platform selected above; or by the available libraries that implement the privacy control mechanisms selected in the design.
4) Implementing the system following target OS, development languages and products' security and privacy best practices guidelines. Examples of such guides are:
    a. Android best practices for security & privacy[74]

[74] http://developer.android.com/training/best-security.html

b. iOS Security guide[75]

c. Red Hat Enterprise Linux 6 Security Guide[76]

d. OWASP Secure Coding Practices Quick Reference Guide[77]

e. ENISA Smartphone Secure Development Guidelines for App Developers[78]

Implementation of GreenPriTech

This process takes as input the Design elaborated in Section 6.3.3 and decides on a concrete implementation:

1) *For each of the components it decides on the best hardware platform for the different elements (e.g., an ARM7 microcontroller could be chosen as host for the on-board system, and an HP ProLiant server could be used to host the Billing service).*
2) *Concrete mechanisms will be selected to implement the privacy and security protections identified in the design (e.g., use the TLS protocol configured to use AES-256 in GCM mode for symmetric encryption, SHA256 as hash function and RSA-PKCS# 1 v1.5 as algorithm for key transport; use cloaking (i.e., reporting a large region instead of an accurate point) as means to obfuscate the users' location; use Pedersen-based commitments as part of the privacy plugin; etc.*
3) *Given the hardware choices in 1, an option is to use implementations of the cryptographic functions in the C language (either native from the OS installed on the hardware or publicly available such as OpenSSL).*
4) *Integrate and implement the system following the choices in the previous steps*

[75] https://www.apple.com/privacy/docs/iOS_Security_Guide_Oct_2014.pdf

[76] https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/

[77] https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf

[78] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines/at_download/fullReport

6.5 Verification

As mentioned earlier, privacy by design is a continuous process encompassing all steps of the life cycle of the system (and personal data). In addition to the preventive techniques and *a priori* verifications described in the previous sections, it is therefore necessary to implement *a posteriori* compliance controls, as mandated by the accountability principle.

6.5.1 Accountability

Three types of accountability need to be considered: accountability of policy, of procedures, and of practice. Accountability of policies and accountability of procedures are cross-cutting requirements which correspond to the proper documentation of all policies and procedure put in place to enforce the policies. Accountability of practices requires the documentation of the actual personal data processing, including all operations involving personal data, from their collection to their use, storage, forwarding and deletion.

Accountability				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
PSMO Project managers	Privacy requirements Functional requirements	- Define precisely and document the privacy policy of the system - Define precisely and document the procedures set up to implement the policies and show that they are adequate - Define precisely the analysis procedure to ensure accountability of practices - Define precisely the audit procedure including the roles of the parties (auditor, system owner, etc.) and the conditions of the audit.	privacy policy documentation procedures documentation analysis procedure audit procedure	PSMO, DPA, data subjects, independent auditors (external)
Tools & Techniques	Definition of procedures, audits, log analysis			
Knowledge	Log security and analysis			
Responsible	System designer			

When a formal language is used to express privacy policies, it should be possible to complement it by human verification. Indeed, some obligations expressed by policy languages may entail events that cannot be checked mechanically, for instance because they entail physical realization and are therefore beyond the scope of formal semantics. Checking these obligations involves human intervention. Verification tools can still partially integrate this aspect by outputting instructions to be followed by human agents to carry out manual compliance checking, or providing a semi-interactive mode prompting the auditor for information about the informal assumptions during the audit. Compliance can then be justified more strongly through a complete argumentation that ties in formal and manual verification (e.g. log analysis).

A key accountability requirement for the GreenPriTech project would be design of a secure log to record transactions with precise access control rules defining the entities able to get access to (parts of) the log and the conditions of this access. If the privacy requirements have been defined formally they can give rise to a log analysis tool that can facilitate the audits. Such a tool could, for example, check that no information about the identity of a customer is sent to the wrong entity.

6.5.2 Security & Privacy static analysis (a priori verification)

The goal of this step is to check that the implementation meets its privacy and security requirements without executing the code (in contrast with dynamic analysis, see section 6.5.3, which involves code execution).

Security & Privacy static analysis (a priori verification)				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Privacy manager, Project manager, System owner	Implementation	- Express the implementation in a language with a formal semantics (e.g. the pi-calculus or traditional imperative language with a formal semantics) - Express the expected properties in a formal language (e.g. observational equivalence properties) - Check that the implementation meets the properties (e.g. using a theorem prover or a verification tool)	Verification results	Privacy manager, Project manager, System developer
Tools & Techniques	Process algebra, theorem provers, verification tools			
Knowledge	Formal modelling and verification			
Responsible	System designer			

Static analysis can be conducted either informally (e.g. through code inspection) or formally (in a mathematical framework). In the latter case, the program or protocol has to be expressed in a language endowed with a formal semantics. The most widely used languages for the definition of protocols are process calculi such as the pi-calculus. Dedicated tools such as TL SAVE[79] and TL

[79] http://trusted-labs.com/security-consulting/tools-training/tl-save/

SAT[80] are also available for the static verification of traditional (e.g. Java or binary) code with respect to security rules. An alternative option consists in using a dedicated language to express privacy properties. For example:

- SIMple Privacy Language (SIMPL)[81] makes it possible to prove certain properties about privacy policies (for example that a given third party may never receive a given piece of data) and to prove that a given implementation is consistent with the semantics – in other words, that the system behaves as expected by the user.
- Contextual Integrity (CI)[82] is a temporal logic language inspired by the notion of contextual integrity, which makes it possible, for example, to express the fact that an agent acts in a given role and context.
- S4P[83] is an abstract language based on notions of declaration, permission (*e.g.* "Company may use email addresses for marketing purpose") and obligation (*e.g.* "Company will delete any email within 2 weeks").

Last but not least, static information flow analysis techniques have also been proposed to identify security weaknesses[84] or privacy leaks (for example for Android applications[85] or iOS applications[86]).

Strong secrecy property: *An example of privacy property is strong secrecy, expressed as the fact that an adversary cannot notice secret changes to personal data. Strong secrecy is stronger than confidentiality which expresses the mere fact that the attacker cannot know the personal data.*

Formal model of strong secrecy: *In a bottom-up approach in which protocols are expressed in the applied pi-calculus, strong secrecy can be defined as the observational equivalence between a process P and a process P' similar to P except for the changes in the personal data*[87]: observational equivalence ensures that an external observer cannot distinguish between P and P'.

Verification of strong secrecy: *Strong secrecy of the electricity provider can be proven on an enhanced version of the POPCORN electric vehicle charging protocol using the ProVerif tool.*

[80] http://trusted-labs.com/security-consulting/tools-training/tl-sat/
[81] http://pop-art.inrialpes.fr/~lemetayer/fast2008.pdf
[82] http://www.andrew.cmu.edu/user/danupam/bdmn-oakland06.pdf
[83] http://research.microsoft.com/pubs/122108/main.pdf
[84] https://www.owasp.org/index.php/Static_Code_Analysis
[85] http://www.mais.informatik.tu-darmstadt.de/WebBib/papers/2012/android-sac12.pdf
[86] https://www.cs.ucsb.edu/~chris/research/doc/ndss11_pios.pdf
[87] http://prosecco.gforge.inria.fr/personal/bblanche/proverif/

6.5.3 Security & Privacy dynamic analysis

The goal of this step is to check that the implementation meets its privacy and security requirements through code execution.

Security & Privacy dynamic analysis				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Privacy manager, Project manager, System developer	System Implementation	- Identify test scenarios and exercise the code to detect vulnerabilities prior to its exploitation and/or - Instrument the code to make monitoring possible during the exploitation of the code	Test results (pass/fail) and/or information about program execution (e.g. information flows)	Privacy manager, Project manager, System developer
Tools & Techniques	Testing tools, instrumentation techniques, dynamic flow analysis			
Knowledge	Testing, dynamic analysis			
Responsible	Project manager			

Dynamic analysis can be conducted either before or during the exploitation of the implementation. In the first case, the code is exercised through well-chosen test scenarios, for example through penetration testing targeted at identifying security vulnerabilities in the code. In the latter, the code is instrumented and monitored during its normal use. An illustration of systematic testing is the TL CAT[88] environment, which makes it possible to generate test scenarios (including specific security tests) systematically with code coverage guarantees. An illustration of the monitoring approach for privacy is TaintDroid[89], a system for the dynamic tracking of information flows that allows the discovery of undesired leaks on the Android platform.

While following this approach under simple and well defined scenarios may be simple, there are many other complex environments where many challenges have to be addressed. Challenging scenarios include those which involve cloud and distributed computing, enormous amounts of data (big data) or a high number of systems (Internet of Things).

> ! Prior to the release of any system, this should be subject to privacy and security in order to ensure they are adequately covered and controls are effective throughout the development process. The OWASP testing guide[90] is a useful reference document to understand both, the process and the techniques to conduct this testing. The RACOMAT tool[91] integrates the security testing as an integral part of a risk management process.

[88] http://trusted-labs.com/security-consulting/tools-training/tl-cat/

[89] http://appanalysis.org/

[90] https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf

[91] http://www.rasenproject.eu/the-racomat-tool-2/

Dynamic analysis for the GreenPriTech project could include systematic testing of all use scenarios of the protocol and the application of a monitoring tool to tack the information flows between the vehicles. This tool could apply on the fly checking rules to ensure that, for example, no information about the identity of a customer is sent to the wrong entity (or at least without being detected).

6.6 Release

This phase includes the process that must be followed immediately before or in the moment of the release of a new system (or after a significant modification). The processes included under this phase are:

- The creation of an incident response plan
- The creation of a system decommissioning plan
- A final security and privacy review
- Publishing the PIA report

At this stage, it is very important to identify the people responsible for these plans, reports, actions and reviews as there is a need to provide accountability. All documents must be signed by those responsible who will be held **accountable** for their contents.

6.6.1 Create Incident Response Plan

Any project collecting, storing or processing personal data should have an incident response plan which will guide system operators in the eventual case of a privacy or security breach

This process establishes the process and documentation process to be followed in case of a privacy breach. Its scope is to guide the organisation during the preparation of a specific process, according to the specificities of the system, such as the domain and its regulations, and the kind of personal data involved.

The incident response plan outlines the steps an organisation should follow in the event of a privacy breach. Having an incident response plan in place can help an organisation to respond quickly to any privacy or security breach, and aid in mitigating the effects and/or impact of that privacy or security breach.

<table>
<tr><th colspan="5">Create incident response plan</th></tr>
<tr><th>Suppliers</th><th>Inputs</th><th>Process</th><th>Outputs</th><th>Consumers</th></tr>
<tr><td>PSMOs</td><td>Risk assessment, impact assessment,
System description,
Data flows</td><td>- Identify the technical team which is responsible of responding to security and privacy breaches
- Clearly establish its priorities (containment, assessment, availability, notification…)
- Outline the process which must be followed in case of a breach</td><td>The incident response plan</td><td>System engineers, System operators</td></tr>
<tr><td><b>Tools &amp; Techniques</b></td><td colspan="4">Risk assessment, impact assessment, privacy breach risk impact assessment</td></tr>
<tr><td><b>Knowledge</b></td><td colspan="4">Risk assessment, impact assessment methodologies</td></tr>
<tr><td><b>Responsible</b></td><td colspan="4">Privacy & security manager (& wider privacy breach management team)</td></tr>
</table>

In order to establish a response plan to be followed during or after a security or privacy breach, the first step is to clear identify who is the people responsible and their role in response to the breach.

The second step is to clearly state what are the priorities in terms of business and security (e.g. keeping the system online vs assessing its origin vs containing the breach).

The third step is to outline which should be the process to be followed by the responsible and according to the pre-established priorities. The following steps could be included in an incident response plan. These steps have been taken from the Treasury Board of the Canadian Secretariat's 'Privacy Breach Management Toolkit'[92]:

- Preliminary assessment and containment, which includes focusing on whether a privacy breach has occurred and how it occurred. A tool that could be used for this step is that provided by the Treasury Board of the Canadian Secretariat[93].
- Full assessment, which includes making a reasonable effort to identify the individuals or groups of individuals likely to have been affected. This should be documented as part of a privacy breach checklist.
- Notification, which includes the prompt notification of any individuals likely to have been affected by the privacy breach, in order to provide them with information to take measures to protect themselves.
- Mitigation and prevention, which includes developing potential corrective measures.
- Notification to the relevant Data Protection Authority, which involves submitting a formal, written notification of the privacy breach in the form of a report. This report could include: the nature and extent of the breach; the type of information involved; the parties involved; the anticipated risks of harm; steps taken or to be taken to notify individuals; and what remedial action has been taken.
- Lessons learned which includes identifying trends within each step of the privacy breach management process.

The GreenPriTech ubiquitous charging programme potentially involves the collection and processing of geolocated data, which may reveal the behavioural aspects of any data subject. The incident response plan created by GreenPriTech has established the following steps to be followed in case of a privacy breach:

- Contain the breach and undertake a preliminary assessment

- Evaluate the risks associated with the privacy breach

- Notification to the DPA and data subjects

- Report to prevent future breaches

The process clearly identifies the name of the security responsible for the project and how to contact him in case of a security breach. The process advises against going on full-shutdown in case of detecting a breach. It, however, does contemplate shutting down individual systems which will still allow charging EVs.

[92] https://www.tbs-sct.gc.ca/atip-aiprp/tools/pbmt-togap/pbmt-togaptb-eng.asp

[93] https://www.tbs-sct.gc.ca/atip-aiprp/tools/pbmt-togap/opipac-bprepc-eng.asp

Article 31 and 32 of the EU GDPR draft approved by the European Council[94] clearly state that "as soon as the controller becomes aware that (…) a personal data breach which may result in (…) physical, material or moral damage has occurred the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours " and that "When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall also communicate the personal data breach to the data subject without undue delay"

The regulation at this moment foresees as potential results of personal data breaches "physical, material or moral damage to individuals such as loss of control over their personal data or limitation of (…) their rights, discrimination, identity theft or fraud, financial loss, [breach of (…) pseudonymity], damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned"

WP29 opinion in personal data breach notifications[95] provides useful guidelines to determine under which circumstances data breaches have to be notified to the corresponding data protection authorities and to the data subjects.

