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

Deliverable D4.3

Final Educational Material

Due M24 - September

Project:	PRIPARE
Project Number:	ICT-610613
Deliverable:	D4.3
Title:	Final educational material
Version:	v0.1
Date:	30/9/2015
Confidentiality:	Public
Author:	Claudia Roda, Susan Perry, Jed Carty (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	Initial draft	10/1/2015
v0.2	First version of modules for students and general public	3/6/2015
v0.3	Final version of modules for students and general public	31/7/2015
v0.4	Introduction, conclusions	5/9/2015
v0.5	Final version of modules for policy makers and ICT-Practitioners	15/9/2015
v0.6	Final draft to partners for internal revision	20/9/2015
v1.0	Final	30/9/2015

Approval		
	Name	**Date**
Prepared	Claudia Roda (Ed.)	20/9/2015
Reviewed	All Project Partners	28/9/2015
Authorised	Antonio Kung	30/9/2015

Circulation	
Recipient	**Date of submission**
Project partners	30/9/2015
European Commission	30/9/2015

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

The deliverable is composed by this document and a set of knowledge tools (modules) available online. It includes all the educational material produced by partners during the project.

The knowledge tools are available at https://pripare.aup.edu/ and will be made available to the general public once approved by the project reviewers.

1 Introduction

This deliverable collects the educational material prepared by Pripare project partners. This material is designed to address the needs of a large set of stakeholders identified during the stakeholder analysis phase that took place at the beginning of the project and is described in Deliverable 4.1. Stakeholders include: the general public, ICT practitioners, Students, and policy makers. Previous deliverables have described how stakeholder needs have been identified and how we had planned to address these needs through the creation of educational and informational "modules" that could be organised into unit of teaching, seminars, workshops, dissemination sessions, etc. Modules address two possible level of knowledge that we have named "general" and "specific". Modules at the "general" level are normally introductory and don't require any specific previous knowledge about Privacy or Privacy by Design. Modules at the "specific" level explore in detail a subject related to Privacy by Design and may require some previous knowledge of the context they address. All modules have been prepared by experts in the subject being addressed but much attention has been paid, by project partners, that appropriate interdisciplinary links are highlighted. Modules addressing regulation, for example, frequently refer to privacy enhancing technologies, and vice versa, modules focused on technologies for privacy highlight their connections to regulatory issues.

1.1 Using Pripare educational material

The great majority of the modules we propose have been tested by the authors or other project partners in class, at seminars, workshops, etc. and the feedback we have received is very positive. Modules have been and can be used both as standalone and as part of a learning sequence composed of several modules.

Below are some examples of sequences that can be created by using the Pripare modules. Following the name of the module is a reference to the section of this document containing its description.

- A workshop for ICT practitioners
  - Module "Privacy Motivation and Introduction" - Section 4.19
  - Module "Privacy as a Human Right" – Section 4.20
  - Module "Basic Principles of European Data Protection and Privacy Law" – Section 5.1
  - Module "Privacy Enhancing Technologies" – Section 3.10
- A lecture sequence on Privacy by Design as part of a master level course on human rights
  - Module "Privacy Motivation and Introduction" - Section 4.19
  - Module "Privacy as a Human Right" – Section 4.20
  - Module "History of technology related to PbD" – Section 4.18
  - Module "EU regulation and privacy" – Section 4.21
- A lecture sequence on Privacy by Design as part of a master level course in law
  - Module "Basic Principles of European Data Protection and Privacy Law" – Section 5.1
  - Module "The Data protection reform" – Section 5.2 (part of this may be skipped

in case the audience already has legal or policy background)
    - Module “Privacy by Design - Context” – Section 5.3
    - Module “Privacy by Design and Risk Assessment” – Section 5.4
    - Module “How Do Legal Principles Affect Policy Making?” – Section 5.5
- A lecture sequence on Privacy by Design as part of an undergraduate course in computer science
    - Module “Understanding privacy” – Section 4.2
    - Module “Security vs. Privacy” – Section 4.7
    - Module “Privacy Enhancing Technologies and limitations” – Section 4.1
    - Module “Introduction to Secure Programming” – Section 4.4
    - Module “Secure and Privacy Preserving Software Engineering” – Section 4.5
    - Module “Cryptography” – Section 4.6
    - Module “Anonymisation” – Section 4.8
- A lecture sequence on Privacy by Design as part of an undergraduate course in business administration
    - Module “Privacy Motivation and Introduction” - Section 4.19
    - Module “Basic Principles of European Data Protection and Privacy Law” – Section 5.1
    - Module “Trust and Reputation” – Section 4.17
    - Module “Security management” – Section 4.12
    - Module “Privacy Impact Assessment” – Section 4.13
    - Module “Privacy Enhancing Technologies” – Section 3.10

