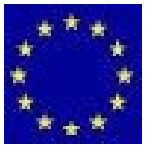
PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Deliverable D4.2

Initial Educational Material

Due M15 - December

Project:	PRIPARE
Project Number:	ICT-610613
Deliverable:	D4.2
Title:	Initial educational material
Version:	v0.2
Date:	31/12/2014
Confidentiality:	Public
Author:	Claudia Roda, Susan Perry (AUP) José M. del Álamo, Yod-Samuel Martin (UPM) Pagona Tsormpatzoudi, Fanny Coudert (KUL) Hisain Elshaafi (TSSG) Frank Kargl, Henning Kopp (UULM) Carmela Troncoso (Gradiant)



Funded by the European Union's Seventh Framework Programme

Table of Contents

Document History

Version	Status	Date
v0.1	Draft	15/5/2014
v0.2	Added structure and partners contributions	4/11/2014
v0.3	Added partners' modules	10/12/2014
v0.4	Added partners' comments	17/12/2014
v1.0	Final	21/12/2014

Approval		
	Name	**Date**
Prepared	Claudia Roda (Ed.)	14/12/2014
Reviewed	All Project Partners	17/12/2014
Authorised	Antonio Kung	21/12/2014

Circulation	
Recipient	**Date of submission**
Project partners	21/12/2014
European Commission	21/12/2014

List of Figures

None

List of Tables

Abbreviations and Definitions

Acronym Table	
Acronym	**Definition**
29WP	Article 29 Working Party
AFCO	Constitutional Affairs' Committee
Belspo	Belgian Science Policy Office
C2C	Car to Car
C2I	Car and Infrastructure
CEPS	Centre for European Policy Studies
CIPM	Certified Information Privacy Manager
CIPP/IT	Certified Information Privacy Professional/Information Technology
CNECT	Communications Networks, Content and Technology
CS	Computer Science
DG	Directorates-General
DPA	Data Protection Authorities
DPO	Data Protection Officer
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
EMPLO	Employment, Social Affairs & Inclusion
EU	European Union
FRA	Fundamental Rights Agency
FTC	Federal Trade Commission
GRC	Governance, risk management, and compliance
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IAPP	International Association of Privacy Professionals
ICT	Information Communication Technology
IT	Information Technology

JHA	Justice and Home Affairs
JRC	Joint Research Centre
MARKT	Internal Market and Services
NGO	Non-Governmental Organization
OECD	Organisation for Economic Co-operation and Development
PSbD	Privacy and Security-by-Design
PET	Privacy-Enhancing Technology
PIA	Privacy Impact Assessment
PRIPARE	Preparing Industry to Privacy-by-design by supporting its Application in Research
REST	Representational State Transfer
RFID	Radio Frequency Identifier
RTD	Research and Technological Development
SbD	Security-by-Design
SOAP	Simple Object Access Protocol
TTE	Transport, Telecommunications, and Energy Council
UN	United Nations
WSDL	Web Services Description Language

Table 1 - Abbreviations and Definitions

Executive Summary

This deliverable, composed by this document and a set of knowledge tools (modules) available online, compiles the teaching materials to be used in the PRIPARE training seminar as well as the initial version of the teaching and educational material for the General Public and Practitioners.

The knowledge tools are available at https://pripare.aup.edu/. Although only the final version of the material will be made available to the general public, partners and reviewers are provided access.

1 Introduction

The objective of this deliverable, as described in the DoW, is to compile all teaching materials that are to be used in the PRIPARE training seminar planned as Task 3.3. Further, the deliverable also contains the initial version of the teaching and educational material for the General Public and Practitioners. As a consequence, the development of the various educational supports has been guided by two objectives:

- First the consortium aimed at addressing the educational needs of the General Public and Practitioners as recognized in section 2 of D4.1 by implementing a number of the modules identified in section 4 of the same deliverable.
- Secondly, we needed to design the teaching material necessary to cover the educational goals of the training seminar aimed at introducing the privacy engineering methodology to participants from research and industry.

In order to ensure consistency in the presentation of the material a set of templates were prepared and used by all partners for the design of the modules. The templates also display the Creative Commons licence agreed upon by all partners in the consortium. This licence allows for commercial use but no derivatives of the material. The following templates were made available:

- A template for slides (PPT) plus a template for a descriptive of the module called below "PRIPARE description"
- A template for reading lists
- A template for miscellaneous modules

1.1 Multidisciplinarity

In creating the educational material for the PSbD methodology we have considered that PbD is impacted by, and impacts on, several domains as the various teaching subjects normally include regulatory, technological, business, and societal aspects. All these are taken into account by the various modules and, as discussed below, must be properly integrated in any curricular sequence. For example, practitioners acting mostly at the technology level (ICT-practitioners) will need a good knowledge of PbD (methodology, terminology, applicability), know how to conduct a Privacy Impact Assessment and use it to guide system design and steer choices throughout the lifecycle of the system. They will also need a deep knowledge of Privacy and Security Enhancing Technologies, including, for example, cryptography and anonymisation techniques. They must understand the limitations of such techniques as tools capable of supporting the implementation/enforcing of regulations of which they will need to be aware of but at a lesser level of details than, for example, regulators. On the other hand practitioners concerned with regulatory aspects will need to have a detailed knowledge of the current and proposed EC regulation and of how their interventions should be based on a risk management approach, they will need to be able to manage controversial regulatory issues and be aware of business-related privacy issues, work with PIA and know PbD (methodology, terminology, applicability) but their level of knowledge about Privacy and Security Enhancing Technologies will need a lesser level of detail than that of ICT-practitioners.

As planned in D4.1 each module may present a subject to a set of stakeholders at one of two **levels**, either "general knowledge" or "specific knowledge". Modules at the "general knowledge" level are meant to introduce a subject to an audience who may be completely new

to that subject and may not need to acquire in-depth knowledge about it (e.g. a module covering Privacy Enhancing Technologies at the "general knowledge" level may be suitable for presentation to regulators in the context of a course on privacy regulations). Modules at the "specific knowledge" level are meant to provide in-depth knowledge on a given subject (e.g. the same module covering Privacy Enhancing Technologies at the "general knowledge" level may be suitable for introducing the subject to ICT practitioners and will be followed by a module at "specific knowledge" level on the same subject in the context of a course on privacy technology). The two level system is therefore ideal for ensuring that multidisciplinarity is not only embedded in the modules but can be furthered when building complete sequences.