6.6.2 Create system decommissioning plan

Any project collecting, storing or processing personal data should have a decommissioning plan which will guide system operators whenever the system ceases its operation

This process guides the design of a decommissioning plan outlining the actions to perform when the system ceases its operation.

Create system decommissioning plan				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Project manager PSMOs	List of threats List of assets (data) Legislation	Step 1- identify sensitive data Step 2 – decide actions to take on data (e.g., delete, anonymize) Step 3 – decide who has to perform the actions	Decommissioning plan	Privacy & Security managers System engineer (developer and tester)
Tools & Techniques	Privacy and security evaluation frameworks			
Knowledge	Attacks on privacy, legislation, privacy metrics			
Responsible	PSMOs, Privacy expert			

[94] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

[95] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

Taking into account the data collected and stored by the system, the list of threats derived from the risk analysis and the requirements established by legislation, this process establishes a decommissioning plan to be conducted when the system ceases its operation. This plan shall establish what should be done with the hardware composing the system, and in particular what should be done with the data it has collected during the system's life:

1) Identify which of the data collected by the system is sensitive and should not be available after the system has stopped its operation.
2) Decide what should be done with this data, and with the hardware that stores it. Operations to be done may include deletion, anonymisation, obfuscation or other mechanisms to eliminate sensitive information.
3) Decide who should be responsible of the different operations to be performed on the data.

Special attention should be paid to Article 29 Data Protection Working Party on Anonymisation Techniques[96] which describe most common anonymisation techniques and their strengths and weaknesses

Please note that personal data contained in backups is still subject to the legislation and must be taken into account during the development of the decommissioning plan.

Create decommissioning plan for GreenPriTech

This process takes as input the Design and Implementation elaborated in the previous sections and creates a decommissioning plan:

1) Identify sensitive data: personal data of customers (name, address...), location records, consumption behaviour...

2) Personal data could be deleted, and location records anonymized and further obfuscated with respect to the implementation. Consumption profiles could be aggregated to avoid storage of fine-grained information.

3) Project managers are in charge of instructing engineers to implement the measures identified in the previous stem. Engineers are responsible of implementing. The PSMOs are held responsible of validating the plan and its execution.

[96] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

6.6.3 Final Security & Privacy review

Any project with potential privacy and security issues should be thoroughly evaluated to ensure it respects data subjects privacy and it is compliant with the regulation

This process performs a review of the privacy and security properties of the final implementation of the system, verifying that it complies with the privacy and security requirements identified during the analysis phase.

Final Security & Privacy review				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
System engineers, PSMOs, DPA	- Threat model-Decommissioning plan -Incident response plan -Risk assessment -Static and dynamic analysis results -System design - System implementation	- Review all security and privacy activities - (Re-) Examine threat models, analysis reports and test results - Ensure the project is still legally compliant	- Final Privacy & Security review (FSPR) (passed, passed with exceptions, not passed)	System engineers, DPAs
Tools & Techniques	Verification checklists			
Knowledge	Privacy and security technologies, state of the art attacks			
Responsible	PSMOs, Privacy Expert			

This process will revisit the design and implementation of the system, checking whether it fulfils the requirements established in the analysis phase:

1) Re-examine the threat model of the system, taking into account the environment in which it will be deployed and the state of the art in attacks that may have evolved during the design and implementation phase.
2) Validate that the security and privacy mechanisms selected in the design phase, and its concrete realization selected in the implementation phase fulfil the requirements in the re-examined threat model. This step includes revisiting the results in the reports output by the static and dynamic security and privacy analysis of the system verifying that they hold considering changes in the threat model with respect to the adversary considered in the design.
3) Validate that the response and decommissioning plans are adequate for the system. This step includes revisiting the effectiveness of the plan in the light of changes in the threat model that may have happen with respect to the adversarial model considered in the verification and release phases.

4) Examine the privacy and security roadmap developed during the preliminary process and verify that all processes have been followed according to the roadmap. Justify any deviation from the original roadmap.
5) Examine the initial legal compliance and ensure that after the design and implementation, the assessment is still valid and the system continues to be compliant.

Developing an **organizational verification checklist template** which should include common verification items to most projects that should be checked before any release **may help practitioners**. Examples of such items are:

		Y	N
Q1	Is there an incident response plan available which guides the employee in case of a privacy or security breach?		
Q1.1	Does it clearly identify which people have to be alerted?		
Q1.2	Has it been updated in the last year?		
Q2	Is there a list of privacy risks associated to the system?		
Q2.1	Does each of the system's privacy and security remaining risks have a justification of why they are not addressed?		
Q2.2	Is there any new vulnerability that may affect the system[97]		

OWASP provides through its Application Security Verification Standard Project an example of a security checklist[98] which may orientate PRIPARE practitioners.

The result of this process will be described in a Final Privacy & Security review (FSPR) that documents whether the system, response, and decommissioning plans fulfil the requirements in any situation, if there are exceptional cases when the system needs further protection, or if the system fails to protect users' data.

Final Security & Privacy review of GreenPriTech

This process revisits the implementation of the system to check it fulfils the privacy and security requirements established in the analysis phase:

1) Re-examine the threat model. For instance if a new attack on TLS has appeared while the system is being implemented this may bring in a new set of threats.

2) Re-conduct the static and dynamic analysis (see Sections 6.5.2 and6.5.3) in the light of the new threat model, which may uncover vulnerabilities (e.g., .the communications are not secure anymore).

3) Re-conduct the analysis for the response and decommissioning plans (e.g., new vulnerabilities found in TLS implementation do not affect the decommissioning plan, so the analysis is still valid).

All results are written in the FSPR report signed by both, the PSMO and the CTO.

[97] https://cve.mitre.org/

[98] https://www.owasp.org/images/5/58/OWASP_ASVS_Version_2.pdf

6.6.4 Publish PIA report

Any project with potential privacy and security issues should publish a PIA report in order to provide transparency to the data subjects and corresponding data protection authorities

Organisations should publish a report containing the results of the PIA. Publishing the results of the PIA can improve transparency and build public trust with regard to how information about individuals is collected, stored, processed and transferred. The preparation of a report, which documents the PIA process, is an important part of conducting a PIA.

Publish PIA report

Suppliers	Inputs	Process	Outputs	Consumers
PIA team, PSMOs, project managers	Results from conducting the previous PRIPARE process	Analysing the results from previous PRIPARE processes, including input from stakeholders, risk assessment, solutions to risks outlined	PIA report	PIA team, PSMOs, data protection officer, management, project managers, technical/legal/audit staff, internal and external stakeholders, system engineers, end users, DPA
Tools & Techniques	PIA			
Knowledge	PIA process and analysis of results			
Responsible	project managers, PSMOs			

Producing a PIA report involves summarising, analysing and reporting on the results of the PIA process. The report should include: an executive summary; an introduction and overview of the PIA process; a description of the information flows; a project description; a summary of the privacy risks and impacts identified; compliance with laws, regulations, codes and guidelines; results of any stakeholder consultation; and an analysis of any solutions to the aforementioned identified privacy risks and impacts; as well as a set of recommendations in terms of risks identified and making the report publicly available.

PRIPARE recommends, in pursue of transparency, to provide and make public a version of such report, after erasing all sensitive information.

In the case of GreenPriTech, a PIA team is assembled from within the organisation. Once the analysis has been undertaken and before the release of the system, the PIA team analyses and summarises the results of the processes within the PIA report. This PIA report includes feedback from internal and external stakeholders. The PIA report is made public, and a copy is also offered to the DPA for review. The PIA report is revisited when changes are made to the system.

6.7 *Maintenance*

In the case where incidents have been detected, the data controller must, as part of his security obligations, take all useful measures to minimize the damage for the subjects

6.7.1 Execute incident response plan

✓ **Any project suffering a privacy or security breach**

The goal of this process is to implement all useful measures to minimize the damage for the subjects in case of incident and to comply with the notification obligation of the EU DPR.

Execute incident response plan

Suppliers	Inputs	Process	Outputs	Consumers
System operator	Incident involving personal data	- Take all traditional security incident measures (log analysis to find the source of the incident, assessment of the consequences, corrective measures, etc.). - Implement the notification requirements of the applicable legislation (e.g. the EU DPR). - Assess future measures in order to avoid further breaches.	- identification of the source of the incident - corrective measures - notification to the DPA - notification to the subjects (if they are likely to be adversely affected)	- DPA - data subjects (indirectly)
Tools & Techniques	Log analysis, forensics tools			
Knowledge	Log analysis, forensics, security			
Responsible	System designer, System owner (notifications)			

This process is carried out in three steps:

1) Take all traditional security incident measures (log analysis to find the source of the incident, assessment of the consequences, corrective measures, etc.) in order to contain the breach
2) Carry out the actions defined in the incident response plan, including following the notification requirement of the applicable legislation
3) Verify that the actions achieve the intended objective. This includes following a retrospective analysis in order to understand valuable lessons on how to avoid future breaches.

Execute incident response plan of GreenPriTech

After detecting a potential breach the incident response plan is activated and the security team focuses in containing the breach. In very short time, DPA have to be notified of the breach, following EU GDPR. The security breach is isolated and the team is capable to *identify that "only" the personal data of 95 people was affected. GreenPriTech instructs its press office to individually communicate with affected data subjects as well as creating a press release which announces the breach and its impact.*

Article 29 issued Opinion 03/2014 on Personal Data Breach Notification[99] that provides a non-exhaustive list of examples where data subjects should notified and examples where notifications would not be required, e.g.:

- Should be notified
  - Personal data related to the customers of a life insurance broker was unduly accessed by exploiting web application vulnerability. Data subjects were identified by name and address, and completed medical questionnaires were included. 700 data subjects were affected.
  - The encrypted laptop of a financial adviser has been stolen from the boot of a car. All the details of financial assessments - e.g. mortgage, salary, loan applications of 1000 data subjects were affected. The encryption key, the passphrase, is not compromised but no backup is available
- Notification not required
  - A personal data breach only relating to confidentiality, where data was securely encrypted with a state of the art algorithm, the key to decrypt the data was not compromised in any security breach, and the key to decrypt the data was generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key. Indeed, such measures make the data unintelligible to any person not authorised to access it.

Article 31 and 32 of the EU GDPR clearly state that "as soon as the controller becomes aware that (…) a personal data breach which may result in (…) physical, material or moral damage has occurred the controller should notify the breach to the supervisory authority without undue delay and, where feasible, within 72 hours " and that "When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall also communicate the personal data breach to the data subject without undue delay"

The regulation at this moment foresees as potential results of personal data breaches "physical, material or moral damage to individuals such as loss of control over their personal data or limitation of (…) their rights, discrimination, identity theft or fraud, financial loss, [breach of (…) pseudonymity], damage to the

[99] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned”

6.7.2 Security & Privacy verifications

Any project with potential privacy and security issues should regularly verify its impact assessment and privacy controls to ensure the system is compliant and updated to most recent developments (in threats, attacks, risks or controls)

This process comprises security and privacy analyses carried out during the system’s operation. Its goal is to verify that the system behaviour, stemming on the users’ actions and the environment in which it is deployed, does not result in a privacy or security breach. This process is, in spirit, very similar to the Security & Privacy final review (see section 6.6.3) but the conditions in which the analysis is carried out may change depending on the system’s environments and advances in the state of the art attacks, PETs or in security technologies.

Security & Privacy verifications				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
System engineers, PSMOs, DPA	-Decommissioning plan -Incident response plan -Risk assessment -Static and dynamic analysis results -System design - System implementation - Privacy & Security Management Analysis	- (Re-) Examine threat models, analysis reports and test results - Review all security and privacy activities - Review decommissioning and response plans - Ensure privacy controls are in place and working as expected - Review and ensure the documentation is accurate	Operation security and privacy reports	System engineers, DPAs
Tools & Techniques	Verification checklists, audits			
Knowledge	Privacy and security technologies, state of the art attacks			
Responsible	PSMOs, Privacy expert			

This process will **periodically, and after major changes, revisit the security and privacy analyses** of the system during its operation in order to check whether it fulfils the requirements established in the analysis phase:

1) Re-examine the threat model of the system, taking into account the environment in which it is being deployed, the way users interact with it, and the state of the art in attacks that may have evolved while the system is running.
2) Validate that the security and privacy mechanisms that the system implements fulfil the requirements in the re-examined threat model. This step may include modifying the results in the reports output by the static and dynamic security and privacy analysis of the system performed after design and implementation.

3) Validate that the response and decommissioning plans are still adequate for the system. This step includes revisiting the effectiveness of both plans in the light of changes in the threat model or on the system environment that may have happen while the system is running.
4) Validate that the technical and organizational measures which are in place in order to provide security and protect data subject's privacy are effectively working as expected and described during the analysis and design of the system. E.g. ensure that the logs are examined in order to detect intrusions. Periodical drills can take place in order to test the real level of security or privacy-protection achieved which can also raise the level of awareness in the organization.
5) Validate that all accountability-related documentation (see section 6.5.1) is accurate.
6) If any problem is found, the incident response plan should be activated.

Security and Privacy verification of GreenPriTech

This process revisits the implementation of the system to check it fulfils the privacy and security requirements established in the analysis phase:

1) *Re-examine the threat model. For instance if the entity hosting the billing service has started providing other services the users and administrators of these services could be considered as new potential adversaries, bringing a new set of threats.*
2) *Re-conduct the static and dynamic analysis (see 6.5.2 and 6.5.3) in the light of the new threat model, which may uncover vulnerabilities (e.g., .the administrator of the other service has access to data stored by GreenPriTech).*
3) *Re-conduct the analysis for the response and decommissioning plans*
4) *Check the system logs are recording all expected levels and according to the design. Also check who has access to the logs.*
5) *Review the system's privacy policy and ensure that it is aligned with the "real" system operations.*

If any problem is found, activate the incident response plan. For instance, countermeasures to avoid information being leaked to other system administrators should be put in place.

6.8 Decommissioning

This phase is launched when the system ceases its operation. Its purpose is to make sure that, after stopping, the data collected by the system cannot result in a privacy or security breach. For this purpose it implements the decommissioning plan elaborated during the release phase.