1.2 Contents of the deliverable

The deliverable is organised in four parts each containing a description of the learning module for a different type of stakeholders. As shown in the examples above, although modules have been designed with a specific audience in mind, they can be used, in conjunction with other modules, to address the needs of a different type of audience.

The modules themselves are available online at https://pripare.aup.edu/

2 General Public Education Material

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

The booklet *Tools for Privacy Protection*, which is a combination of "tools for privacy protections" "smart use of smart devices" listed in D4.1, is included as part of D4.3 while the other modules were delivered with D4.2. The booklet is a reference tool for lay users that provides guidelines and information about practical actions that they may take to protect their privacy online.

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

The modules implemented 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, Tools for privacy protection booklet)

Below is a short description of each module available.

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: Employee protection of privacy in the workplace

Audience: Employees and their employers.

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 in Transportation Systems*

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 Tools for privacy protection

Title: *Tools for privacy protection*

Theme: General Public Education: Privacy Protection Tools

Audience: General Public

Presentation: Booklet

Level: General Knowledge

Available at: https://pripare.aup.edu/node/124

Summary: This booklet is a collection of simple privacy enhancing tips and tools suitable for members of the general public.

Authors: Jed Carty (AUP)

Related modules: All other general public material

Overview:

The use of technology in everyday life exposes the general public to a wide variety of opportunities for privacy violations. There are simple actions that can protect from many of these invasions. This module is a collection of tips and tools for protecting personal privacy.

Learning Objectives:

- Readers from the general public will be made aware of simple techniques and tools for protecting privacy in everyday life

2.11 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 organised as described in table 3. As compared to D4.2 the module "Privacy in transport systems" has been removed due to overlap with the module "Location Privacy". A separation into two modules would either have had a significant amount of overlapping or the module about privacy in transport systems would not have been easily understandable without the module about location privacy.

The modules in grey are included as part of D4.3. All other modules were delivered with D4.2.

ICT practitioners				
Subject	Module	Mode of presentation	Content	Contributing partner
PbD methodology PRIPARE	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	Privacy Strategies	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 in electric vehicle charging	Slides, exercises	We introduce the topic of location privacy using charging an electric vehicle to illustrate.	UULM
PET	Privacy Enhancing Technologies	Slides	PETs, what are they, examples of PETs, anonymous credentials.	Gradiant

Table 2 - ICT Practitioner Education Material

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 PRIPARE Methodology: Privacy Requirements Engineering

Title: *Privacy Requirements Engineering*

Theme: Privacy-by-design methodology

Audience: ICT Practitioners

Presentation: Slides

Level: Specific Knowledge

Available at: https://pripare.aup.edu/node/132

Summary: This module introduces a method to engineer privacy-friendly systems including the analysis and design stages. The module describes first the analysis stage, to move on to the architectural design and finally to the detailed design.

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

Related modules:

- PRIPARE: Principles and Concepts. It provides an overview of the main concepts regarding security- and privacy-by-design.
- PRIPARE: Methodology Overview. It introduces the PRIPARE methodology to develop privacy-friendly systems by design.

Overview:

The module introduces the following topics:

- **Privacy requirements operationalization:** Introduction to the privacy requirements operationalization method as a way to move from abstract privacy principles to detailed technical requirements.
- **Privacy-enhancing architectural design:** Introduction to 3 different approaches used within PRIPARE to define the architecture of a privacy-friendly system.
- **Privacy-enhancing detailed design:** Introduction to the method to move from detailed technical requirements to privacy-enhanced designs, with examples of application.

Essential Readings:

PRIPARE: Deliverable 1.2 – Privacy and Security by Design Methodology

Learning Objectives:

By following this module you will:

- understand how to move from abstract privacy principles to technical privacy requirements;

- know some approaches for privacy-enhancing architectural design; know an approach for privacy-enhancing detailed design.