1.2 Contents of the deliverable

This deliverable is organised in four parts, the first two covering our first objective (educational material for the general public and practitioners), the third part covering our second objective (material for the training seminar) and a fourth part reporting on the state of advancement of material planned for D4.3.

In order to distribute the material we have temporarily made it available via a portal open only to partners and reviewers. The portal can be accessed at https://pripare.aup.edu/

2 General Public Education Material

The stakeholder analysis presented in D4.1 has resulted in the identification of a set of educational modules for the general public that have been reorganised as described in table 2.

As compared to the modules described in D4.1 the "tools for privacy protections" and "smart use of smart devices" have been reorganised to form a single booklet on privacy protection so that lay users can have a single reference tools providing guidelines and information about practical actions that they may take to protect their privacy online. The booklet will be delivered as part of D4.3. Also, the module "The PbD cartoon" has been joined to the section on "Dangers of privacy violations and privacy rights" rather than being on its own section on "Privacy by design in privacy protection" since the utility of PbD for the protection of privacy has been mentioned throughout the modules.

General Public				
Subject	Module	Presentation mode	Content	Partner
Dangers of privacy violations and privacy rights	A Day in the Life of Max	Infograph	Typical privacy violations	AUP
	The PbD game	Puzzle game	Typical privacy violations for children	AUP
	Do you feel observed?	Printed brochure	Addressed to the *digitally reluctant explaining* what happens to citizens' private information, even if they do not use digital tools	AUP
	The PbD cartoon	Cartoon for children	Explains to children the basic tenets of privacy by design and what sort of embedded privacy choices they should look for when online	AUP
PbD in specific contexts	Work	Infographic or brochure	Privacy threats and risk management: at work	AUP
	School		Privacy threats and risk management: at school	AUP
	Transport System		Privacy threats and risk management: transport	AUP
	Smart spaces		Privacy threats and risk management: smart spaces	AUP
	Medical records		Privacy threats and risk management: medical records	AUP
Privacy Protection	Tools for privacy protection	booklet	Guidelines and information about practical actions users can take to protect their privacy online	AUP
EU Legal Order	Existing legal sources	Slides + reading material	The module describes the legislative initiatives that illustrate the state of the art in the EU legal order as well as the context within which they function	KU Leuven

Table 2 – General Public Educational Material – highlighted in grey is the module that will be released as part of D4.3

The modules implemented so far (all except the booklet) include:

- Awareness material on PbD (e.g. A day in the life of Max, Do you feel observed?)
- Material for short information sessions or distribution to families on PbD for children (e.g. The PbD cartoon, The PbD game)
- Material for short information sessions or distribution to families on PbD for adults (e.g. A day in the life of Max, EU Legal order: existing legal sources)

Below is a short description of each module available in final draft form.

2.1 Dangers of privacy violations and privacy rights: A Day in the Life of Max

Title: A Day in the Life of Max

Theme: the hidden dangers and consequences of the use of our everyday technologies

Audience: general public, writ large

Presentation: infographic

Level: general knowledge

Available at: https://pripare.aup.edu/node/aDayInTheLifeInfograph

Summary: The average person has a basic understanding that improper use of social media sites, spam emails, and banking sites can have a negative impact on their lives but there are so many more invasive technologies that this very same "average person" doesn't think twice about.

Authors: Alicia Weber, Dayna Foudy, Othmane Mechatte, Zona Zarić, Susan Perry and Claudia Roda (AUP)

Related modules: PbD at work; PbD at school, PbD in transport systems, PbD in smart spaces, PbD for medical records

OVERVIEW:

The general idea of the infographic is presenting the reader with the normal day-to-day activities of the average person (such as Max buying a coffee on the way to a medical check-up) along with information on how some of our most quotidian activities (getting into a car with GPS for example) may be privacy invasive. The infographic follow the subject from the time he wakes up until he sleeps at night to see how many times a day his privacy is invaded possibly without his knowledge. Different icons correlate to the four different key issues pinpointed (Facial recognition, cloud, geo-location and WI-FI) that will allow the reader to relate to specific technologies.

LEARNING OBJECTIVES:

Raise awareness about the extremely sensitive and vulnerable nature of personal information in any aspect of the daily lives of the general public, writ large. Information privacy is only one aspect of privacy. Other types of privacy include bodily privacy, territorial privacy, and communications privacy. The infographic not only provides the public with information about "old habits" and the way they impact our privacy, but also informs about some of the new forms of threats to privacy.

2.2 Dangers of privacy violations and privacy rights: The PbD game

Title: *The PbD game*

Theme: dangers encountered online and throughout social media

Audience: children, parents and young adults

Presentation: cross-word puzzle

Level: general knowledge

Available at: https://pripare.aup.edu/node/116

Summary: *This crossword puzzle presents in a simple and visually attractive way the vocabulary associated to the misuse of digital tools and consequent dangers and violations of privacy. It aims to raise awareness amongst children, parents and young adults about important questions such as how to keep personal data confidential, how to protect from unwanted advances, what is allowed and what is punishable by law etc.*

Authors: Estelle Nguyen, Susan Perry and Claudia Roda (AUP)

Related modules: The PbD cartoon

OVERVIEW:

This simple game serves as a visual tool that easily attracts and explains the gravity of the every-day threats children can encounter online. Children and minors are the most vulnerable members of the general public, and in most cases also the least informed about privacy. This game helps children becoming acquainted with the vocabulary of online threats and defence mechanisms.

LEARNING OBJECTIVES:

Raise awareness of the need for better privacy protection through Privacy by Design principles in order to reduce the risk of cyberbullying, online sexual harassment, catfishing or online indoctrination.