6.8.1 Execute decommissioning plan

Any project storing personal data should follow its decommissioning plan once its ceased to work

During this phase the actors appointed by the decommissioning plan elaborated in the Release phase (see section 6.6.2) and updated during the Maintenance phase (section 6.7.2), carry out the activities specified in the plan itself.

Execute decommissioning plan				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**
Project manager **PSMOs**	System decommissioning plan System architecture Risk analysis	- identify responsible people according to plan - take actions according to plan - validate actions are properly taken	Sanitized system (no personal data)	Users
Tools & Techniques	Encryption, Secure deletion, Anonymisation			
Knowledge	Privacy and security attacks, privacy and security threats			
Responsible	PSMOs			

This process is carried out in three steps:

1) Identify the people that perform the roles assigned to each of the actions in the decommissioning plan.
2) Carry out the actions defined in the decommissioning plan.
3) Verify that the actions achieve the intended objective. This includes a security and privacy analysis on the sanitized system (like the ones done in the Implementation and Verification phases).

Special attention should be paid to Article 29 Data Protection Working Party on Anonymisation Techniques[100] which describe most common anonymisation techniques and their strengths and weaknesses

[100] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

4) Proofs should be created to demonstrate all actions taken during the decommissioning, enabling accountability for the process.

It is important to also take in to account, besides the data residing in the system to be retired, any backup which was created during its operation..

Execute decommissioning plan of GreenPriTech

This process activates the execution of the decommissioning plan once GreenPriTech stops its operation:

1) *Identify the people in charge of the plan actions: PSMOs, project manager, engineers...*
2) *Carry out the actions as mentioned in the plan: aggregate behavioural data, obfuscate locations, and delete personal data.*
3) *Have the PSMO checking that the actions taken by other principals have been effective by carrying a security and privacy analysis of the sanitized data, considering the state of the art attacks at that point.*

7 Methodology application guidelines

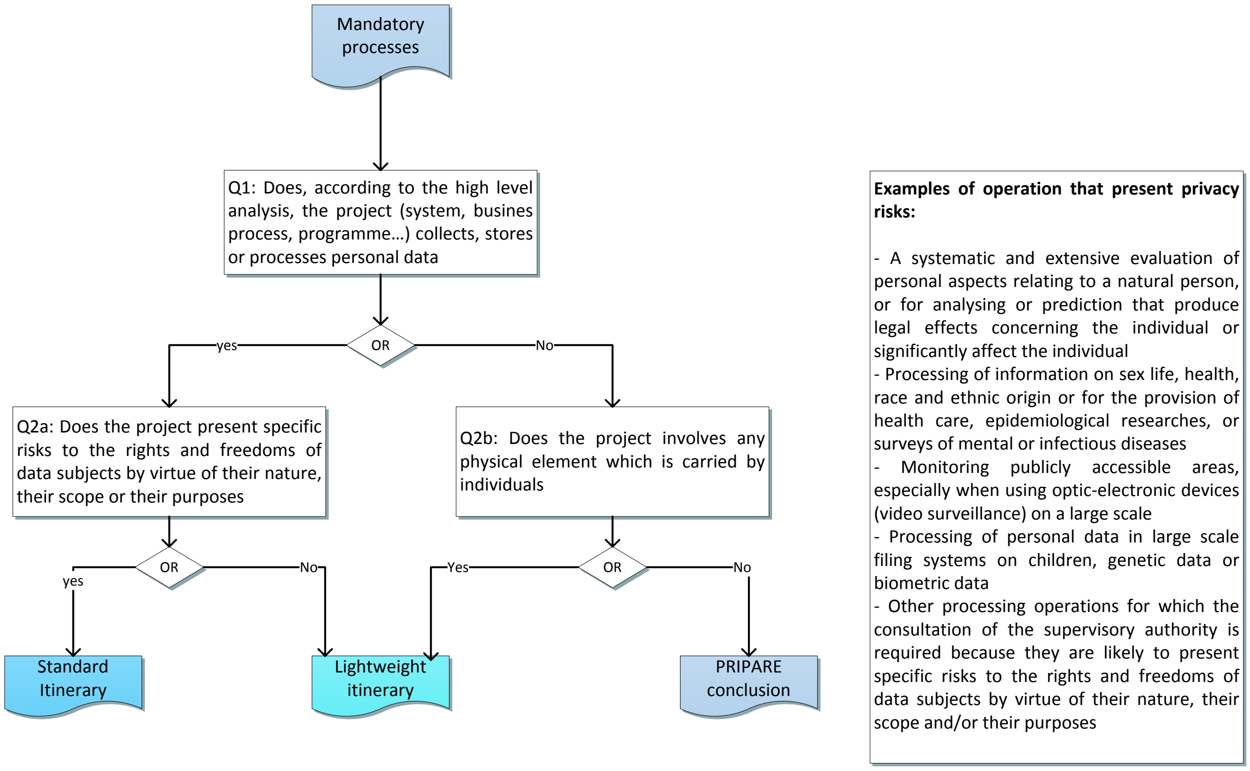
7.1 Itineraries

Because organizations and projects are so heterogeneous, it is impossible to present a one-size methodology which fits all cases. Hence is imperative to assist new adopters through the process of merging PRIPARE with their everyday practices and to select the right processes to follow. This handbook presents two main guides, one to help practitioners in choosing amongst a set of pre-selected processes (see section 7.1) and the second one to assists with the merging aspects (see section 7.2).

PRIPARE is designed to provide flexibility to its practitioners. Practitioners may choose whatever processes they want to implement or follow, adapt them to their own needs and merge them with their own practices.

However, providing a number of itineraries (set of ordered processes) may help beginners understand the process and facilitate a faster adoption of the PRIPARE's methodology

The following diagram (Figure 14) has been developed in order to help practitioners to discover the right itinerary to follow:


Mandatory processes
Q1: Does, according to the high level analysis, the project (system, busines process, programme…) collects, stores or processes personal data
OR
yes
No
Q2a: Does the project present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes
Q2b: Does the project involves any physical element which is carried by individuals
OR
yes
No
OR
Yes
No
Standard Itinerary
Lightweight itinerary
PRIPARE conclusion

Examples of operation that present privacy risks:

- A systematic and extensive evaluation of personal aspects relating to a natural person, or for analysing or prediction that produce legal effects concerning the individual or significantly affect the individual
- Processing of information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases
- Monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale
- Processing of personal data in large scale filing systems on children, genetic data or biometric data
- Other processing operations for which the consultation of the supervisory authority is required because they are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes

Figure 14: Itinerary selection process

Following, and in order to ease non privacy experts in the determination of the collection, storage or processing of personal data, a non-exhaustive list of attributes, extracted from ISO 29100[101], which can be considered personal data:

- Age and special needs of vulnerable natural persons
- Home address
- Criminal investigation reports
- Personal identification numbers (PIN) or passwords
- Allegations of criminal conduct IP address
- Customer number
- Personal interests derived from tracking use of web sites
- Any information collected during health service provision
- Location derived from telecommunications systems
- Date of birth
- Personal or behavioural profile
- Bank account or credit card number
- Medical history
- Diagnostic health information
- Personal telephone number
- Biometric identifier
- Name
- Disabilities
- Photograph or video identifying a natural person
- Credit card statements
- National identifiers (e.g. passport number)
- Doctor bills
- Product and service preferences
- Criminal convictions or committed offences
- Personal e-mail address
- Employees' salaries and human resources files
- Racial or ethnic origin
- Financial profile
- GPS position
- Trade-union membership
- Religious or philosophical beliefs
- Gender
- GPS trajectories
- Utility bills
- Sexual orientation

Processes identified as mandatory provide the necessary insight of the project and the assessment which will lead to decide if a project needs to follow PRIPARE (or other PSbD methodology) and the scope of its application (lightweight or heavyweight)

[101] ISO 29100 - Privacy Framework, http://standards.iso.org/ittf/PubliclyAvailableStandards/c045123_ISO_IEC_29100_2011.zip

7.1.1 Mandatory

This itinerary includes the necessary steps to identify if the project collects or processes any personal data and if it presents specific privacy or security risks. After identifying the main components, features, protocols, etc. of the system and its compliance with the regulation, practitioners must decide to continue (or not) with the application of PRIPARE and to follow a lightweight or a heavyweight itinerary. Including these basic processes as mandatory will help practitioners to take well-assessed and documented decisions. The main output of this itinerary is an initial impact assessment describing the systems and processes involved; the collected and processed data and potential privacy or security risks which affect the system (if any). If there is no personal data involved, the initial impact assessment will reflect so and, by having it signed by a responsible, will provide the necessary means to ensure certain level of accountability.

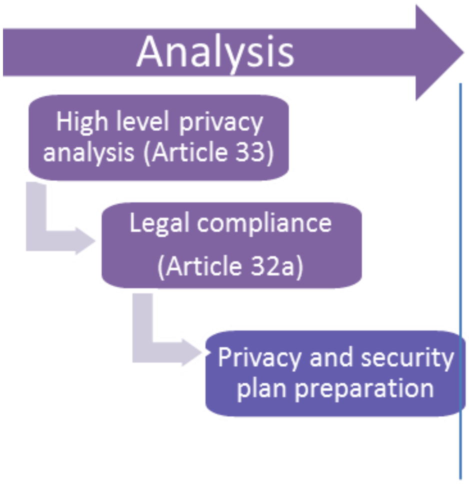

Analysis
High level privacy analysis (Article 33)
Legal compliance (Article 32a)
Privacy and security plan preparation

Figure 15: PRIPARE's mandatory processes

7.1.2 Lightweight

This itinerary has been designed for organizations with limited resources (e.g. SMEs) and for organizations engineering system where no sensible personal data is collected or processed and there are not specific risks on the rights and freedoms of the data subjects.

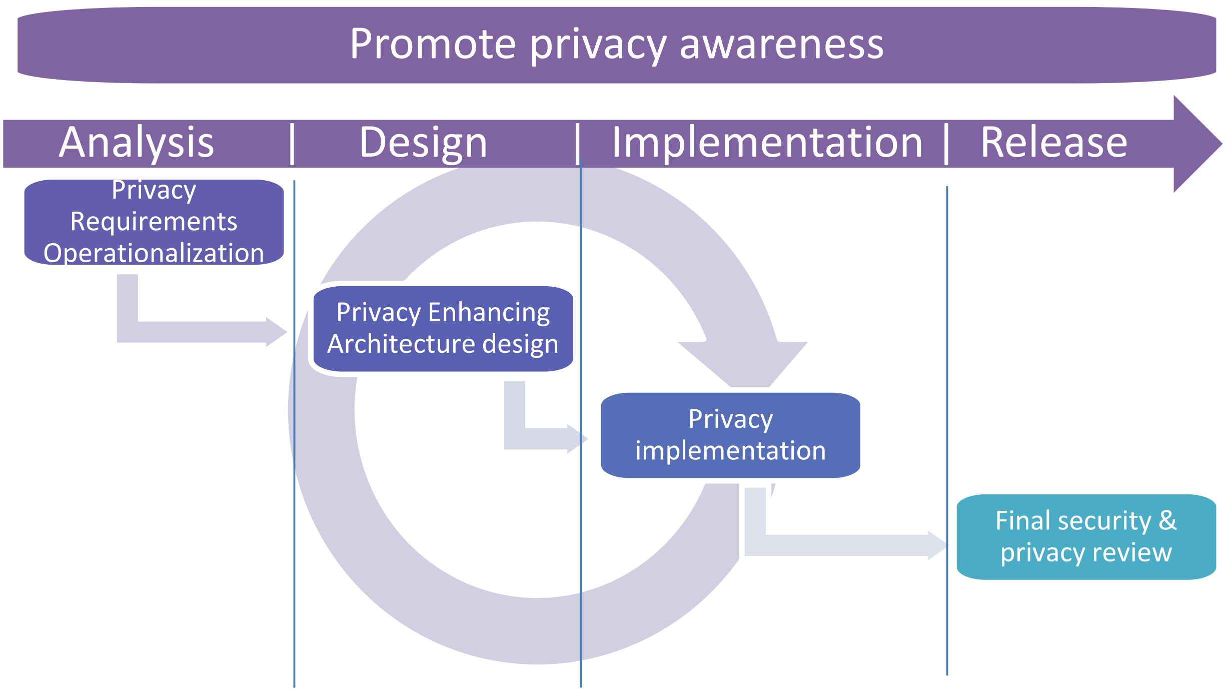

Promote privacy awareness
Analysis
Design
Implementation
Release
Privacy Requirements Operationalization
Privacy Enhancing Architecture design
Privacy implementation
Final security & privacy review

Figure 16: PRIPARE's lightweight itinerary

Considering that the organizations may be small and probably will not have appointed privacy officers nor security or privacy specialists, the best approach for the **privacy awareness** process is to encourage self-education. PRIPARE will publish useful material for this purpose as part of the work in Work Package 4[102].

The **high level privacy analysis** should be enough to identify the security and privacy needs for the engineered system and will probably be affected by standard threats to the security and privacy. A **privacy requirement operationalization** process based in a standardized list of guideline and controls, will allow engineers to identify to effectively achieve the privacy goals.

Having the list of privacy controls to incorporate to the system, engineers will **choose the right architecture** for their implementation, refining it **by applying relevant privacy patterns**. The privacy implementation process will ensure that developers will follow the best security and privacy practices that are relevant for the underlying system (e.g. OS, programming language…).

Before the system release, the person/office responsible for the project must **ensure that the PRIPARE methodology has been correctly followed** and the system has **incorporated all the privacy and security controls** specified during the system analysis.

[102] PRIPARE methodology's final version will link to the educational material-

7.1.3 Standard

The following itinerary has been designed for small organizations developing systems and wishing to be compliant with the current EU DPD and the forthcoming EU GDPR whenever the systems are likely to present specific risks on the rights and freedoms of the data subjects.