Overview of Presentation:

Slide	*Title*	*Theme*
1	PRIPARE methodology	Session introduction
2	License	Terms of (re-)use of the material
3	Outline	Introduction to the topics of the session
4	Learning goals	Briefly introduction to the goals of the session
5-13	Privacy requirements operationalization	Introduction to the privacy requirements operationalization
14-20	Privacy-enhancing architectural design	Introduction to 3 different methods to draft a system architecture considering privacy requirements.
21-27	Privacy-enhancing detailed design	Presentation of a method to move from detailed technical requirements to a detailed design using a techniques catalogue.
28	Further reading material	Comments on useful documents

3.4 PRIPARE Methodology: PIA and Risk Analysis

Title: *PIA and Risk Analysis*

Theme: Privacy-by-design methodology

Audience: ICT Practitioners

Presentation: Slides

Level: Specific knowledge

Available at: https://pripare.aup.edu/node/133

Summary: This module describes some of the recommended best practices for developing privacy-friendly systems by following a privacy- and security-by-design methodology, namely, privacy impact assessment and privacy risk analysis. The module deals first with privacy impact assessment by describing its steps, and then moves on to privacy risk analysis introducing different approaches such as CNIL and LINDDUN proposals.

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

Related modules:

- PRIPARE: Principles and Concepts. It provides an overview of the main concepts regarding security- and privacy-by-design.
- PRIPARE: Methodology Overview. It introduces the PRIPARE methodology to develop privacy-friendly systems by design.

Overview:

The module introduces the following topics:

- **Privacy impact assessment**: Introduction to this best practices in the privacy domain
- **Privacy risk management:** Introduction to the risk management process, and description of its application to the privacy domain.

Essential Readings:

- PRIPARE: Deliverable 1.2 – Privacy and Security-by-design Methodology

Learning Objectives:

By following this module you will:

- gain an understanding of the concepts and terms related to Privacy Impact Assessment and Risk Management;
- be aware of the benefits of carrying out a Privacy Impact Assessment in the development of a software product or service.

3.5 PRIPARE Methodology: Best Practices

Title: *Best Practices*

Theme: Privacy-by-design methodology

Audience: ICT Practitioners

Presentation: Slides

Level: Specific knowledge

Available at: https://pripare.aup.edu/node/134

Summary: This module introduces the recommended best practices for developing privacy-friendly systems by following a privacy- and security-by-design methodology. The module introduces best practices in general, to move on to the best privacy practices identified by the community including privacy risk management, privacy impact assessment, and privacy patterns. Then it details the properties of a privacy pattern and introduces the privacy pattern catalogue developed by the PRIPARE project, describing some of the available patterns.

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

Related modules:

- PRIPARE: Principles and Concepts. It provides an overview of the main concepts regarding security- and privacy-by-design.
- PRIPARE: Methodology Overview. It introduces the PRIPARE methodology to develop privacy-friendly systems by design.
- Privacy impact assessment and risk analysis. It details these best privacy practices

Overview:

The module introduces the following topics:

- **Best privacy practices**: Introduction to the best practices in the privacy domain
  - Privacy Risk Management
  - Privacy Impact Assessment
  - Privacy Patterns
  - Privacy Anti-Patterns
- **Privacy patterns catalogue:** Introduction to the catalogue of privacy patterns developed by the PRIPARE project.

Essential Readings:

- PRIPARE: Deliverable 2.1 – Best Practice Template
- PRIPARE: Deliverable 2.2 – Best Practice Examples
- PRIPARE: Deliverable 2.4 - Guidelines for Best Practice Templates

Learning Objectives:

By following this module you will:

- understand what a best practice is for the development of privacy-friendly systems and services;
- know some best privacy practices and when to use them;
- know how to find, select and use more best practices.

3.6 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

3.7 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.

3.8 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.

3.9 Location Privacy in Electric Vehicle Charging

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.

3.10 Privacy Enhancing Technologies

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 Students

The modules presented in this section are focused on students, both CS and engineering students as well as non-technical students, as an introduction to the concepts of PbD and privacy in the context of technology. The modules available are listed in Table 5.

As compared to D4.2 the section “Privacy enhancing techniques for Web Services” has been combined with the section “Privacy in the Internet of Things” because of the overlapping subject matter. Similarly, the section “Web security and vulnerabilities” was removed due to overalap with the section “Web and database security and vulnerabilities”. The section “PbD: perspectives and limitations” was removed in favour of the section “Privacy Enhancing Technologies and limitations”.