2.3 Dangers of privacy violations and privacy rights: Do you feel observed?

Title: *Do you feel observed?*

Theme: Dangers of privacy violations and privacy rights

Audience: General public: digitally reluctant

Presentation: Brochure

Level: general knowledge

Available at: https://pripare.aup.edu/node/117

Summary: *Addressed to the digitally reluctant explains that digital privacy breaches may occur to them even if they do not use digital tools and informs them of their rights of their new rights under the upcoming EU Data protection Act (2017).*

Authors: S. Perry, C. Roda (AUP)

Related modules:

OVERVIEW:

Even those citizens who do not use computers or are rarely online may be subject to privacy violations. Because information is stored online by banks, stores and even grocers, all citizens run the risk that their private information may be sold or made available to unauthorized businesses. The Data Protection Regulation, which is expected to be enforced from 2017, will guarantee citizens the right to be forgotten; the right to give consent; the right to be informed of all online breaches within 72 hours; and the right to due process through their national data protection agency.

LEARNING OBJECTIVES:

- Awareness about the fact that digital privacy breaches may occur even if someone is not online
- Awareness about citizens right to protect their privacy according to the EU Data Protection Act
- Awareness about Data Protection Authorities

2.4 Dangers of privacy violations and privacy rights: The PbD cartoon

Title: The PbD cartoon

Theme: privacy by design in privacy protection

Audience: children, parents and young adults

Presentation: comic strip

Level: general knowledge

Available at: https://pripare.aup.edu/node/118

Summary: This comic strip is designed to educate children and young adults about their rights and responsibilities while online, as well as the risks and dangers, showing them how to protect their own and respect others privacy, and empowering them to realise the importance of doing so.

Authors: Monica Selledj, Susan Perry and Claudia Roda (AUP)

Related modules: The PbD game

OVERVIEW:

This comic strip serves as a sample visual tool that easily attracts and explains the gravity of cyberbullying. Children and minors are the most vulnerable members of the general public, and in most cases also the least informed about privacy. It is tailored primarily for children, to attract their attention and spark their curiosity about privacy and privacy by design.

LEARNING OBJECTIVES:

Raise awareness of the need for better privacy protection through Privacy by Design principles in order to increase online security and avoid having children be the victims or suspects of cyberbullying.

2.5 PbD in specific contexts: Work

Title: *Privacy at Work*

Theme addressed: Employee protection of privacy in the workplace

Target Audience: Employees and their employers.

Mode of Presentation: Infographic

Level: General knowledge

Available at: https://pripare.aup.edu/node/119

Summary: This infographic provides a balanced presentation of employer concerns and employee rights concerning privacy. Statistics and examples allow anyone in the workplace to have a better idea of what is at stake and how to protect their privacy through Privacy by Design in the broad sense, i.e. through principles such as transparency, proportionality, empowerment of the user and the rights of data subjects.

Authors: Zona Zaric, Susan Perry, Claudia Roda (AUP)

OVERVIEW:

Employers are concerned about productivity in the workplace and may wish to monitor worker performance through, for example, online surveillance of Internet connections at work or the review of employee emails on office servers. The 1995 European Union Data Protection Directive provides no information on any aspect of employment relationships, leaving this to the discretion of Member States. Certain States, such as France, prohibit email monitoring without express consent. Other States, such as Poland, have few rules regarding workplace surveillance. Nonetheless, the European Union Working Party 29 suggests that "monitoring must be proportionate, not excessive for the intended purposes, and carried out in the least intrusive way possible". Privacy by design encourages proportionality, a balance in employer-employee relations with respect to the use of digital technology allowing the creation of systems which enable employers to monitor worker performance while respecting employees privacy. Employees who suspect that their employer does not respect such a balance are encouraged to contact their national data protection agency in order to know their rights with respect to privacy in the workplace.

LEARNING OBJECTIVES:

- Better understand employer and employee concerns regarding digital privacy in the workplace
- Know where to go for further information (national data protection agency)

2.6 PbD in specific contexts: School

Title: *Privacy at School*

Theme: Protecting student and teacher privacy at school

Audience: Parents, students and teachers

Presentation: Infograph

Level: General knowledge

Available at: https://pripare.aup.edu/node/120

Summary: This infographic provides parents and older students with a clear summary of three key issues regarding digital privacy at school and the right to freedom of expression. Freedom to speak and write freely is circumscribed only by the rights of others to be free from defamation, hate speech and obscene language. Privacy by design anticipates the need for privacy at school by focusing on principles such as transparency, proportionality, the rights of data subjects and user empowerment.

Authors: Zona Zaric, Susan Perry, Claudia Roda (AUP)

OVERVIEW:

Freedom of expression must be balanced with the right to privacy. Any online activity must be respectful of the rights of others to be free from defamation, hate speech, threats and obscene language. Students may be held responsible for their online opinions, and may not engage in digital bullying or harassment of any kind. No conversation may be recorded without prior permission of all speakers, and sexually explicit information is prohibited. Students cannot defame teachers or one another online. The immediacy of the Internet and the extension of social networks render it a powerful tool that students must learn to use responsibly.

LEARNING OBJECTIVES:

- Students should understand how to balance freedom of expression with the right to privacy
- Students should understand that they are fully responsible for their online content

2.7 PbD in specific contexts: Transportation System

Title: *Privacy when using Transportation*

Theme: Privacy by Design in modes of transport

Audience: General public

Presentation: Infographic

Level: General knowledge

Available at: https://pripare.aup.edu/node/121

Summary: In our effort to make transportation safer, cleaner and more efficient, intelligent transportation systems and GPS technology may violate the user's right to privacy. By tracking an electric vehicle's location or charging activity, for example, more data may be transmitted to unauthorized sources than we are aware. **Privacy by design introduces concepts to minimize the amount of information collected and to control its use while we commute to work, go to the doctor, to a political meeting, to a friend's house, etc**.

Authors: Zona Zaric, Susan Perry, Claudia Roda (AUP)

OVERVIEW:

Cameras may film us when we board a train or metro car, enabling public authorities to control crime and manage commuter traffic. A charging meter for an electric car may facilitate our payment by accepting credit cards or a digital fingerprint. In both cases, the user has little control over the use of this personal information - the video image or digital fingerprint. While safety, greener transport and effective payment methods are of critical importance for commuters, so is the right to individual privacy. Privacy by design systems, such as Anonymous Authentication Protocols, allow us to decouple our credit card information, for example, from our name and car location, thereby preserving our right to individual privacy.