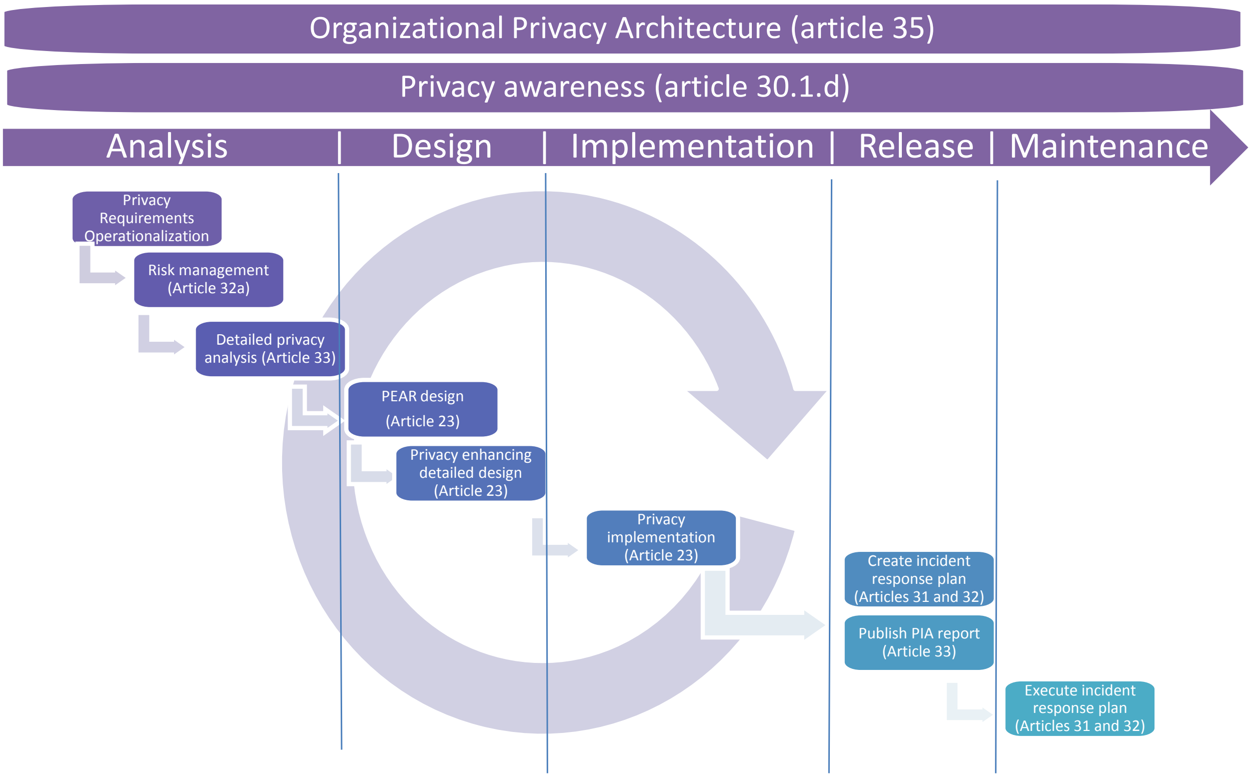

Organizational Privacy Architecture (article 35)
Privacy awareness (article 30.1.d)
Analysis | Design | Implementation | Release | Maintenance
Privacy Requirements Operationalization
Risk management (Article 32a)
Detailed privacy analysis (Article 33)
PEAR design (Article 23)
Privacy enhancing detailed design (Article 23)
Privacy implementation (Article 23)
Create incident response plan (Articles 31 and 32)
Publish PIA report (Article 33)
Execute incident response plan (Articles 31 and 32)

Figure 17: PRIPARE's standard itinerary

Each of the processes has been matched to corresponding articles in the regulation (as proposed in the draft approved by the European Council[103]) in order to reflect the obligations that are specifically addressed within the processes.

Other articles of the EU DPD and the GDPR (e.g. 6, 7, ,9 …) are contemplated along all processes thanks to their reflection in privacy principles and targets, whose threats are analysed and mitigated by the means of privacy & security controls which are incorporated into the system's design and implementation.

The scope of the privacy awareness process will likely depend on the size and resources of the organization applying the methodology. Large organizations which may have privacy and security organizational architecture and/or dedicated personnel may establish privacy and security programmes in order to raise awareness about these issues among their employees and even customers. Small organizations may base this process on self-awareness using online resources (such as the ones provided by PRIPARE).

[103] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

7.2 Merging with existing methodologies

PRIPARE methodology is not a standalone methodology and must be merged with existing engineering practices. As the integration of an engineering/management process may not be evident in some cases, PRIPARE provides suggestions on how it can be merged with some of the most prevalent engineering practices.

> PRIPARE has considered Annex four – "Mapping project and risk management concepts onto the PIA process" of the UK ICO Conducting privacy impact assessments code of practice[104] in order to determine some of these mappings.

7.2.1 Integrating ISO 9241-210 User-Centered Design Process

The ISO 9241-210 already captures the main phases that a user-centered design process must follow. PRIPARE can integrate this as showed in which shows ISO's main phases and how PRIPARE' processes map to them.

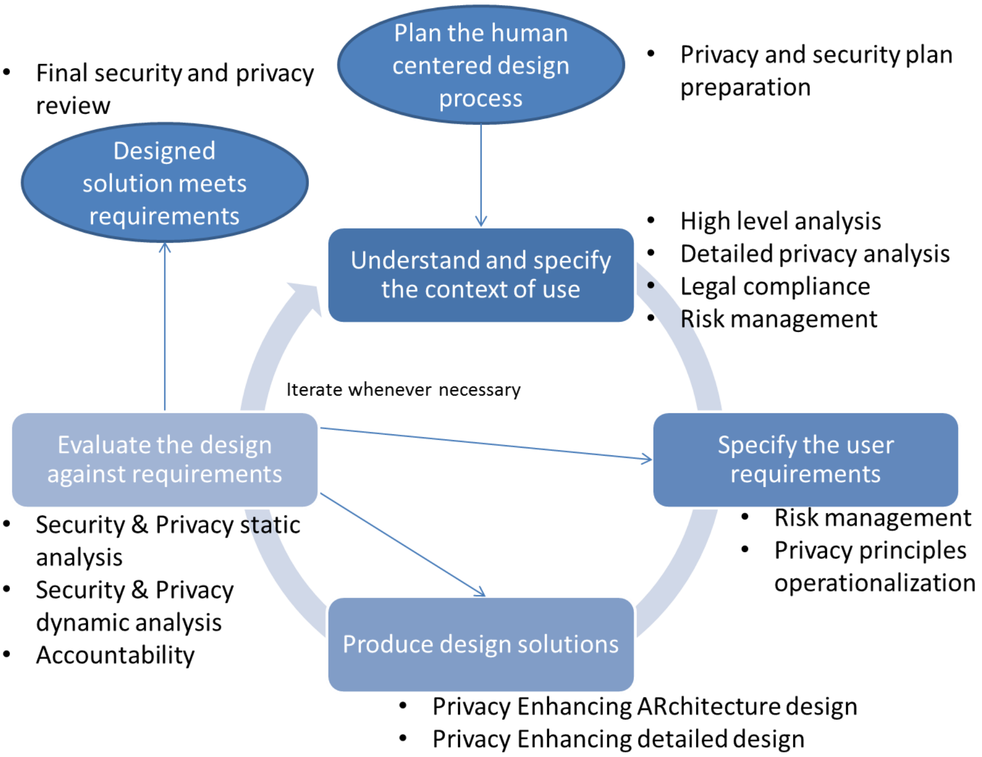

Plan the human centered design process
Privacy and security plan preparation
Final security and privacy review
Designed solution meets requirements
Understand and specify the context of use
High level analysis
Detailed privacy analysis
Legal compliance
Risk management
Iterate whenever necessary
Evaluate the design against requirements
Specify the user requirements
Security & Privacy static analysis
Security & Privacy dynamic analysis
Accountability
Risk management
Privacy principles operationalization
Produce design solutions
Privacy Enhancing ARchitecture design
Privacy Enhancing detailed design

Figure 18: ISO 9241-210 user-centered design process mapped to PRIPARE processes

The following process could be used to ensure that the design of the UI, and specially its security and privacy aspects, follows a user-centered process.

User-centered UI design				
Suppliers	**Inputs**	**Process**	**Outputs**	**Consumers**

[104] http://ico.org.uk/about_us/consultations/~/media/documents/library/Corporate/Research_and_reports/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

- Business and system analysts	- Functional description (external) - Privacy analysis	- Contextualize: Identify users and context - UI Prototype development - UI evaluation - Usability testing - Against specified privacy controls	- User Interface Specification	System developer
Tools & Techniques	Prototyping, focus groups			
Knowledge	Usability, accessibility			
Responsible	UI designer			

The process is based in three main steps:

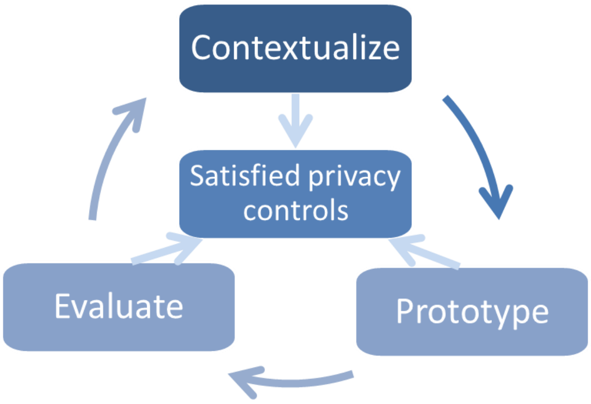


Figure 19: User-centered UI design process

Contextualize

Privacy controls that require to interact with end users and which have been identified to be a necessary part of the final design have to be contextualized so they are meaning and useful for these end users and data subjects. Hence the need to identify and categorize these users in order to understand their background needs and how they usually interact with systems. E.g. is not the same to design the UI of an eHealth system oriented for elder people than a fitness application for youngsters. While in both cases the same principles should be embedded and operationalized, the privacy controls which have to embedded have to be contextualized to the users and the environment in which the system will be used.

UI Prototype development

Creating draft versions of a product enables measuring system attributes before its development, reducing expenses due to inefficient versions. These interactive drafts or UI prototypes must reflect the expected functionality for the system focusing on the interface while not including distracting visual elements. Practitioners should pay specific attention to:

- **Awareness**: ensure that data subjects are aware of the existence of privacy preferences (set at the most privacy-preserving mode by default), of opportunities to exercise their rights and of the existence of privacy policies.
- **Discoverability**: ensure that that design emphasizes the ease which with data subject find and access privacy information and functionality (e.g. preferences).

- **Comprehension**: ensure that the data subject easily understands what privacy policies and settings actually mean (e.g. privacy icons).

Some sources can and should be consulted in order to guide practitioners in the development of privacy-friendly UI components and metaphors:

- Article 29 issued Opinion 10/2004 on More Harmonised Information Provisions[105] which recommends having multi-layered formats for presenting information for data subjects;´
- Article 29 issued Opinion 02/2013 on apps on smart devices[106] which includes specific recommendations at different levels (e.g.: application, app store and operating system levels) for following privacy principles;
- PrivacyPatterns.org[107] includes several UI privacy patterns (e.g. ambient notices or asynchronous notice) which can be applied in the design of privacy-friendly UIs.
- Mozilla foundation has worked on some privacy icons[108] which can be used to visually represent privacy policies, enhancing its comprehension.
- Amendments[109] provided by the EU Parliament to the EU DPR in March 2014 included an annex describing a set of privacy icons which shall be used to provide information to the data subject.
- Ann Cavoukian also includes some examples of good UI PbD practices in its Privacy by Design and User Interfaces guide[110].

UI Evaluation

The developed prototypes must be evaluated in order to measure usability and functional aspects. In order to keep focus on the user-centric aspects of this process, evaluation techniques must involve end-users representatives. Practitioners may follow “qualitative” approaches where small focus groups are presented with the prototypes and asked to interact with them while experts ask them question and take notes of their interactions, discovering improvement points. Other potential approach is the so called “quantitative” approach, a prototype is sent to a large number of potential users which individually test the prototype and send their feedback which is aggregated to provide meaningful information.

Engineers must also evaluate the prototypes in order to ensure that expected and UI based privacy controls have been reflected in the design.

[105] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf

[106] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[107] http://privacypatterns.org/

[108] https://wiki.mozilla.org/Privacy_Icons

[109] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402

[110] https://www.ipc.on.ca/images/Resources/pbd-user-interfaces_Yahoo.pdf

This process is iterative in itself, meaning that in order to maximize the results, several iterations should be conducted, producing each time a more privacy-friendly and usable UI prototype.

Contextualize: *GreenPriTech programme is aimed to all their customers which own EV. These represent a very broad spectrum of the society: users which are in driving age range,*

Prototype development: *GreenPriTech designers create a three-layered privacy notice which is presented in the organizations web, its mobile application and the charging customers' terminals. Each version is visually optimized to the screen size.*

Evaluate*: GreenPriTech conducts an online survey presenting the privacy notices for the three layers followed by a questionnaire to measure the users' understanding. The prototype is refined until the result is satisfactory.*

7.2.2 Software and system engineering methodologies

7.2.2.1 Waterfall methodologies

The figure below describes a waterfall methodology.