In order to address the needs of the PRIPARE training workshop the module addressing the history of human rights treaties relevant to privacy and the module on “Principles and processes of PbD” were delivered earlier as part of D4.2.

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
	Introduction to Secure programming		Technical description of how security and privacy related techniques are considered in programming practices.	WIT
	Secure and privacy preserving 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
	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	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 and security 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 and 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

Table 5 - Educational Material for Students

4.1 Privacy Enhancing Technologies and Limitations

Title: *Privacy Enhancing Technologies and Limitations*

Theme: Privacy Enhancing Technologies

Audience: Undergraduate non-CS students

Presentation: Reading list

Level: Specific Knowledge

Available at: https://pripare.aup.edu/node/144

Summary: Description of privacy preserving technologies including their capabilities and limitations. The reading list includes non-technical resources for students to understand the role of PETs in protecting privacy of individuals.

Authors: Hisain Elshaafi (WIT)

Related modules:

- Anonymisation
- Cryptography

Overview:

Privacy enhancing technologies (PETs) refer to computer tools, applications and mechanisms which when integrated in online services or applications allow online users to protect their privacy including personally identifiable information (PII). The protection may take one or more forms such as providing control to users, ensuring anonymity, unlinkability, auditing, etc. The reading list aims to provide some non-technical or light technical resources for non-CS students to help them gain a good understanding of what PETs are, some tool examples, how they function in general and what their role in protecting privacy of individuals. The list will cover other aspects such as the economic aspects of using PETs. The referenced material also discusses limitations of PETs including hindrances to wide-spread adoption.

Learning Objectives:

- Gain understanding of non-technical functional aspects of PETs.
- Gain understanding of the role of PETs in protecting privacy.

4.2 Understanding Privacy

Title: *Understanding Privacy*

Theme: Privacy in ICT environments

Audience: Undergraduate CS students

Presentation: reading list

Level: specific knowledge

Available at: https://pripare.aup.edu/node/145

Summary: The reading list helps students understand the basic concepts of privacy and privacy enhancing technologies. The list includes a mix of high level discussions of privacy related topics as well as more in-depth analysis of research in the area of privacy.

Authors: Hisain Elshaafi

Related modules:

- Privacy Enhancing Technologies and limitations
- Security vs. Privacy

Overview:

As technologies develop, conceptualizations of privacy have developed alongside them to capture the complexity of privacy issues within frameworks that highlight the social, economic or political concerns caused by the technologies. The module provides reading resources that help students understand the basic concepts of privacy and privacy enhancing technologies. The list includes a mix of high level discussions of privacy related topics as well as more in-depth analysis of research in the area of privacy.

Learning Objectives:

- Students understand principles and main concepts related to privacy and privacy protection.

4.3 Privacy in the Internet of Things

Title: *Privacy in the Internet of Things*

Theme: Privacy in ICT environments

Audience: Undergraduate and postgraduate CS and engineering students

Presentation: Slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/146

Summary: These slides introduce the Internet of Things (IOT) and discuss the privacy concerns that arise from a ubiquitous network of smart devices.

Authors: Jed Carty (AUP)

Related modules:

- Privacy Enhancing Technologies
- Security and Privacy Patterns

Overview:

New advances in both smart devices and connectivity are leading to a future where everything from cars to coffee pots will be part of a global network. This will create novel privacy concerns that must be addressed in the basic design of the network. The module will help students understand the potential presented by the IOT as well as the possible privacy invasions caused by an omnipresent network.

Essential Readings:

- "Is the Internet of things really the internet of sensors?" http://www.enterprisetech.com/2015/05/08/is-the-iot-really-internet-of-sensors/
- "What does IOT big data mean to you?" http://www.ecnmag.com/blog/2015/04/what-does-iot-big-data-mean-you
- "FTC urges IOT privacy, security-by-design at consumer electronics show" https://threatpost.com/ftc-urges-iot-privacy-security-by-design-at-consumer-electronics-show/110265/

Learning Objectives:

- Students are introduced to the concept of the internet of things
- Students understand the privacy challenges presented by the internet of things

4.4 Introduction to Secure Programming

Title: *Introduction to Secure Programming*

Theme: Security relationship to privacy

Audience: Undergraduate CS students

Presentation: slides, exercises

Level: specific knowledge

Available at: https://pripare.aup.edu/node/148

Summary: The slides and exercises aim to best practices in secure coding and programming of applications. The also describe risks from insecure programming and methods of addressing common vulnerabilities and risks.