LEARNING OBJECTIVES:

- Alert transport users of how much data is being gathered by intelligent transport systems en route
- Encourage transport users to privilege systems that protect their privacy

2.8 PbD in specific contexts: Smart Spaces

Title: *Privacy in Smart Spaces*

Theme: Privacy by design in smart spaces

Audience: General Public

Presentation: Infographic

Level: General knowledge

Available at: https://pripare.aup.edu/node/122

Summary: Most people are unaware that computers, smartphones, surveillance cameras, and many other digital devices can obtain all sorts of information from anyone in their vicinity by using sensors. These sensors may recognize a human face, speech or the gestures of up to four people at a time, and share that information with other computers. This violates our right to individual privacy.

Authors: Zona Zaric, Susan Perry, Claudia Roda (AUP)

OVERVIEW:

Most personal data gathered by computer sensors in a smart space is stored and shared with other machines without the humans in the room either knowing, or giving their consent. In order to allow for optimal functionality of these smart spaces, individual privacy must be protected through privacy-by-design systems. Computer data generated through sensors should be minimized, stored anonymously and for a limited period, and shared with other machines only when necessary. Individuals need to be aware that the information gathered by computer sensors is subject to use that is beyond their control. Privacy by design systems provide individuals with greater protection in smart spaces through privacy enhancing protocols.

LEARNING OBJECTIVES:

- Raise citizens' awareness about the potential privacy violations posed by smart spaces
- Raise citizens' awareness about the need for privacy-by-design systems in these interconnected spaces

2.9 PbD in specific contexts: Medical Records

Title: *Privacy and our medical records*

Theme: Privacy by design to protect our medical information

Audience: General public.

Presentation: Infographic

Level: General knowledge

Available at: https://pripare.aup.edu/node/123

Summary: Our medical records contain sensitive information. Digitization of medical records and trends such as cloud computing or big data can endanger our right to medical privacy. **Privacy-by-design** systems enhance protection from human error and access to our personal data by unauthorized third parties.

Authors: Zona Zaric, Susan Perry, Claudia Roda (AUP)

Related modules:

OVERVIEW:

The digitization of medical records means that sensitive personal information is available to a larger pool of individuals than ever before. While certain individuals, such as the family doctor or local clinic, have our consent to access our medical history and prescribed treatment, insurance companies, health businesses and hackers do not. The protection of our medical privacy is closely connected to our sense of dignity and autonomy; the release of our medical records to an unauthorized party could also influence our ability to access insurance, credit and employment. **Privacy-by-design** systems protect our information by minimizing data collection, reinforcing security, and possibly rendering data that is released anonymous and untraceable.

LEARNING OBJECTIVES:

- Alerting citizens to potential violations of their medical privacy
- Encouraging citizens to privilege the protection of their medical records

2.10 EU Legal Order: Existing legal sources

Title: *The EU legal order: Data protection and privacy*

Theme: General Public Education: Existing legal sources

Audience: general public, policy stakeholders with no legal background

Presentation: slides

Level: general knowledge

Available at: https://pripare.aup.edu/node/125

Summary: The slide set provides general knowledge on the legal system governing the EU and introduces how privacy and data protection is regulated into it. Existing legislative sources but also legislative initiatives that are currently under discussion are presented. Given their impact on individuals' lives, emphasis is given on the Data Protection Directive and e-Privacy Directive as well as on the data protection reform.

Authors: Pagona Tsormpatzoudi, Fanny Coudert (KU-Leuven)

Related modules:

Modules related to general public education, introduction to the modules for legal and policy stakeholders.

OVERVIEW:

- The EU legal order
- Privacy and data protection in the European Charter of Fundamental Rights
- From the Data Protection Directive 46/95/EC to the Data Protection Reform
- Other privacy-relevant European legislation

ESSENTIAL READINGS:

- Data Protection Directive 95/46/EC
- Directive on Privacy and Electronic Communications (2002/58/EC)
- European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union Brussels, 4.11.2010 COM(2010) 609 final
- European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

LEARNING OBJECTIVES:

To understand the structure of the EU legal order and the meaning of different legislative acts that regulate data protection. To acquire a general overview on the basic legislative sources on privacy and data protection (EU Charter of Fundamental Rights, Data Protection Directive, e-Privacy Directive, Regulation on Processing of Personal Data by EU Institutions and Bodies) and the discussions on the data protection reform.

The EU legal order: Data Protection and privacy

Overview of Presentation

Slide	*Title*	*Theme*
1	The EU legal order	Title slide
2	European Data Protection law	Cover slide
3	Towards an EU single market	Cornerstones and architecture of EU law
4	Privacy and Data Protection in the EU	The two rights as they appear in the European Charter of Fundamental Rights
5	Data protection directive	Goal of the directive
6	Data protection directive	content
7	Data protection reform	Reasons
8	Data protection reform key objectives	Objectives
9	Data protection reform package	Introduction of draft regulation and directive
10	Other privacy-relevant legislation	Cover slide
11	Directive on Privacy and Electronic Communications (2002/58/EC)	Main content
12	Regulation 45/2001/EC on processing of personal data by EU institutions and bodies	Main content

3 ICT-Practitioner Training Material

The stakeholder analysis presented in D4.1 has resulted in the identification of a set of educational modules for the ICT-practitioners that have been reorganised as described in table 3. As compared to the modules described in D4.1 here we have assembled the 7 modules on privacy strategies into a single module and we have added a module on Privacy Enhancing Technology. We have removed the module focused on anonymous cash systems, since it is not relevant to practitioners as current technologies used for example in Bitcoin, like the blockchain, are yet highly experimental and their privacy or security ramifications are not sufficiently examined.

The modules in grey will be available as part of D4.3 because their contents are currently being developed within WP1 (methodology) and WP2 (Best practices). All other modules are delivered, in their final draft form, with this document.