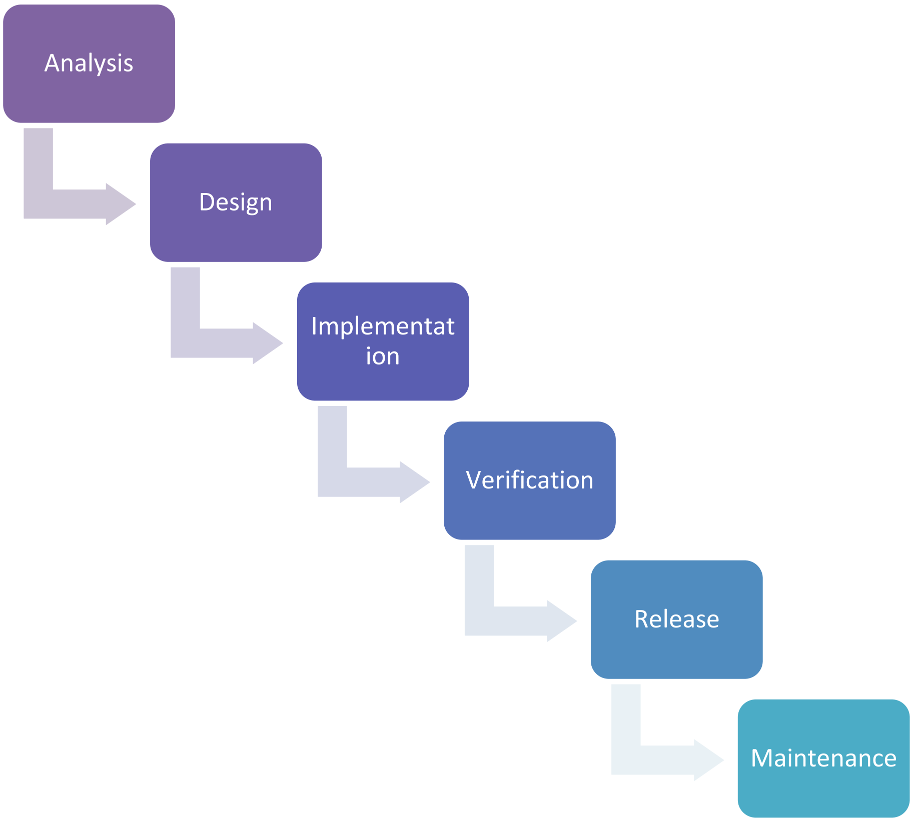


Figure 20: Waterfall methodology

The integration of this kind of methodologies with PRIPARE is straightforward as the phases are easily matched, as reflected in Table 6:

	Organization	Analysis	Design	Implementation	Verification	Release	Maintenance	Decommissioning
Environment & Infrastructure								
Organizational Privacy Architecture	x							
Promote privacy awareness	x							
Analysis								
Privacy and security plan preparation		x						
Functional Description and High-Level Privacy Analysis		x						
Operationalization of Privacy Principles		x						
Legal compliance		x						
Risk management		x						
Detailed privacy analysis		x						
Design								
Privacy Enhancing Architecture (PEAR) design			x					
Privacy Enhancing Detailed Design			x					
Implementation								
Privacy implementation				x				
Verification								
Accountability					x			
Security & Privacy static analysis					x			
Security & Privacy dynamic analysis					x			
Release								

	Organization	Analysis	Design	Implementation	Verification	Release	Maintenance	Decommissioning
Create Incident Response Plan						**x**		
Create system decommissioning plan						**x**		
Final Security & Privacy review						**x**		
Publish PIA report						**x**		
Maintenance								
Execute incident response plan							**x**	
Security & Privacy verifications							**x**	
Decommissioning								
Execute decommissioning plan								**x**

Table 6: PRIPARE complementing a waterfall methodology

7.2.2.2 Iterative or incremental methodologies

Iterative and incremental methodologies solve the risks that are present in waterfall methodologies due to the lack of flexibility. Such as in the waterfall case, the integration with PRIPARE is a pretty straightforward exercise. Most of PRIPARE processes should be followed during each iteration of the engineering processes in order to address new privacy and security issues stemming from the development within the previous iteration.

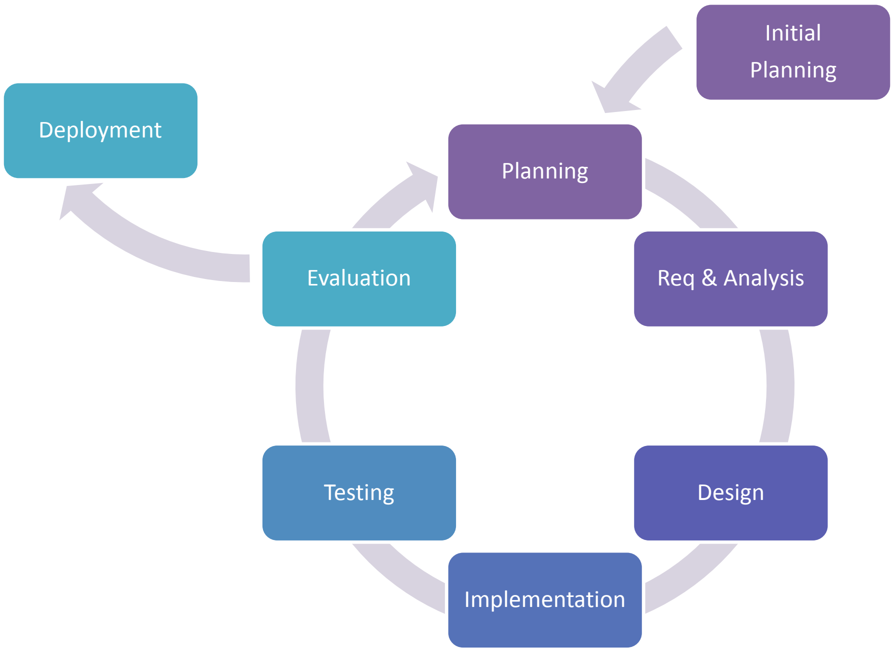


Figure 21: Iterative methodology

The following table reflects how PRIPARE processes may be matched to the phases of an iterative or incremental methodology.

	Organization	Initial planning	System decommissioning	For each iteration						
				Planning	Analysis / Requirements	Design	Implementation	Testing	Evaluation	Deployment
Environment & Infrastructure										
Organizational Privacy Architecture	x									
Promote privacy awareness	x									
Analysis										
Privacy and security plan preparation		x								
Functional Description and High-Level Privacy Analysis					x					
Operationalization of Privacy Principles					x					
Legal compliance					x					
Risk management					x					
Detailed privacy analysis					x					
Design										
Privacy Enhancing Architecture (PEAR) design						x				
Privacy Enhancing Detailed Design						x				
Implementation										
Privacy implementation							x			
Verification										
Accountability								x		
Security & Privacy static analysis								x		
Security & Privacy dynamic analysis								x	x	
Release										
Create Incident Response Plan										x

Create system decommissioning plan										**x**
Final Security & Privacy review										**x**
Publish PIA report										**x**
Maintenance										
Execute incident response plan				**Whenever necessary**						
Security & Privacy verifications									**x**	
Decommissioning										
Execute decommissioning plan			**x**							

Table 7: PRIPARE complementing an iterative methodology

7.2.2.3 Prototyping methodologies

Prototyping methodologies are a special case of iterative methodologies where intermediate and non-releasable versions are presented to the customer in order to evaluate the design and obtain their feedback.

As the system is only fully released once, PRIPARE release and verification processes have only to be followed once. However, it is strongly recommended to have a continuous verification system in order to address issues as soon as possible.

The integration of this kind of methodologies with PRIPARE is not complex and it is reflected in the following table:

	Organization	Initial planning	For each iteration						System Deployment	System decommission
			Planning	Analysis / Requirements	Design	Implementation	Testing	Evaluation		
Environment & Infrastructure										
Organizational Privacy Architecture	x									
Promote privacy awareness	x									
Analysis										
Privacy and security plan preparation		x								
Functional Description and High-Level Privacy Analysis				x						
Operationalization of Privacy Principles				x						
Legal compliance				x						
Risk management				x						
Detailed privacy analysis				x						
Design										
Privacy Enhancing Architecture (PEAR) design					x					
Privacy Enhancing Detailed Design					x					
Implementation										
Privacy implementation						x				
Verification										
Accountability							x			
Security & Privacy static analysis							x			
Security & Privacy dynamic analysis							x		x	
Release										
Create Incident Response Plan									x	

	Organization	**Initial planning**	**For each iteration**						**System Deployment**	**System decommission**
			Planning	**Analysis / Requirements**	**Design**	**Implementation**	**Testing**	**Evaluation**		
Create system decommissioning plan									**x**	
Final Security & Privacy review									**x**	
Publish PIA report									**x**	
Maintenance										
Execute incident response plan			**Whenever necessary**							
Security & Privacy verifications			**Continuously**							
Decommission										
Execute decommissioning plan										**x**

Table 8: PRIPARE complementing a prototype methodology

7.2.2.4 *Agile methodologies*

A full but summarized description of agile methodologies can be found in Michael James Scrum Reference Card[111]. Given the current relevance of SCRUM as the most prominent agile methodology, it has been chosen to demonstrate how PRIPARE can complement most of agile methodologies.

It is important to highlight the short-term vision of agile methodologies in the engineering of systems. Agile methodologies such as Scrum do not specifically contemplate an overall analysis or design phase which may limit the scope of these phases to the ongoing sprint. Scrum expects the architecture to emerge and evolve as the iterations go by, relying in the experience of the team rather than in traditional system architecture specifications. Hence, the need to establish mechanisms that may guarantee the correct addressing of privacy and security issues.

Figure 22 shows a generic Scrum process:

- The vision of the system is represented in the system/product backlog
- Each iteration or sprint consists on:
  - Planning what it is going to be done
  - Analyse, design and implement the features that were decided to be included in the ongoing iteration
  - Verify the developed features with the customer
  - Release the developed features

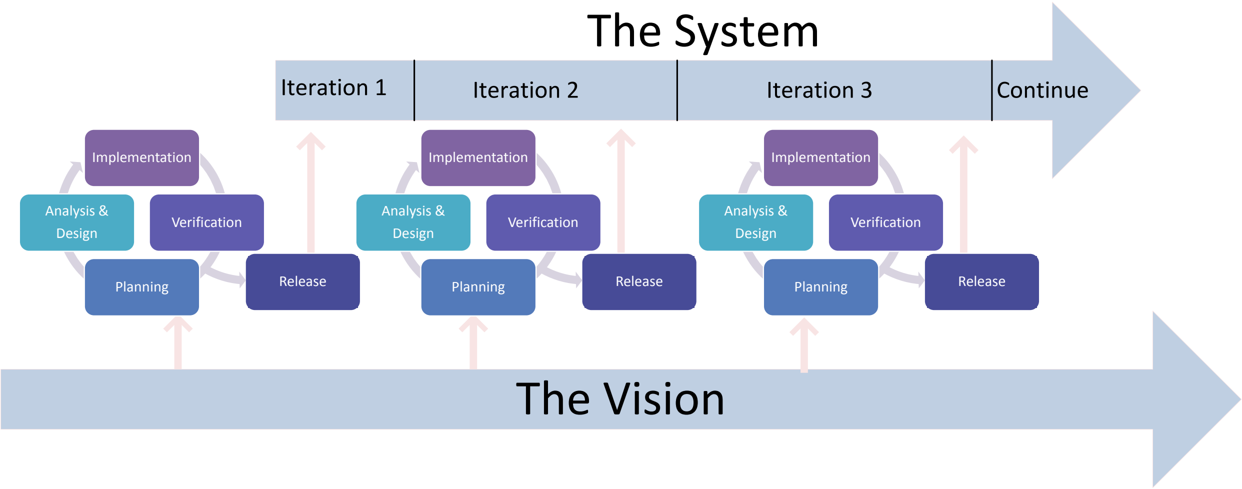


Figure 22: The scrum process

Applying privacy by design to agile methodologies poses a major challenge given that the concept of a global design does not exist. The global design emerges along the iterations and it is constantly refined to allow the integration of new features. This challenge does not only exist for privacy and security but is also applicable to all non-functional requirements or quality attributes. Two major trends exist to tackle this issue:

- **Backlog constraints**: it consists of linking backlog items (user stories) to specific non-functional requirements and specific tests;

[111] http://scrumreferencecard.com/ScrumReferenceCard.pdf

- **Non-functional user stories**: transform non-functional requirements into user stories that have to be addressed in some sprint.

Both trends have pros and cons and PRIPARE believes that a combination of the two approaches provides the best results; the selected approach at each stage should depend on the specific system and requirements.

PRIPARE has identified three different approaches to complement agile methodologies:

Incremental privacy and security

This approach highly adheres to agile principles. The main idea is to focus on only addressing the privacy and security issues stemming from the ongoing sprint, ignoring the overall vision of the system that is still to be developed. While this approach implies some business risks, e.g. having to conduct refactors due to the inclusion of features which include privacy or security risks, it allows for an agile management of privacy & security.

For each iteration, the engineering team would need to update the PSMA accordingly in order to reflect the inclusion of new systems, domains, data flows, risks, controls, impact assessment… Identifying new controls to implement should be reflected in the vision of the system by, for example, including new user stories to address the controls. The benefit of this approach is that is an incremental effort avoiding long and tedious privacy and security analysis of the whole system.

Sprint Zero

This practice is not new in the Scrum world. A sprint zero is a sprint that delivers none or a minimum amount of code but can also be used to:

- Build the backlog;
- Setup the physical environment;
- Adjust the team to the work cadence;
- Provide a high level architecture, also known as **architectural runway**[112]

Privacy and security activities can be included in this sprint in order to provide an initial analysis and design. Following sprints will be used to refine it.

Privacy and Security sprints

A different approach may be to intercalate special sprints oriented to address potential security and privacy issues. While these sprints may not add any business feature, they will allow building the PSMA and including privacy and security features that will enhance the engineered system.

[112] http://scaledagileframework.com/architectural-runway/

The following table shows how PRIPARE processes can match into an agile methodology.

	Horizontal To the Organization	System Decommission	Incremental privacy and security		Sprint Zero		Privacy and Security sprints		
			Beforehand	Each Sprint	Sprint Zero	Each Sprint	Beforehand	Each Normal Sprint	Privacy and Security sprints
Environment & Infrastructure									
Organizational Privacy Architecture	x								
Promote privacy awareness	x								
Analysis									
Privacy and security plan preparation			x		x		x		
Functional Description and High-Level Privacy Analysis				For new features	x				x
Operationalization of Privacy Principles				For new features	x				x
Legal compliance				For new features	x				x
Risk management				For new features	x				x
Detailed privacy analysis				For new features					x
Design									
Privacy Enhancing Architecture (PEAR) design				For new features	x				x
Privacy Enhancing Detailed Design				For new features	x				x
Implementation									
Privacy implementation				x		x		x	x
Verification									
Accountability				x		x		x	x
Security & Privacy static analysis				x		x		x	x
Security & Privacy dynamic analysis				x		x		x	x
Release									
Create Incident Response Plan			x	Update if necessary	x	Update if necessary	x		Update if necessary

	Horizontal To the Organization	System Decommission	Incremental privacy and security		Sprint Zero		Privacy and Security sprints		
			Beforehand	**Each Sprint**	**Sprint Zero**	**Each Sprint**	**Beforehand**	**Each Normal Sprint**	**Privacy and Security sprints**
Environment & Infrastructure									
Create system decommissioning plan			**x**	**Update if necessary**	**x**	**Update if necessary**	**x**		**Update if necessary**
Final Security & Privacy review				**At the end of the sprint**	**x**	**At the end of the sprint**		**At the end of the sprint**	**At the end of the sprint**
Publish PIA report				**Update if necessary**	**x**	**Update if necessary**			**x**
Maintenance									
Execute incident response plan				**If necessary**		**If necessary**		**If necessary**	**If necessary**
Security & Privacy verifications				**x**		**x**		**x**	**x**
Decommission									
Execute decommissioning plan		**x**							

Table 9: PRIPARE complementing an agile methodology

7.2.3 Project management methodologies

7.2.3.1 Project Management Body of Knowledge (PMBOK©)

The PMI (Project Management Institute) developed the PMBOK® guide in an attempt to document a standard terminology and a compendium of guidelines and good practices for project management.