Authors: Jimmy McGibney and Hisain Elshaafi (WIT)

Related modules:

- Secure and privacy preserving software engineering
- Security and privacy patterns
- Web security and vulnerabilities

Overview:

A program that can be executed on a machine may have all the rights and privileges of the user who is (directly or indirectly) executing it including deleting or disclosing sensitive files. Secure programming aims to minimise accidental flaws in code, so that it only does what it's meant to do. It also restricts the ability to run code on a system, where the code has the potential to do damage. Insecure and poor programming practices can take many forms such as lack of appropriate validation of data input/output, insecure encryption algorithms, or inadequate security testing. The module covers those issues and aims to prepare CS students to face security challenges in developing and providing quality assured software.

Essential Readings:

Secure Coding: Principles & Practices, M. Graff & K. van Wyk, O'Reilly, 2003.

Software Security: Building Security In, G. McGraw, Addison-Wesley, 2006.

Learning Objectives:

- Students appreciate risks from bad and insecure programming practices.

Students learn common methods in securely programming applications.

4.5 Secure and Privacy Preserving Software Engineering

Title: *Secure and Privacy Preserving Software Engineering*

Theme: Security relationship to privacy

Audience: Undergraduate and postgraduate CS students

Presentation: slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/149

Summary: The slides describe issues around addressing security and privacy during the development of software from early stages to installation and operation. They describe the principles and best practices that need to be followed in software engineering and the methods required to apply security and privacy based on requirements and use cases.

Authors: Jimmy McGibney and Hisain Elshaafi (WIT)

Related modules:

- Security vs. privacy
- Secure programming
- Security and privacy patterns

Overview:

Traditionally, software development and security/privacy functions haven't overlapped substantially as features are considered more important than security. However, there is a growing acceptance now of need to build security and privacy into the entire software development process (often called Security and Privacy by Design). The module provides an overview of addressing security and privacy in the whole software development lifecycle (SDLC) from requirements to deployment and maintenance operations. A range of issues are covered such as security and privacy use/misuse cases, design patterns and vulnerability testing.

Essential Readings:

Software Security: Building Security In, G. McGraw, Addison-Wesley, 2006

Learning Objectives:

- Students gain understanding of the techniques for addressing security and privacy in the stages of software development life cycle.
- Students understand the use of general and specific (for privacy and security) modelling approaches in engineering secure software.

4.6 Cryptography

Title: *Cryptography*

Theme: Security relationship to privacy

Audience: Undergraduate CS students

Presentation: slides and exercises

Level: specific knowledge

Available at: https://pripare.aup.edu/node/151

Summary: The material provides a discussion of cryptography types, algorithms and techniques including symmetric encryption, public key cryptography and message digests (hash functions). It also outlines public key management, certificates, trust models and attacks against encryption.

Authors: Jimmy McGibney, Hisain Elshaafi (WIT)

Overview:

Cryptography protects information by transforming it into an illegible format, called cipher text. Only those who own a secret *key* can decipher the data into plain text. Encrypted messages can sometimes be broken by cryptanalysis, although modern cryptography techniques are virtually unbreakable. This module discusses cryptographic methods both symmetric and asymmetric and details some of the common algorithms. Limitations and strengths of those algorithms are also described. The module describes also security applications of the different algorithms, management of keys and certificates. Finally, the module discusses trust models including direct trust, hierarchical trust and web of trust. The exercises cover Openssl; an open source cryptographic toolkit that implements SSL/TLS, and PGP; a privacy, confidentiality and authentication service using encryption and decryption that can be used for storage and messaging applications.

Learning Objectives:

- Gain understanding of the fundamental ingredients of most security protocols & products; symmetric Encryption, public key cryptography and message digests
- Gain understanding of public key management, certificates, trust models, etc.

4.7 Security vs. Privacy

Title: *Security vs. Privacy*

Theme: Security relationship to privacy

Audience: Undergraduate CS students

Presentation: slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/152

Summary: Security and privacy concepts overlap, yet they are different. Security techniques can help support privacy. On the other hand, enforcing some forms of security can violate privacy.