ICT practitioners				
Subject	Module	Mode of presentation	Content	Contributing partner
PbD methodology	PRIPARE principles and concepts	Slides	Introduce the PbD concept, the PRIPARE methodology, and its foundations, providing an overview of the related terms, and motivating ICT practitioners to adopt PbD approaches.	UPM
	PRIPARE methodol. Overview	Slides	Introduce the PRIPARE methodology and its steps.	UPM
	PRIPARE methodol. Privacy requirements engineering.	Slides	Describe the PRIPARE steps to move from privacy requirements to operational requirements.	UPM
	PRIPARE methodol. PIA and risk analysis	Slides	Describe the PRIPARE steps to carry out a Privacy impact assessment and a risk analysis.	UPM
	PRIPARE methodol: Best practices	Slides	Describe the best practices selected by PRIPARE, and how they can be applied within the PRIPARE methodology.	UPM
Privacy Patterns	privacy patterns	Slides	In this module we introduce privacy design patterns, their possibilities and limitations.	UULM
Privacy Motivation	Failures in Privacy Systems	Slides	In this module we are going to examine some examples of failures in privacy systems.	UULM
Privacy Strategies	Minimise, Hide, Separate, Aggregate, Inform, Control, Enforce, Demonstrate	Slides	This module explains Hoepmans privacy design strategies, i.e., it examines abstract ways how to achieve privacy. Privacy Strategies are more abstract than patterns	UULM
Location Privacy	Location privacy	Slides, exercises	We introduce the topic of location privacy.	UULM
	Privacy in transport systems	Slides, exercises	We examine the role of privacy in transport systems and ways and technologies to achieve privacy.	UULM
PET	Privacy Enhancing Technologies	Slides	PETs, what are they, examples of PETs, anonymous credentials.	Gradiant

Table 2 - ICT Practitioner Education Material - highlighted in grey are the modules that will be released as part of D4.3

3.1 PRIPARE principles and concepts

Title: *PRIPARE: Principles and Concepts*

Theme: Privacy-by-design Principles and Concepts

Audience: ICT Practitioners

Presentation: Slides

Level: General knowledge

Available at: https://pripare.aup.edu/node/130

Summary: *This module provides ICT practitioners with general knowledge regarding privacy-by-design principles and concepts e.g. what privacy-by-design is, why it matters, PbD foundational principles, benefits of applying a PbD methodology, etc. The goal is to introduce the topic from an ICT practitioner point of view, providing an overview of related terms, and motivating and introducing the next themes.*

Authors: Jose M. del Alamo & Yod-Samuel Martin (UPM)

Related modules: The following modules provide specific topics of the PRIPARE methodology:

- PRIPARE Methodology: An overview
- Privacy requirements engineering
- Privacy impact assessment and risk analysis
- PRIPARE best practices

OVERVIEW:

The module introduces the following topics:

- **Privacy concepts**: Introduction to some privacy concepts such as personal data; privacy; informational privacy and data protection; and, privacy and PRIPARE principles.
- **Privacy-by-design grounds**: Motivation on the importance of privacy, and the current status of the state of the art in privacy engineering e.g. PbD, PIA, PETs and best practices.
- **PRIPARE methodology**: Introduction to the methodology, its phases and activities.

ESSENTIAL READINGS:

- Notario, N., Crespo, A., Kung, A., Kroener, I., Le Métayer, D., Troncoso, C., Del Álamo, J.M., Martín, Y.S., PRIPARE: A New Vision on Engineering Privacy and Security by Design, Cyber Security and Privacy Forum 2014 - CSP2014, Atenas (Grecia), 21-22 mayo 2014
- PRIPARE: Deliverable 1.1 - Privacy and Security, Concepts and Principles Report

LEARNING OBJECTIVES:

By following this module ICT practitioners will:

- be aware of the privacy-by-design concept and related terms;
- understand why privacy-by-design matters and the benefits of applying a privacy-by-design methodology to a software or system development process;
- know the PRIPARE principles and concepts supporting privacy-by-design

3.2 PRIPARE methodology: Overview

Title: *PRIPARE: Methodology overview*

Theme : Privacy-by-design methodology

Audience: ICT Practitioners

Presentation: Slides

Level: Specific knowledge

Available at: https://pripare.aup.edu/node/131

Summary: *This module introduces the PRIPARE methodology for privacy- and security-by-design to ICT practitioners. The module details each phase of the PRIPARE methodology, as well as the activities involved. Finally, it describes the different itineraries that ICT practitioners may follow to introduce the PRIPARE methodology in the project development lifecycles.*

Authors: Jose M. del Alamo & Yod-Samuel Martin (UPM)

Related modules: The following modules provide specific topics of the PRIPARE methodology:

- PRIPARE: Principles and Concepts
- Privacy requirements engineering
- Privacy impact assessment and risk analysis
- PRIPARE best practices

OVERVIEW:

The module introduces the following topics:

- **Methodology overview**: Introduction to the PRIPARE methodology, phases, activities and roles
- **Phases**: Detailed description of each phase in the software development process and the activities that a PbD-oriented development process should carry out, including:
  - **Environment & Infrastructure**
  - **Analysis**
  - **Design**
  - **Implementation**
  - **Verification**
  - **Release**
  - **Maintenance**
  - **Retirement**
- **Itineraries**: Introduction of the different itineraries of the methodology, and how to choose among them

ESSENTIAL READINGS:

- Notario, N., Crespo, A., Kung, A., Kroener, I., Le Métayer, D., Troncoso, C., Del Álamo, J.M., Martín, Y.S., PRIPARE: A New Vision on Engineering Privacy and Security by Design, Cyber Security and Privacy Forum 2014 - CSP2014, Atenas (Grecia), 21-22 mayo 2014
- PRIPARE: Deliverable 1.2 - Privacy and Security-by-Design Methodology

LEARNING OBJECTIVES:

By following this module ICT practitioners will:

- **understand** the key aspects of the **PRIPARE methodology**, and its phases and activities;
- compile information necessary for **introducing the PRIPARE methodology** in their software development process.

3.3 Privacy patterns

Title: *Privacy Patterns*

Theme: Best practices, Privacy Patterns

Audience: ICT practitioners

Presentation: Slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/126

Summary: *In this module we introduce the idea of patterns, focusing on privacy patterns.*

Authors: Henning Kopp, Frank Kargl (UULM)

Related modules: Privacy strategies

OVERVIEW:

We first introduce the idea of patterns. We also explain about the origins in architecture and of course the gang of four and then go on to explain an exemplary privacy pattern, namely location obfuscation.