PMBOK® defines a set of processes in terms of inputs, tools and techniques and outputs. The process list is organized into five groups and ten different knowledge areas that should be followed during the project lifecycle.

		Process groups				
		Initiating	Planning	Executing	Monitoring & Controlling	Closing
Knowledge areas						
	Scope					
	Time					
	Cost					
	Quality					
	Human resource					
	Communication					
	Risk					
	Procurement					
	Stakeholders					

Figure 23: PMBOK process and knowledge matrix

In order to fit PMBOK knowledge/process groups structure, PRIPARE suggests to include a new knowledge area (Privacy & Security) that will work as a container for PRIPARE processes. It is important to highlight two aspects:

- PMBOK includes a risk knowledge area which is oriented to the management of the project's risk. Privacy risks should be included as part of the project risk management area. An organisation's risk management processes can be used to contribute to PRIPARE's process.
- Some processes may have some overlapping with other areas or with existing processes, Table 10 shows a proposal of process mapping that may and should be adapted for each organization.

As PMBOK® describes its set of processes in terms of inputs, tools and techniques and outputs, the SIPOC process description chosen for PRIPARE eases the merging of both methodologies.

	Process groups					Knowledge areas				
	Initiating	Planning	Executing	Monitoring & Controlling	Closing	Privacy & Security	Integration	Scope	Time	…
Environment & Infrastructure										
Organizational Privacy Architecture				x		x				
Promote privacy awareness				x		x				
Analysis										
Privacy and security plan preparation	x					x		x		
Functional Description and High-Level Privacy Analysis		x				x				
Operationalization of Privacy Principles		x				x				
Legal compliance		x				x				
Risk management		x	x			x				
Detailed privacy analysis		x	x			x				
Design										
Privacy Enhancing Architecture (PEAR) design			x			x				
Privacy Enhancing Detailed Design			x			x				
Implementation										
Privacy implementation			x			x				
Verification										
Accountability				x		x				
Security & Privacy static analysis				x		x				
Security & Privacy dynamic analysis				x		x				
Release										
Create Incident Response Plan			x			x				
Create system decommissioning plan			x			x				
Final Security & Privacy review			x			x				
Publish PIA report			x			x				
Maintenance										
Execute incident response plan				x		x				

	Process groups					Knowledge areas				
	Initiating	**Planning**	**Executing**	**Monitoring & Controlling**	**Closing**	**Privacy & Security**	**Integration**	**Scope**	**Time**	**…**
Security & Privacy verifications				x		x				
Decommission										
Execute decommissioning plan					x	x				

Table 10: PRIPARE complementing PMBOK®

7.2.3.2 PRINCE2

PRINCE2 is a project management methodology developed by the Office of Government Commerce (OGC). It is widely used in the UK but has also been adopted more globally (mostly in Australia or Europe. Despite the fact that PRINCE2 was initially developed for ITC project development; its last version is compatible with any project typology.

PRINCE2 is a process driven methodology that is based on:

- Seven principles: continued business justification, learn from experience, defined roles and responsibilities, manage by stages, manage by exception, focus on products and tailored to suit the project environment;
- Seven themes: business case, organization, quality, plans, risk, change and progress;
- Seven processes: Starting up a project, initiating a project, directing a project, controlling a stage, managing stage boundaries, managing

PRIPARE proposes to include a new Privacy and security theme, as it is an area of the project that must be addressed continuously. This theme must be integrated into each of the seven processes. One possible approach to this integration is presented in Table 11. Most of design and implementation processes are mapped to the “Controlling a stage” PRINCE2 process. PRIPARE wants to reflect with this mapping that they are day to day system engineering activities that should be controlled by project managers during the corresponding stages.

	Corporate or Program Management	Processes							Themes				
		Starting up a project	Initiating a project	Directing a project	Controlling a stage	Managing product delivery	Managing Stage boundaries	Closing a project	Privacy & Security	Business case	Organization	Risk	…
Environment & Infrastructure													
Organizational Privacy Architecture	x								x				
Promote privacy awareness	x								x				
Analysis													
Privacy and security plan preparation		x							x				
Functional Description and High-Level Privacy Analysis			x						x				
Operationalization of Privacy Principles			x						x				
Legal compliance					x				x				
Risk management					x				x			x	
Detailed privacy analysis					x				x				
Design													
Privacy Enhancing Architecture (PEAR) design					x				x				
Privacy Enhancing Detailed Design					x				x				
Implementation													
Privacy implementation					x				x				
Verification													
Accountability						x			x				
Security & Privacy static analysis						x			x				
Security & Privacy dynamic analysis						x			x				
Release													
Create Incident Response Plan							x		x				
Create system decommissioning plan							x		x				

	Corporate or Program Management	Processes							Themes				
		Starting up a project	Initiating a project	Directing a project	Controlling a stage	Managing product delivery	Managing Stage boundaries	Closing a project	Privacy & Security	Business case	Organization	Risk	…
Final Security & Privacy review							x		x				
Publish PIA report							x		x				
Maintenance													
Execute incident response plan					x				x				
Security & Privacy verifications					x				x				
Decommission													
Execute decommissioning plan								x	x				

Table 11: PRIPARE complementing PRINCE2

Annex A: PSMA Template

TITLE

A.1 Purpose

A short introduction to the purpose of following and PRIPARE as a privacy & security by design methodology and documenting elicited issues, decisions…

A.2 Privacy & security team

Identify main responsibles for the conduction of PRIPARE and their roles within the project.

E.g. specify who is the data protection officer or the privacy and security expert/s in the organization, which are the stakeholders (internal and external) consulted and involved in the process.

Name	Role description
Name	**Position and description**

Table 12: Privacy & Security team

A.3 Introduction and objective

A high level conceptual description of the system to be engineered, what are its main goals….

A.4 Itinerary and roadmap

Describe the set of processes which will be followed, establish their scope and how they relate to organization's own practices.

A.5 Definitions

Provide a glossary with domain and technological specific terms that will accompany the assessment.

A.6 Functional description

Provide a description of how the system should work, a useful way to present this description us by providing user stories a functional requirement catalogue…

A.6.1 Privacy stakeholders / actors

Provide a list of *any stakeholders creating, managing, interacting with, or otherwise subject to, personal data managed by a system within a privacy domain.*

A.6.2 Domains and roles

Systems and data subjects should be associated to different domains where different policies may apply.

A.6.3 Relevant business processes, products, systems and applications within systems

- The relevant business processes within the identified products. E.g. in a billing system the customer enrolment process would be very relevant.
- Identify all the products relevant to the system, including third party ones. E.g. if developing a new billing system, other products or programmes may be point rewarding system, discount programmes…
- The relevant business processes within the identified products and processes. E.g. in a billing product, a relevant system would be the one which collects the billing data, the one which generated the bills, the one which charges the bills.…

A.6.4 Data subject(s) associated

Identify which are the subjects that are associates with the engineering system/process. E.g. different system operators with different roles, end users, customers…

A.6.5 Data flows and touch points

Identify all the data flows. Presenting it in a multi-level (domain, system) matrix allows for an easy identification of the relevant touch points.

		Domain 1				Domain2	Domain3	Domain4
		System1.1	System1.2	System1.3	System1.4	System2.1	System3.1	System4.1
Domain 1	System1.1							
	System1.2							
	System1.3	Flow1	Flow2					
	System1.4				Flow3			
Domain2	System2.1							
Domain3	System3.1					Flow4		
Domain4	System4.1	Flow5						

Table 13: Data flow matrix

A second table can provide extra information for each of the data flows.

Data flow	Description	Non-personal data	Personal data	Identifiable data	Example
Flow1	Description of flow1	Data1, data2	Data3, Data4	Data3, Data4	D1,D2,D3,D4

Table 14: Data flow details

A.7 Impact assessment

A.7.1 Policies and regulation

All policies and practices which affect the system, it may include different regional regulations, organization's policies, best practices…

A.7.2 Privacy principles / targets

Identify the privacy principles or targets and sub-targets that apply to this system taking into account organizations and stakeholder policies, regulations, best practices and standards that may affect the system. Privacy principles and targets may be at a very high level and should be identified with a unique code. It is useful to also identify the "origin" of the principle (e.g. the EU Data Protection Directive).

Code	Privacy target	Description	Reference
P1	Safeguarding quality of personal data	Quality of data and transparency are key targets that need to be ensured. Data should be accurate and, where necessary, kept up to date.	EU DPD 6d (Section I)

Table 15: Privacy targets

Sub-targets must be related to these high level targets but much more specific. They also should be uniquely identified

Code	Privacy or security target	Description
P1.1	Ensuring fair and lawful processing through transparency	E.g. providing a description of the data processing activities required for product and service delivery, ensuring internal and external transparency
P1.2	Providing purpose specification and limitation	E.g. providing the specific purposes for every collected or processed data
P1.3	Ensuring quality of data	E. g. ensuring accuracy, up-to-dateness, erasure or rectification of data that is incorrect or incomplete.
P1.4	Ensuring limited duration of data storage	E.g. ensuring that data permitting identification of the data subject is not stored longer than necessary.

Table 16: Privacy sub-targets

A.7.3 Risk assessment

For each privacy target evaluate the protection demand for it. Several methods can be followed, but should take into account, the impact of not achieving the target, from the customer (or end user) point of view as well as from the organization. PRIPARE suggests following CNIL approach[113].

A.7.3.1 Information assets

Identify what are the assets that must be protected. These assets can be categorized into primary information assets and secondary information assets. Secondary information assets include any information that strongly correlates with any primary information assets (e.g., charging location correlates with home and working place, the total fee correlates with financial status, etc.). Any adversary having access to primary information assets might potentially be able to infer any secondary information assets. The reason for this distinction between primary and secondary assets is that the real harm from access to primary assets generally materializes for the data subjects through the secondary assets. Therefore, instead of assessing the harm of primary assets, we focus on the harm of the correlated secondary assets, which are usually the most sensitive assets for the data subjects.

A.7.3.2 Adversary/Risk sources

Identify what is the threat model to be considered and what are the potential risk sources. E.g. a cloud provider can or cannot be trusted to follow agreed policies.

A.7.4 Feared events

Identify and list all the feared events that may prevent the achievement of the identified privacy principles and targets. Feared events affect the processing and operation of the system and may affect the principal and secondary information assets;

CNIL’s approach categorizes the potential impacts of the materialization of the feared event

- The level of identification of all personal data (identified beforehand) must be assessed. In other words, how easy is it to identify data subjects
- The prejudicial effect. In other words, how much damage would be caused by all the potential impacts?

Both estimations follow a 1 to 4 scale (from negligible to maximum) and are added in order to calculate the severity using the following table:

Level of identification + prejudicial effects	Corresponding Severity
< 5	Negligible
= 5	Limited
= 6	Significant
> 6	Maximum

Table 17: CNIL's severity mapping

[113] http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf

Target	Level of identification of personal data	Feared event	Prejudicial effects of potential impacts	Maximum Severity
P1.1.	3 - Significant	Data subject disclosing personal data that can be used to modify credit rating	4. Maximum	Maximum

Table 18: Threats severity

A.7.5 Threats

Identify the threats (and their likelihood) that may help feared events to materialize:

Code and name	Sub-threat/guideline	Description	Likelihood	Associated privacy target
TG1 Lack of transparency	TG1.1	E.g. providing a description of the data processing activities required for product and service delivery, ensuring internal and external transparency	Significant	P1.1
	TG 1.2	Existing information describing the service is not easily accessible for the data subject. The information is not well-indexed and / or searchable	Maximum	P1.1
	TG 1.3	The basic concept as well as the purpose underlying the service is not clearly explained.	Negligible	P1.1, P1.2
	TG 1.4	Existing information describing the service is not easily understandable and / or special knowledge is needed to understand it, e.g. jurisdictional terminology, company-internal abbreviations, a distinct language, etc.	Limited	P1.1

Table 19: Threats

A.7.6 Initial Impact Assessment

An initial impact assessment can give some stakeholders a useful insight to what are the major risks, at a high level, determining the need to follow PRIPARE methodology and what specific itinerary should be followed.

A.8 Conformance criteria

Identify the privacy and security-related conformance criteria of the system with an applicable privacy and security policy. These criteria must be objectively testable and/or measurable. Not implying being automatable. Rather, conformance criteria can be regarded as a list of check-points against which the system compliance can be assessed.

A.9 Design Logbook

Logbooks can be used in the engineering profession as a way to document progress and decision within a particular project. The information discovered during the engineering process as well as the decisions taken during it can be used during and after the project to discover the steps that have led to a given situation allowing to rollback wrong decisions or to understand successful ones. They also can be used as legal records in professional liability.

A.10 Privacy controls

Identify all the privacy controls that have to be implemented; they can be classified using several categories:

- Internal, External or Inherited (as in PMRM)
- By family as suggested by NIST
- The services where they belong to

They should be linked to the addressed threats/guidelines and heavily depend on the potential impact of the threats it address and the probability they occur. E.g. the control to mitigate a threat classified with a potential impact of maximum and very likely must be more exhaustive that one addressing a negligible control and with very little likeliness.

Privacy control	Affected privacy risk/conformance criteria	Implications for the project	Result
Privacy control 1	Threat 1	None	Minimised risk
Privacy control 2	Conformance criteria 1.1	Technological choice reduced to option A or B	Conform to level III

Table 20: Privacy controls

A.11 Remaining threats and recommendations

Besides the selection of threats it is possible that some threats are not fully addressed because of timeline or technical limitations. A roadmap can be established to determine how and when they will be addressed. Some action points may also be included whenever future events are foreseen (new regulations). A revision of this document must be scheduled to determine if there are new potential threats or new risks ensuring it is up to date.