Authors: Hisain Elshaafi (WIT)

Related modules:

- Privacy Enhancing Technologies and limitations,
- Understanding privacy

Overview:

There is often confusion between the concepts of security and privacy. For example, confidentiality is often confused with privacy. The slides aim to help students understand the meaning of security and privacy, some of the main related concepts and the lines of difference between the two. The slides describe examples of how security can enhance privacy or sometimes breach privacy.

Learning Objectives:

- Students understand the difference and the relationship between security and privacy

4.8 Anonymisation

Title: *Anonymisation*

Theme: Privacy in ICT environments

Audience: Undergraduate and postgraduate CS students

Presentation: Reading list

Level: General knowledge

Available at: https://pripare.aup.edu/node/153

Summary:

This reading list aims to provide some pointers to useful material on anonymisation techniques and mechanisms.

Authors: Hisain Elshaafi (WIT)

Overview:

Anonymisation involves encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous. Anonymisation is not always safe; attacks that compromise anonymisation techniques can reveal protected information in released datasets.

Learning Objectives:

- Learning the basics of anonymisation techniques and their vulnerabilities

4.9 Security and Privacy Patterns

Title: *Security and Privacy Patterns*

Theme: Security relationship to privacy

Audience: Undergraduate and postgraduate CS students

Presentation: Slides

Level: Specific Knowledge

Available at: https://pripare.aup.edu/node/154

Summary: The slides provide an overview of privacy and security patterns, their structure and common characteristics as well as issues on incorporating those patterns into secure and privacy preserving design. Other issues discussed include consideration of implications of applying general software design patterns on privacy and security.

Authors: Hisain Elshaafi (WIT)

Related modules:

- Clould Privacy Patterns and Best Practices

Overview:

The module introduces software design patterns focused on ensuring security and privacy in developed software. The module provides examples of such patterns and covers a number of related issues such as the common structure and characteristics of patterns. In addition to patterns that are developed to support privacy and security, there are design patterns that influence privacy and security of the software being built. Therefore, one of the considerations in pattern selection and implementation is the trade-off between various options that ensuring adhering to the client requirements and addressing regulatory and other constraints.

Essential Readings:

Gamma, Erich, Richard Helm, Ralph Johnson, and John Vlissides. Design patterns: elements of reusable object-oriented software. Pearson Education, 1994.

Learning Objectives:

- Students become familiar with the concept and structure of patterns particularly in the fields of security and privacy.
- Students appreciate potential role of patterns in preserving privacy and the need for further development of the area of privacy patterns.

4.10 Web and Database Security and Vulnerabilities

Title: *Web and Database Security and Vulnerabilities*

Theme: Database Privacy

Audience: Undergraduate CS students

Presentation: slides, exercises

Level: specific knowledge

Available at: https://pripare.aup.edu/node/156

Summary: The learning material aims to help students learn about privacy and security in Web applications as well as databases. The slides discuss common protection mechanisms of web applications and databases. They also describe common risks and threats. The objectives of the exercises are to get some understanding of digital certificates and to configure TLS (a.k.a.

SSL) on a web server.

Authors: Jimmy McGibney, Hisain Elshaafi (WIT)

Related modules:

- Secure programming
- Security and privacy in software engineering

Overview:

Security and privacy of Web applications and connected databases are fundamental issues that need to be considered during the development, installation and operation of such systems. However, security and privacy cannot be implemented using one or even few measures and mechanisms. There need to be a range of considerations at various levels from analysis of client's requirements from security and privacy perspective to ensuring proper handling of customer data by software systems during storage as well as communications. The slides and exercises aim to challenge students to learn how they can take part in such processes through understanding privacy and security risks and the countermeasures that need to be followed proactively or in response to incidents. Additional considerations are also needed such as the impact of security mechanisms on performance and scalability.

Essential Readings:

Web Application Security, A Beginner's Guide, B. Sullivan, & V. Liu, McGraw-Hill, 2012.

Learning Objectives:

- Students gain understanding of best practices and a number of mechanisms in relation to database and Web security and privacy.
- Students learn about common threats and risks in Web applications and databases.

4.11 Privacy Preserving Data Management

Title:	*Privacy Preserving Data Management*
Theme:	Database Privacy
Audience:	Undergraduate and postgraduate CS students
Presentation:	Reading list
Level:	Specific knowledge
Available at:	https://pripare.aup.edu/node/157

Summary: This reading list aims to provide some pointers to useful material on the principles of privacy preserving data management such as data collection, processing, storage and mining.