ESSENTIAL READINGS:

None

LEARNING OBJECTIVES:

Privacy patterns, their origin, structure and use

3.4 Failures in Privacy Systems

Title: *Failures in Privacy Systems*

Theme: Best practices, Privacy Patterns

Audience: ICT practitioners

Presentation: slides

Level: general knowledge

Available at: https://pripare.aup.edu/node/127

Summary: *In this module we describe how failures in privacy systems can occur by choosing privacy patterns in a non-optimal way. In particular we focus on the instant messaging service iMessage and its design problems.*

Authors: Frank Kargl, Henning Kopp (UULM)

Related modules: Privacy strategies, Privacy Patterns

OVERVIEW:

In this module we focus on the instant messaging service iMessage and its design problems. They implemented encryption but did not take attention of the fact that their different messages had different length and therefore one can deduce knowledge of the type and language of the message, although it is encrypted. This also highlights the difference between security, namely preserving the integrity of the message, and privacy.

ESSENTIAL READINGS:

None

LEARNING OBJECTIVES:

The audience should learn to think about the concrete attacker model and which privacy patterns defend against that attackers and which one do not.

3.5 Privacy Strategies

Title: *Privacy strategies*

Theme: Privacy Patterns

Audience: ICT practitioner

Presentation: slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/128

Summary: *This presentation introduces Hoepmans Privacy design strategies and their rationale.*

Authors: Frank Kargl, Henning Kopp (UULM)

Related modules:

- Privacy Patterns

OVERVIEW:

This presentation introduces Hoepmans Privacy design strategies, namely minimize, hide, separate, aggregate, inform, control, enforce, and demonstrate. Privacy Design strategies are on a more general level than Privacy patterns. We discuss how they fit into the software design process and how they can be used to categorize privacy patterns.

ESSENTIAL READINGS:

Hoepman, Jaap-Henk. "Privacy design strategies." *ICT Systems Security and Privacy Protection*. Springer Berlin Heidelberg, 2014. 446-459

LEARNING OBJECTIVES:

The participants learn what privacy design strategies are, what they are good for, and how they integrate into the software design process.

3.6 Location privacy

Title: *Location Privacy in electric vehicle charging*

Theme: Privacy Patterns, Best practices

Audience: ICT practitioner

Presentation: slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/129

Summary: *This presentation talks about privacy in an electric vehicle charging scenario. We look especially at ISO 15118 and a privacy friendly reengineering of the standard, called Popcorn.*

Authors: Frank Kargl, Henning Kopp (UULM)

Related modules:

- Privacy Patterns
- Exercises for Location Privacy

OVERVIEW:

We present privacy issues in an electric vehicle charging scenario. We look at ISO 15118 and how they did not implement privacy. We then go on how Ulm University did a privacy friendly reengineering of the standard, called Popcorn. The protocol will be discussed in detail, together with the cryptographic mechanisms.

ESSENTIAL READINGS:

Höfer, Christina, et al. "POPCORN: privacy-preserving charging for emobility." Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles. ACM, 2013.

LEARNING OBJECTIVES:

The participants learn the role privacy plays in unexpected areas. They learn about location privacy and ISO 15118. They also see at an example how one can reengineer a privacy-friendly architecture.

3.7 PETs, what are they, examples of PETs, anonymous credentials

Title: *Privacy Enhancing Technologies*

Theme: Technologies and solution for implementing PbD

Audience: e.g. CS Students, ICT practitioners

Presentation: slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/114

Summary: *This lecture gives and introduction to privacy from a technical point of view, including an overview of privacy-preserving technologies. It first explains different privacy-properties and then presents technologies to protect both the privacy of data that has been disclosed, as well as technologies to minimize disclosure of data.*

Authors: Carmela Troncoso (Gradiant)

Related modules:

OVERVIEW:

This is a module presenting a technical perspective on privacy.

It first explains how privacy can be formalized from a technical point of view, in terms of privacy properties that can be achieved. Secondly, it delves in the description of a series of privacy-enhancing technologies suitable to provide privacy in presence of different adversarial models. On the one hand technologies that allow users to exercise control on how their data is processed by a trusted data controller; and on the other hand technologies that allow to minimize the amount of data disclosed to controllers or other third parties.

LEARNING OBJECTIVES:

- Understanding what achieving privacy means from a technical point of view
- Learn available methods to support privacy-protection from a technical point of view

4 Material for Training Seminar

This section identifies the educational material selected for inclusion in the training workshop, see table 4 below. The training workshop, briefly described in the introduction of this document, is organised under the direction of WP3 partners and more details are available as D3.1.

The two modules developed for the lecture on "**Privacy motivation and introduction**" are part of the material planned for students. They have been delivered earlier than originally planned to respond to the needs of the training workshop. A descriptive is available in sections 5.1.1 and 5.1.2 of this document.

The material developed for the session on "**Data protection and law**" is a first draft of the module "Basic Principles/Relevant Legislation" to be delivered within D4.3 (see Section 5.2). This material will be further elaborated to address information needs of policy stakeholders with non-legal background and of legal stakeholders with no specific background in data protection law

The material for the lecture on "**Privacy Enhancing Technologies**" has been developed specifically for the workshop by Gradiant (a partner who is not part of WP4 but has a strong knowledge of the subject) and has been added to the ICT-Practitioners' material; see section 3.9 of this document.

The two modules "PRIPARE principles and concepts" and "PRIPARE methodology: Overview", which are part of the ICT-Practitioners material (see descriptions in section 3.1 and 3.2 of this document), constitute the material that will be used to cover the two workshop lectures **Privacy Methodology I** and **Privacy Methodology II**. The latter will be linked to a case-study / example during the workshop presentation.

The introductory material for the workshop is not part of this deliverable.