Threat	Remaining severity	Remaining likelihood	Rationale
TG 1.1	Limited	Negligible	The rationale while there are no further controls which will try to take the severity of this threat to "negligible

Table 21: Remaining threats

A.12 Accountability

- Include the privacy policy documents or, at least, its foundations, expressed in natural language or using a dedicated formal language.
- Relate the privacy policy with specific privacy controls
- Describe the procedures to ensure that the privacy controls are in place and effectively working (e.g. periodically check a log or perform a specific test)

A.13 Incident response plan

Description of the response plan that has been devised to be used in case of privacy or security breaches

A.14 System Decommissioning plan

Description of the plan to be followed whenever the system is decommissioned. It shows how and what personal data can be safely removed/stored.

A.15 Final PIA report

A final report that can be shared with stakeholders showing the results of the assessment: identified risks, privacy controls, overall design, remaining risks…

Annex B List of Privacy Principles, Guidelines, and Criteria for Requirements Operationalization

This annex presents the result of compiling privacy guidelines and privacy criteria from different sources, so as to develop privacy principles defined by ISO 29100. Privacy principles, guidelines, and criteria are shown as a nested numbered list (e.g. 1.3.4 represents the fourth privacy criteria attached to the guideline 1.3, which in turn specifies principle “1. Consent and choice”). As above explained, it should be noted that these set of criteria should not be taken as definitive, despite that it represents an improved iteration over a first version: they should rather be considered as a seminal proposal for the community at large, where they can be discussed and surely improved.

1. Consent and choice

G-1.1. - Require the user’s consent or a legal basis to collect or process their personal data:

C-1.1.1. - Before collecting personal data, allow data subjects to freely authorize or deny the collection, creation, use, maintenance and sharing of personal data.

C-1.1.2. - Before collecting personal data, inform the data subjects, in a way they can understand, of the consequences of their decisions to approve or decline the collection, creation, use, maintenance and sharing of personal data.

C-1.1.3. - Before collecting personal data, provide complete and correct information upon which the data subjects can base their consent.

C-1.1.4. - Before collecting personal data, offer equitable conditions to those data subjects which do not consent to provide their personal data (that is, do not threat them with unfair disadvantage).

C-1.1.5. - When the legal framework allows the collection, creation, use, maintenance or sharing of personal data without the explicit consent by the data subjects, provide a legal basis (e.g. legal obligation, performance of a contract, vital interest, public interest, balancing right to information, scientific research, etc.), respect it, and ensure its limits are not trespassed.

C-1.1.6. - Require the data subject’s consent for international data transferences, subject to applicable legal conditions.

G-1.2. - Provide adequate privacy information when personal data is directly collected from the data subjects, so as to guarantee that they can make a free, specific and knowledgeable choice:

C-1.2.1. - When personal data is directly collected from the data subjects, inform them about: which is the data controller and who represents it; which data will be processed, for what purposes it will be used and under which processes it will be go; what third parties will receive the personal data and what personal data will each receive; which personal data is optional and what are the consequences if the data subject opts for not providing it; plus the data subject’s access and rectification rights.

C-1.2.2. - When personal data is directly collected from the data subjects, ensure that they read the relevant information, by employing affordances that make difficult to bypass the privacy notice.

C-1.2.3. - When personal data is directly collected from the data subjects, ensure that they understand the relevant privacy information without any special knowledge, by providing easy to access and read information.

G-1.3. - Provide adequate privacy information when personal data is obtained without the direct intervention of the data subjects:

C-1.3.1. - When personal data is obtained from a third party, inform the data subjects about: which is the data controller and who represents it; for what purpose the personal data will be processed; which categories of personal data will be obtained from the third party and from which third party; what other third parties will receive the personal data and what personal data will each receive; which personal data is optional and what are the consequences if the data subject opts for preventing the third party source from providing it; plus the subject's access and rectification rights.

C-1.3.2. - When personal data is obtained from a third party, ensure that the data subjects read the relevant privacy information, by employing affordances that make difficult to bypass the privacy notice.

C-1.3.3. - When personal data is obtained from a third party, ensure that the data subjects understand the relevant privacy information, including the source of the personal data, without any special knowledge.

C-1.3.4. - Display notifications of privacy policies at the entrance of physical locations where personal data is collected.

C-1.3.5. - Display notifications of privacy policies on the products that may collect personal data and their packaging.

G-1.4. - Keep honouring the consent granted by the user afterwards:

C-1.4.1. - Once the data subjects have provided their consent, allow them to revoke their consent in a manner that is as easy as that which they used to initially provide their consent, and without imposing any cost.

C-1.4.2. - When the data subjects provide their consent, honour any preferences they express regarding the collection, creation, use, maintenance and sharing of personal data

C-1.4.3. - Before using or disclosing personal data for new uses, obtain consent from data subjects.

G-1.5. - Require the data subject's explicit consent to collect or process sensitive personal data:

C-1.5.1. - When sensitive personal data is collected or processed, obtain explicit consent from the data subjects to collect or process that sensitive personal data, on the basis of complete and correct information.

C-1.5.2. - When sensitive personal data is collected or processed, offer equitable conditions to those data subjects which do not consent to provide their sensitive personal data (that is, do not threat with unfair disadvantage).

2. Purpose legitimacy and specification

G-2.1. - Ensure legitimacy to collect and process personal data:

C-2.1.1. - Collect, create, use, maintain, and share personal data, only if and to the extent authorized by a clearly defined legal basis (including user consent or any other legal basis).

C-2.1.2. - Collect, create, use, maintain, and share sensitive personal data only if and to the extent strictly authorized by a clearly defined legal basis that provides a relevant case for the collection of that sensitive personal data.

G-2.2. - Communicate the specific purpose of personal data collected to all the stakeholders concerned:

C-2.2.1. - In the privacy notice, specify the purposes for which the personal data is collected, created, used, maintained, and/or shared.

C-2.2.2. - Transparently and clearly inform the data subjects / service users of the purposes or services for which the personal data can be used.

C-2.2.3. - If any sensitive data is used for some purpose, make explicit to the data subjects the legitimate rationale that justifies the use for that purpose.

3. Collection limitation

G-3.1. - Limit the personal data collected to the strict minimum consented and necessary.

C-3.1.1. - When personal data is collected or retained, require only those personal data that are relevant and necessary for the purpose that has been previously identified, authorized and consented by the data subject.

C-3.1.2. - Suitably specify the purpose for which the personal data can be used and the rationale for that.

C-3.1.3. - When personal data is processed, only process it for the purpose for which it was originally obtained, or for purposes compatible with it.

C-3.1.4. - When personal data is collected with the aim to use it for marketing purposes: make it optional for the data subjects to provide that information, and in case they provide it, get explicit and informed consent.

C-3.1.5. - When personal data is collected based on a legal mandate, require only the data explicitly mandated and use them for the purposes of that mandate.

4. Data minimization

G-4.1. - Avoid and minimise the use of personal data along its whole lifecycle:

C-4.1.1. - Keep only the strict minimum data necessary for the strictly specific, consented, minimal purposes.

C-4.1.2. - Periodically evaluate that all the personal data held by the organization is identified in the privacy notice and necessary for the specified purposes.

C-4.1.3. - When some personal data is no longer needed for the specified purpose, delete or anonymise it.

C-4.1.4. - When some personal data is no longer needed for the specified purpose, delete or anonymise all the back-up data corresponding to that personal data.

C-4.1.5. - When retention rules prevent unnecessary personal data from being deleted, exclude it from regular processing of personal data.

C-4.1.6. - When doing testing, training and research: Apply procedures to minimise personal data.

G-4.2. - Limit the ability of external parties from inferring personal data from sources coming from different controllers.

C-4.2.1. - Keep data from different services or different parties separated, and avoid combining them.

C-4.2.2. - Reliably separate personal data on the same device which belongs to different issuers or owners.

C-4.2.3. - Prevent unauthorized parties from tracking personal data.

C-4.2.4. - Restrict the parties (either legal entities or natural persons, including employers and contractors) that may gain access to personal data, and keep the data they can access to the minimum they need to know in order to fulfil their legitimate purposes.

G-4.3. - Minimize the traces left by transactions and interactions with a system or service:

C-4.3.1. - When the data subjects perform a transaction or otherwise interact with the system, ensure that any information associated to that event does not disclose the identity of the data subjects, and allows them to remain anonymous.

C-4.3.2. - When the data subjects perform a transaction or otherwise interact with the system, ensure that no two transactions by the same data subject can be linked with each other.

C-4.3.3. - When the data subjects perform a transaction or otherwise interact with the system, ensure that no other party can ascertain or observe whether the transaction has happened.

5. Use, retention and disclosure limitation

G-5.1. - Limit the purpose of personal data for internal use:

C-5.1.1. - Only use personal data internally for those purposes identified in the privacy notice (or the legal framework authorizing the use) and consented by the user.

C-5.1.2. - Enforce access rights and management procedures that ensure personal data can only be used for the specified purposes.

G-5.2. - Limit personal data retention and dispose personal data when no longer needed:

C-5.2.1. - Retain personal data items only for a limited time span, as needed for the purposes consented by the data subject or as required by law.

C-5.2.2. - Schedule retention policies and disposal procedures accordance with legal regulation.

C-5.2.3. - Delete, destroy or anonymise personal data when it is no longer needed.

C-5.2.4. - Ensure secure deletion, destruction or anonymization of personal data in copies, backups and archives.

C-5.2.5. - When personal data is retained for legal reasons beyond what would be needed for the purposes consented, lock that data so that it cannot be used afterwards for those purposes anymore.

G-5.3. - Limit the purpose of personal data shared with third parties:

C-5.3.1. - When personal data is externally shared with third parties, share it only for those purposes identified in the privacy notice (or the legal framework authorizing the sharing) and consented by the user, or for purposes which are compatible with them.

C-5.3.2. - When any new personal data is proposed to be shared with third parties, evaluate whether the sharing is authorized and whether the privacy notice needs to be expanded.

6. Accuracy and quality

G-6.1. - Ensure the quality of personal data collected, created, used, maintained and shared:

C-6.1.1. - When personal data is collected or created, confirm to the greatest extent practicable that it is accurate, useful, objective, relevant, timely and complete.

C-6.1.2. - When the purposes for which the personal data is used may entail benefits or harms to the data subject, particularly ensure the quality of the data.

C-6.1.3. - When personal data is collected or created, collect it directly from the data subject whenever feasible.

C-6.1.4. - When personal data is collected or created from direct input by the data subject, ensure that the data collected is complete and correct.

C-6.1.5. - When personal data is directly input by the data subject, verify all the claims they have made, before storing, sharing or using them for any purpose.

C-6.1.6. - When personal data is collected or created, thoroughly verify the identity of the data subject.

C-6.1.7. - When personal data is not directly collected from the data subject, only use sources whose reliability can be ensured and attested.

C-6.1.8. - When personal data is collected or created by automatic tools, check that the data collected is complete and correct.

C-6.1.9. - When personal data is automatically created, ensure that any personal data enriched by probabilistic algorithms does not lead to false judgements.

C-6.1.10. - Regularly, after personal data is collected: apply procedures to check (either by directly contacting the data subject or from publicly available data) for the accuracy and timeliness of personal data, and correct it as necessary.

C-6.1.11. - Rectify errors in personal data automatically.

7. Openness, transparency and notice

G-7.1. - Provide an appropriate, well-documented, public privacy notice to the data subjects, which completely describes all the processes where any personal data is involved:

C-7.1.1. - Describe [in the privacy notice] the personal data collected and the purposes for which it is collected.

C-7.1.2. - Describe all the activities that impact personal data: collection, creation, storage, use, maintenance, sharing and disposal of personal data.

C-7.1.3. - Explain the source granting the organization with authority to collect personal data.

C-7.1.4. - Describe how the organization processes personal data.

C-7.1.5. - Describe all the internal uses of personal data.

C-7.1.6. - Encompass all the activities and uses of personal data in the privacy policies.

C-7.1.7. - Provide contact information for questions or complaints.

C-7.1.8. - Refer users to the DPA and the applicable legislation.

G-7.2. - Describe any disclosure, access to or transference of personal data that may be allowed:

C-7.2.1. - Describe all the privacy stakeholders to which the data may be disclosed, and under which circumstances this may happen.

C-7.2.2. - Describe the types of external third parties with which personal data may be shared, and the purposes for which it is shared in each case.

C-7.2.3. - Describe the natural persons that may have access to the data subject's personal data, and under which circumstances this may happen.

C-7.2.4. - Describe the retention and disposal policies applied by the organization, and any legitimate rationale to retain the data beyond its initial purpose or the users consented time spam.

C-7.2.5. - Describe the controls the organization will implement in order to protect personal data.

G-7.3. - Inform the data subjects about their rights and choices in relation to their personal data, and the consequences of exercising them.

C-7.3.1. - Describe any choices data subjects have regarding how the organization uses personal data, the consequences of these choices, and the default values if they do not express their choice.

C-7.3.2. - Inform the data subjects of their rights to access, amend, remove and object to the processing of their data, and the procedures to do so.

C-7.3.3. - Inform data subjects about how they may consent or object to specific uses or sharing of personal data.

G-7.4. - Describe the aspects of the service which may be relevant for privacy:

C-7.4.1. - Explain the service concept and its purpose.

C-7.4.2. - Explain the service operation details (data flows of personal data, locations where personal data will be collected, created, stored, processed and shared, communication modes to exchange personal data between subsystems, technologies employed, etc.) and the impacts of the service on privacy.

C-7.4.3. - Cover all the areas where personal data is used and all its purposes.

G-7.5. - Provide information about processed personal data and its purpose:

C-7.5.1. - When personal data is processed, provide the data subjects with an interface to swiftly identify which personal data is processed and for what purposes it is used.

C-7.5.2. - When personal data is processed, inform data subjects whether personal data is processed and, in that case, what personal data categories are processed, for what purposes, and to which recipients it is disclosed.

C-7.5.3. - When personal data is processed, inform the data subjects whose personal data has undergone processing about: which personal data has been processed, the source of the personal data processed, the logic of any automatic processing made and decisions made upon its result.