2015-03-09 Training Seminar – Educational material		
Welcome & Introduction of participants	Structure of workshop, introduction of anonymous course evaluation use case	Ulm
Privacy Motivation & Introduction	Lectures – (1) Privacy Motivation, Seven types of privacy, Privacy principles. (2) Privacy and Human Rights.	AUP
Data Protection and Law	Lecture – Legal aspects of privacy, data protection regulation.	KUL
PETs	Lecture – PETs, what are they, examples of PETs, anonymous credentials.	Gradiant
Privacy Methodology I	Lecture – Introduction of the PRIPARE methodology	UPM
Privacy Methodology II	Lecture – application of the PRIPARE methodology to a sample use case	Atos, Trialog

Table 3 - Material for Training Seminar - highlighted in grey are the modules that will be released as part of D4.3

4.1 Legal aspects of privacy, data protection regulation

Title: *A legal perspective on data protection and privacy: An overview*

Theme: Material for Workshop 2: Data Protection and Law

Audience: Workshop participants (technical background)

Presentation: slides

Level: general knowledge

Available at: https://pripare.aup.edu/node/139

Summary: The slide set provides an introduction to EU data protection law. The right to data protection is unveiled in light of traditional data protection principles focusing on personal data collection, use and user empowerment. The module introduces the concept of privacy impact assessment as a methodological tool to assess compliance with the legal framework.

Authors: Pagona Tsormpatzoudi, Fanny Coudert (KU_Leuven)

Related modules: Privacy motivation and introduction, Modules related to legal education of non-legal audiences

OVERVIEW:

- **Privacy and Data Protection: two fundamental rights**
- **Privacy, Data protection by design: a legal obligation**
- **Privacy Impact Assessment: A tool to assess impact on fundamental rights**
- **Traditional data protection principles**
  - Data collection
  - Data use
  - User empowerment

ESSENTIAL READINGS:

- Data Protection Directive 95/46/EC
- European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

LEARNING OBJECTIVES:

To understand basic terms and principles of EU data protection law. To become familiar with obligations posed by the data protection directive as well as the draft general data protection regulation (data protection by design, data protection impact assessment) and how these can be taken into account in their work.

5 Material for other stakeholders (advancement report)

This section provides a brief advancement report on the material for *Students* and *Policy Makers and Governmental and non Governmental Bodies acting for Human Rights Protection* which is to be delivered as part of D4.3.

5.1 Students

In order to address the needs of the PRIPARE training workshop the planning of some of the material for students has been slightly modified. The module addressing the history of human rights treaties relevant to privacy and the related contemporary issues has been delivered earlier. The module on “Principles and processes of PbD” has been focussed on “Privacy motivation, seven types of privacy and privacy principles”, this module has been also delivered earlier. We have removed a module on “Privacy vulnerabilities and solutions in Android” as it seemed too specific compared to the other modules and better suited to be included as an example.

The early delivery modules are described below, the remaining modules are under development. Most of the slides and exercises that target computer science and engineering students have been developed pending final edits. The main remaining activities in the development of the material over the coming period will focus on finding further reading resources that relate to the topics indicated in the table below, particularly for the modules where we aim to only provide reading lists. The material for non-CS/engineering students is at various stages of development: some is being delivered early, some is being tested in some classes, others.

Students				
Subject	Module	Mode of presentation	Content	Contributing partner
CS/Engineering Students				
PET	Privacy Enhancing Technologies and limitations	Reading list, pointers to existing material	Description of privacy preserving technologies including their capabilities and limitations.	WIT
Privacy in ICT environments	Understanding privacy	Reading list, + existing material,	Overviews of privacy basic concepts, its definitions and current related ethical problems and solutions.	WIT
	Privacy in the Internet of Things	Slides, exercises, reading list	Introduction to the Internet of Things and the emerging privacy issues involved.	AUP
	Privacy enhancing techniques for Web Services	Slides, exercises, reading list	Introduction to current web services, such as SOAP, WSDL, and REST and how they address privacy	AUP
	Secure programming		Technical description of how security and privacy related techniques are considered in programming practices.	WIT
	Security and privacy in software engineering		Introductions on building privacy and security into technology products and services and the related trade-offs. Integration of privacy protection and security into the overall engineering lifecycle of such products and services including requirements, design and testing phases.	WIT
	Web security and vulnerabilities		Descriptions of background issues in Web security and common vulnerabilities. The relationship of those vulnerabilities to user and consumer privacy.	WIT
	Cryptography		Introduction to cryptography techniques with references to detailed learning material particularly in relation to privacy.	WIT
	Security vs. privacy	Slides, exercises, reading list, pointers to existing material	Comparison and relationship between security and privacy concepts.	WIT
	Anonymisation	Pointers to existing material, text, video	Introductions and detailed discussions of anonymisation techniques.	WIT
	Security and privacy patterns	Slides, exercises, reading list, pointers to existing material	Description of design patterns that support security and privacy and references to more detailed discussions.	WIT
Database Privacy	Cryptography	Slides, exercises, reading list, pointers to existing material	Introduction to cryptography techniques for protection of data at rest with references to detailed learning material.	WIT
	Web and database security and vulnerabilities		Descriptions of background issues in Web security and common vulnerabilities. The relationship of those vulnerabilities to user and consumer data privacy.	WIT
	Privacy preserving data management	Reading list, pointers to existing material	Descriptions of privacy preserving techniques in data mining and processing and current limitations, such as scalability.	WIT

PbD Privacy risks and incidents	Security management	Slides, exercises, reading list, pointers to existing material,	Description of management of organisational privacy and security risks and the use of security metrics. Description of techniques to cope with privacy issues including identifying and dealing with privacy incidents and mitigating risks in the context of PbD. Overview of threat modelling techniques.	WIT
	Privacy Impact Assessment (PIA)	Pointers to existing material	References to existing PIAs and related discussions including its applicability to PbD.	WIT
	Compliance reviews		References to resources that describe and discuss issues around compliance audits and review techniques.	WIT
Cloud Privacy	Cloud privacy patterns and best practices	Slides, reading list	Introduction to privacy and security patterns applicable to the cloud environments and references to detailed discussions.	WIT
Mobile Privacy	Privacy issues in mobile devices	Pointers to existing material	Resources on privacy issues in existing mobile device platforms.	WIT
Economic Aspects	Trust and reputation	Slides, reading list, pointers to existing material	Description of the concepts of trust, trustworthiness and reputation as well as related systems and models.	WIT
NON-CS/Engineering Students				
History leading to PbD	History of technology related to PbD	Slides and exam questions	History of technology leading to the convergence underlying current privacy problems	AUP
	History of Human Rights related to PbD	Slides	History of relevant human rights treaties and contemporary issues	AUP
Principles and processes of PbD	PbD: motivation	Slides	Privacy motivation, seven types of privacy and privacy principles	AUP
Application of EU privacy law online	EU regulation and privacy	Slides and exam questions	Current EU regulation and the debate around privacy and PbD in particular	AUP
Technology responses to privacy problems	PbD: perspectives and limitations	Slides and exam questions	How technology addresses privacy issues: perspectives and limitations	AUP

Table 5 - Educational Material for Students – Highlighted in grey are the modules delivered early for presentation at the PRIPARE training workshop

5.1.1 Privacy Motivation, Seven types of privacy, Privacy principles

Title: *Privacy Motivation and Introduction*

Theme: Introduction to privacy

Audience: IT practitioners and students

Presentation: slides

Level: general knowledge

Available at: https://pripare.aup.edu/node/138

Summary: *This module introduces the concept of privacy in digital systems including societal and ethical concerns and possible technical solutions.*

Authors: Claudia Roda (AUP)

Related modules: Privacy and human rights, EU legal order

OVERVIEW:

This module introduces the concept of privacy in digital systems addressing privacy concerns, their causes and their relation to other societal concerns such as freedom of expression, security, and economic benefits. It identifies the types of privacy that we may want to protect and the ethical concerns that arise with recent technology development as well possible technical ways to address them. The language is non-technical.

ESSENTIAL READINGS:

- Claudia Diaz and Seda Gürses (2012) Understanding the landscape of privacy technologies. Extended abstract of invited talk in proceedings of the Information Security Summit, pp. 58-63, 2012
- Rachel Finn, David Wright and Michael Friedewald (2013) Seven Types of Privacy in S. Gutwirth et al. (eds.), European Data Protection: Coming of Age, DOI 10.1007/978-94-007-5170-5_1, © Springer Science+Business Media Dordrecht 2013

LEARNING OBJECTIVES:

- Understand the ethical, societal and personal concerns related to privacy
- Gain a basic awareness of the multiple types of current technological answers to privacy protection issues

5.1.2 Privacy and Human Rights

Title:	*Privacy as a human right*
Theme:	protection of privacy and related rights under the international human rights treaty regime
Audience:	Students and technology specialists
Presentation:	slides
Level:	general knowledge
Available at:	https://pripare.aup.edu/node/142

Summary: *Protection of privacy and other related human rights is guaranteed by the binding treaty law of the international human rights regime, which has been expanding since the founding of the United Nations in 1945. All European Union countries have signed these treaties and the conventions have been incorporated into domestic law.*

Authors: Susan Perry (AUP)

Related modules: Privacy motivation, EU legal order

OVERVIEW:

International Human Rights Treaty Law provides the best framework to understand the legally binding obligations of the IT industry with respect to user privacy. Enshrined under article 12 in the 1945 UN Declaration of Human Rights, the right to privacy has been reinforced by article 17 of the International Covenant on Civil and Political Rights. Moreover, the Internet, the IT industry and users are bound by several other seminal rights, such as the right to be free of degrading treatment, the right to be free of discrimination, the right to freedom of expression, and the right to good health and to be free of environmental pollution caused by the hardware infrastructure necessary to make technology function. All of these rights form a legally binding matrix that is obligatory for the designer, the provider and the user of information technology.

LEARNING OBJECTIVES:

- Citizens should be aware of all of their rights with respect to information technology
- Technology designers and providers need to be aware of their binding obligations under domestic and international law

5.2 Policy Makers and Governmental and non Governmental Bodies acting for Human Rights Protection

The material prepared for the session "Data Protection and Law" of the Training Workshop is a first draft of the module "Basic Principles/Relevant Legislation". This first draft will be used as a basis for further elaboration according to the policy and legal stakeholders needs as identified in D4.1.

Legal and policy stakeholder				
Subject	Module	Mode of presentation	Content	Contributing partner
Data Privacy	Basic principles/ Relevant legislation	Slides + reading material	The module elaborates on the content of principle such as consent principle, data minimization (proportionality), and data quality, and its importance for the protection of the rights of the individual in the EU.	KU Leuven
Data Protection	Data protection reform		The module explains the reasons that triggered the data protection reform, analyses its content and discusses the major changes that are envisaged in the two proposals.	KU Leuven
PbD,: context	Part 1: How did the concept develop?		The module analyses how PbD developed in the EU and internationally. Of particular interest is the work of some European DPAs as well as of the EDPS that stressed the importance of the data minimization principle some time ago.	KU Leuven
	Part 1: How is PbD implemented in the draft regulation?		The module elaborates on how the draft regulation reinforces PbD.	KU Leuven
PbD,: design process	Part 1: Privacy risk management: data governance/ PIA/privacy risk management methodologies		The module discusses PbD within the general context of data governance.	KU Leuven
	Part 2: examples		Privacy by design in the field of cloud computing and biometric verification in border control. Each example follows a set four-part structure.	KU Leuven
	Part 3: How do legal principles affect policy making?		In this module privacy is perceived as a means to effective policy making. In the Commission Impact Assessment Guidelines (2009), privacy is a requirement that should be taken into account in the EU policymaking process.	KU Leuven

Table 6 – Educational Material for Policy Makers – Modules to be delivered in D4.3

6 Conclusions

D4.2 is composed by this document plus the collection of educational material available online which constitutes the initial version of the material for the general public and for the ICT-practitioners. It also covers the material needed for the training workshop (WP3).

We identify a set of challenges that will have to be addressed after the end of the project. First, the need to remove language barriers by translating the material in the languages of the EU. Second, the need to create a solid assessment method enabling to improve on what we are producing; in fact, although we will verify the efficacy of some of our material in a few contexts (training workshop, conference presentations) an evaluation methodology should be devised and quantitative and qualitative data should be collected and analysed to ensure a sustainable assessment of all material. Third, curricular sequences should be formed by aggregating several modules, and possibly integrating them with other educational material produced outside the project. Fourth, given the fast pace of evolution of the technologies that may represent a threat to privacy, a method for the adaptation of the knowledge tools should be devised in order to ensure its durability. Finally, while we currently make available the modules produced using a simple portal, a structure capable of making the information and educational material accessible and “life” in a sustainable manner should be planned for.

We hope that the material we have produced so far, together with that we will produce for D4.3, will provide a solid basis for the education of the stakeholders we have identified and will form the starting point for a growing set of tools for learning about PbD.