C-7.5.4. - Inform the data subjects on their right to object to the processing of their personal data by the organization, and the potential consequences of exercising that right.

C-7.5.5. - When personal data can be used for marketing purposes: Inform the data subjects about the use of their personal data for direct marketing purposes, so as to allow them to object to these purposes.

C-7.5.6. - When personal data can be shared with third parties: Inform the data subject about the disclosure of their personal data to third parties, so as to allow them to object to that.

G-7.6. - Keep the privacy policy updated and the data subjects informed of the latest version.

C-7.6.1. - Upon changes of practice, policy or activities that affect personal data or impact privacy, revise the privacy notice.

C-7.6.2. - Keep the service information updated.

C-7.6.3. - Upon changes of practice, policy or activities that affect personal data or impact privacy, notify the data subjects about the changes.

C-7.6.4. - When personal data is used for purposes not initially described in the privacy notice, ensure the data subjects are aware of the new purposes and consent to them whenever feasible.

G-7.7. - Make the data subjects effectively grasp the contents of the privacy policy:

C-7.7.1. - Ensure that the privacy notice is easy to access and find by the data subjects, indexed and searchable.

C-7.7.2. - Ensure that the relevant service information is easy to access and find by the data subjects, indexed and searchable.

C-7.7.3. - Ensure that the privacy notice is easy to read and understand without any special knowledge (e.g. legal, corporate or company-internal jargon).

C-7.7.4. - Ensure that the relevant service information is easy to read and understand without any special knowledge (e.g. legal, corporate or company-internal jargon).

C-7.7.5. - Make privacy policies available in all the natural languages data subjects will probably use.

G-7.8. - Disseminate privacy activities performed:

C-7.8.1. - Publish privacy practices in an easily accessible way, associated to the organization online presence.

C-7.8.2. - Provide the public with a channel to communicate with the organization CPO.

8. Individual participation and access

G-8.1. - Allow data subjects to exercise their right of access:

C-8.1.1. - Allow data subjects to access their personal data maintained in the organization records.

C-8.1.2. - Process access requests in accordance with the relevant legal requirements and (global or industry-specific) policies.

G-8.2. - Ensure the quality of any access to personal data:

C-8.2.1. - When data subjects request access to personal data, check their identity before allowing access.

C-8.2.2. - When data subjects request access to personal data, automatically obtain individualised personal data.

G-8.3. - Allow data subjects to exercise their right to object:

C-8.3.1. - Allow data subjects to object, when personal data is collected, to the processing of their personal data by the organization.

C-8.3.2. - Allow data subjects to object, at any moment after personal data is collected, to the processing of their personal data by the organization.

C-8.3.3. - When personal data can be used for marketing purposes: Allow data subjects to object, when personal data is collected, to the use of their personal data for direct marketing purposes.

C-8.3.4. - When personal data can be used for marketing purposes: Allow data subjects to object, at any moment after personal data is collected, to the use of their personal data for direct marketing purposes.

C-8.3.5. - When the organization can automatically decide based on personal data in the realm of service: Allow data subjects to object to automated decisions that are merely based on automated processing of personal data.

C-8.3.6. - When personal data can be shared with third parties: Allow data subjects to object to the disclosure of their personal data to third parties.

C-8.3.7. - Notify relevant third parties when the data subjects object to the processing of their personal data.

C-8.3.8. - Notify relevant third parties when the data subjects issue a new objection to the disclosure of their personal data to third parties.

G-8.4. - Allow data subjects to exercise their right to erasure:

C-8.4.1. - Allow data subjects to correct, amend, erase, and block individual data from the personal data maintained about them in the organization records.

C-8.4.2. - Notify the result of the erasure operations to data subjects, whenever feasible.

G-8.5. - Ensure the quality and consistency of personal data upon the exercise of the right to erasure:

C-8.5.1. - When data subjects request that their personal data be corrected, amended, erased or blocked, check the identity of the data subject beforehand.

C-8.5.2. - When data subjects request that their personal data be erased, erase individual data from backup data.

C-8.5.3. - Forward the corrections, amendments, erasures and blockings made, to third parties with which the personal data has been legitimately shared.

G-8.6. - Ensure fair, equal opportunities for data subjects to exercise their participation rights:

C-8.6.1. - Provide a simple, fast, efficient, and inexpensive channel for data subjects to exercise their participation rights.

C-8.6.2. - Publish the rules that determine how data subjects may exercise their right of access.

C-8.6.3. - Publish at the corresponding DPA registry the procedures to access personal data maintained by the organization.

G-8.7. - Keep track of situations where the exercise of the participation right is not admitted:

C-8.7.1. - Record any unresolved challenges regarding participation rights, i.e. whenever the rights to access, rectification or objection are not fulfilled.

C-8.7.2. - Forward any unresolved challenges to data processors and third parties which might have had access to the personal data subject to challenge.

9. Accountability

G-9.1. - Document all the privacy practices, policies, procedures and record the operations performed with personal data:

C-9.1.1. - List all the systems that create, collect, use, maintain, or share personal data, and the personal data managed by each.

C-9.1.2. - Label each personal data item in the information system with the purposes it can be applied to.

C-9.1.3. - Maintain and regularly update the inventory of personal data.

C-9.1.4. - When personal data held by the organization is disclosed, record the details of the disclosure: personal data disclosed, purpose of the disclosure, timestamp and recipient of the disclosed data.

C-9.1.5. - When personal data held by the organization is disclosed, retain the details of the disclosure for as long as the affected personal data is held, and for the minimum duration established legally in case the personal data is deleted before that.

C-9.1.6. - When personal data held by the organization is disclosed, allow the data subjects to access the recorded details of the disclosure, upon their request.

C-9.1.7. - When data subjects request access to personal data, log successful access and disclosure of personal data.

C-9.1.8. - When data subjects request that their personal data be corrected, amended, erased or blocked, log successful access and disclosure of personal data.

C-9.1.9. - Deliver reports to the DPAs to demonstrate accountability with privacy policies and legal regulations.

C-9.1.10. - Deliver reports to the organization managers, so as to monitor progress of and compliance with privacy practice.

G-9.2. - Increase the awareness of privacy throughout the organization and provide internal training:

C-9.2.1. - Transparently inform the employees and contractors of the purposes and services for which the personal data can be used.

C-9.2.2. - Develop, implement, and update a comprehensive training and awareness strategy aimed at ensuring that the staff understands privacy responsibilities and procedures.

C-9.2.3. - Regularly train all the staff on basic privacy aspects.

C-9.2.4. - Regularly train staff responsible for personal data or involved in activities that deal with personal data on specific privacy issues targeting the activities dealt with in their respective positions.

C-9.2.5. - Train internal staff on the appropriate use of personal data by third parties and the consequences of unauthorized sharing.

C-9.2.6. - Periodically enforce staff to sign acceptance of responsibilities for privacy requirements and record their acceptance.

G-9.3. - Establish an organization-wide privacy governance program:

C-9.3.1. - Develop an organization-wide privacy plan which defines the strategies to implement privacy policies, controls and procedures.

C-9.3.2. - Develop operational privacy policies and procedures that govern the use of privacy controls.

C-9.3.3. - Disseminate privacy governance policies.

C-9.3.4. - Enforce the use of privacy controls as established by the privacy governance policies.

C-9.3.5. - Ensure all the legal and regulatory instruments regarding the creation, collection, use, maintenance, sharing and disposal of personal data are obeyed.

C-9.3.6. - Continuously monitor legal changes.

C-9.3.7. - Periodically update the privacy governance program, privacy policies and procedures.

C-9.3.8. - Designate a Chief Privacy Officer (CPO) in charge of the privacy governance program, since its inception to its implementation and update.

C-9.3.9. - Allocate responsibilities to ensure that the privacy principles are abided by throughout the organization:

C-9.3.10. - Assign human and economic resources to implement the measures defined by the privacy governance program.

G-9.4. - Enforce privacy requirements on contractors and external service providers:

C-9.4.1. - Establish privacy roles, responsibilities, and access requirements for contractors and service providers.

C-9.4.2. - Include privacy requirements in documents related to contracts, procurement and acquisition.

C-9.4.3. - When personal data is automatically shared, establish Privacy Service Level Agreements which specify the personal data covered by the agreement and the purposes for which it may be used.

C-9.4.4. - Allocate responsibilities to supervise Privacy Service Level Agreements and ensure that they comply with the privacy regulation.

C-9.4.5. - When personal data is disseminated, define guidelines to maximize its quality and integrity.

G-9.5. - Respond to privacy incidents:

C-9.5.1. - Implement a response plan to privacy incidents.

C-9.5.2. - Respond to privacy incidents in an organized and effective way, and in accordance with the response plan.

C-9.5.3. - Limit the damage if any unauthorised person accesses personal data.

C-9.5.4. - When a privacy breach happens, inform all the data subjects that might have been affected.

C-9.5.5. - When a privacy breach happens, inform all the privacy stakeholders of it.

C-9.5.6. - Establish sanctions and remedies to privacy breaches, and enforce them in the event that any might occur.

C-9.5.7. - Establish compensations of privacy breaches, and apply them to all the data subjects affected in the event of any breach occurring.

G-9.6. - Manage complaints suitably:

C-9.6.1. - Establish a process to receive privacy complaints or questions and providing swift and appropriate responses to them.

10.Information security

G-10.1. - Ensure the system works reliably, even in heterogeneous environments or upon error conditions:

C-10.1.1. - Ensure the compatibility of approved access devices among them and with the system infrastructure (if any), even when they are supplied by different providers or manufacturers, so that the system works as specified.

C-10.1.2. - Provide the necessary throughput levels.

C-10.1.3. - Ensure a low occurrence of problems.

C-10.1.4. - Ensure the system degrades gracefully, so that when the system is not working perfectly, the user can still use the service.

C-10.1.5. - When the system is not working perfectly, ensure that faults do not cause security difficulties.

C-10.1.6. - When the system is not working perfectly, allow authorised persons to use the service on the behalf of the users, while keeping their privacy protected.

C-10.1.7. - When the system is not working perfectly, compensate read errors.

C-10.1.8. - Protect all the system components and infrastructure against denial-of-service attacks throughout the system, considering e.g. network, radio and physical attacks.

G-10.2. - Ensure the usability of the system:

C-10.2.1. - Minimise explanations needed by the users to learn the service without difficulty (making it self-explanatory whenever possible), including all security and privacy features.

C-10.2.2. - Keep the user aware of the process step he or she is at any given time.

G-10.3. - Ensure the confidentiality of personal data, and monitor and control all the attempts to access it:

C-10.3.1. - Use the user personal data to identify them, make payments, deliver products, etc.

C-10.3.2. - Avoid any misuse, manipulation or sharing of personal data by or with unauthorised persons.

C-10.3.3. - Preclude unauthorised persons from accessing organization operations (e.g. shipping) which might compromise personal data.

C-10.3.4. - Secure credentials against counterfeiting, manipulation or damage.

C-10.3.5. - If credentials are stored in the service provider's system, safe-guard them.

C-10.3.6. - Provide credentials for which proofs can be provided.

C-10.3.7. - Employ non-anonymised personal data about the use of a service only for the purposes established by the organization and consented by the data subject.

C-10.3.8. - Establish agreements that regulate the usage of personal data by different organizations, as well as conflict resolution.

C-10.3.9. - Prevent third parties from profiling data subjects by tracking service usage information.

C-10.3.10. - Decouple personal data from transponders allocated to physical objects.

C-10.3.11. - Protect personal data and/or credentials from being used by persons who are willing to commit violent acts.

C-10.3.12. - Ensure confidentiality of non-anonymous usage data.

C-10.3.13. - Safeguard personal data from any intentional or unintentional use or disclosure.

C-10.3.14. - Safeguard personal data to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

G-10.4. - Ensure and account for data integrity of personal data:

C-10.4.1. - Use security controls to ensure the integrity of personal data and document its usage.

C-10.4.2. - When personal data is processed, log any processing made, so that any potential misuse can be detected.

C-10.4.3. - Assure data is available throughout the service lifecycle, including post-sales when applicable.

C-10.4.4. - Ensure the availability and integrity of usage data.

C-10.4.5. - When a service has been used, inform the user of the usage records, including time, service provider, location, etc.

C-10.4.6. - Ensure the reliability of usage data that might influence permissions or billing.

C-10.4.7. - Trace data used for pricing and ensure its reliability.

C-10.4.8. - Allocate incomes from the use of services to the different agents involved in the service provision.

C-10.4.9. - When new or modified systems contain personal data, or when the inventory is updated, inform the chief officer in charge of Information Technology, so as to establish and update the security requirements.

11. Privacy compliance

G-11.1. - Assess privacy impact and risks:

C-11.1.1. - Assess the need for privacy and impact risk assessment in the project.

C-11.1.2. - Consult internal and external stakeholders affected by privacy.

C-11.1.3. - Identify privacy and related risks.

C-11.1.4. - Identify and evaluate the privacy solutions.

C-11.1.5. - Document the actions needed to reduce, mitigate or accept the risks identified.

C-11.1.6. - Integrate the assessment outcome into the project plan.

G-11.2. - Integrate privacy safeguards into products by default and since their inception:

C-11.2.1. - Automate the inclusion and development of privacy controls within information systems designed by the organization, so that they support privacy.

C-11.2.2. - When doing testing, training and research: Implement personal data protection controls.

C-11.2.3. - Provide default settings that protect the privacy of individuals.

G-11.3. - Monitor and audit privacy practice:

C-11.3.1. - Establish internal controls that assure compliance with privacy law and internal policies and procedures.

C-11.3.2. - Make privacy policies, procedures and activity subject to external, independent supervision.

C-11.3.3. - Regularly monitor and audit privacy policies and privacy controls.

C-11.3.4. - Audit sharing of personal data with third parties.

G-11.4. - Register at the applicable Data Protection Authority (or supervisory organism) registries:

C-11.4.1. - Register systems which collect or use personal data at the respective DPA.

C-11.4.2. - Keep records at the DPA current.

C-11.4.3. - Get subject to oversight by DPA.

C-11.4.4. - Publish the procedures to correct, amend, erase, and block personal data at the DPA registry.