Authors: Hisain Elshaafi (WIT)

Related modules:

- Anonymisation

Overview:

The collection, processing, analyzing and exchange of data between different parties including governments, enterprises, communities and individuals creates tremendous opportunities in knowledge sharing and decision making. However, without developing and using privacy preserving techniques they will allow complete loss of privacy. Although a lot of research has been done to support preserving privacy in data management, there is still a long way to go before accomplishing the research goal. The reading list provides some of the useful material on the related concepts, challenges and the latest technologies towards achieving privacy preserving data management.

Learning Objectives:

- Recognize the challenges to privacy protection in data management tasks.
- Understanding some of the techniques for preserving privacy in data management topics.

4.12 Security Management

Title:	*Security Management*
Theme:	PbD Privacy risks and incidents
Audience:	Undergraduate and postgraduate CS students
Presentation:	Slides
Level:	Specific Knowledge
Available at:	https://pripare.aup.edu/node/158

Summary: The slides provide an overview of some of the main topics related to security management in an organization. Topics covered include security and privacy basics, security governance, risk management, threat modelling and privacy risks.

Authors: Hisain Elshaafi, Jimmy McGibney (WIT)

Related modules:

- Compliance Reviews
- PIA
- Trust and Reputation

Overview:

The learning material introduces to students the basic concepts of security and privacy. It then provides discussions of topics that are related to managing security in an organisation. Security management involves ensuring the confidentiality, integrity and availability of an organization's assets, data and IT services. Security Governance is the organizational strategy for managing risk that includes processes, policies, procedures, standards, guidelines and baselines. The development and sustainment of security governance may involve conducting threat, vulnerability and risk analyses based on the specific industry or the organisation.

Part of the security management processes is risk management. Risk Management is periodic but continuous process that involves identifying, evaluating, and mitigating risk to an organization. The slides discuss issues related to risk management such as common security and privacy risks, protection from those risks, risk analysis, quantifying and dealing with risks. Other topics covered in the slides are security assessment, security design, business continuity, incident response, threat modelling and best practices.

Learning Objectives:

- Students learn about a range of topics related to organizational security management.
- Students gain understanding of the procedure of risk management and understand common technical risks in an organization.

4.13 Privacy Impact Assessment (PIA)

Title: *Privacy Impact Assessment*

Theme: PbD Privacy risks and incidents

Audience: Undergraduate and postgraduate CS and Non-CS students

Presentation: Reading list

Level: Specific knowledge

Available at: https://pripare.aup.edu/node/159

Summary:

This reading list aims to provide some pointers to useful material on Privacy Impact Assessments (PIAs). The material will provide understanding of the PIA process and the parameters that need to be taken into consideration when carrying out the assessment.

Authors: Hisain Elshaafi (WIT)

Related modules:

- Security Management
- Compliance Reviews

Overview:

Privacy Impact Assessments (PIAs) form an important part when following a privacy by design approach in a project. PIA is a tool that can be used to identify and reduce privacy risks of projects. PIAs involve some parameters or criteria that determine the extent and depth of the risk management process. The reading list aims to provide students with basic understanding of these issues and allow them gain more detailed understanding as needed. OWASP privacy risks provide students with important examples of privacy risks that should be considered during PIAs.

Learning Objectives:

- Gain understanding of the PIA process and how PIA should be performed considering various project types.
- Appreciate some of the privacy risks that could be considered during PIA.

4.14 Compliance Reviews

Title:	*Compliance Reviews*
Theme:	Incorporating privacy by design Privacy risks and incidents
Audience:	Undergraduate and postgraduate CS students
Presentation:	Reading list
Level:	Specific knowledge
Available at:	https://pripare.aup.edu/node/160

Summary:

This reading list aims to provide some pointers to useful material on carrying out compliance reviews in relation to security and privacy.

Authors: Hisain Elshaafi (WIT)

Related modules:

- Security management

Overview:

A security compliance review or audit is a comprehensive review of an organisation's adherence to regulatory guidelines. Security or IT consultants evaluate the strength and thoroughness of compliance preparations. Auditors review security polices, access controls and risk management procedures depending on the type of organisation.

Learning Objectives:

- Understanding the principles of security and privacy reviews and auditing.
- Gaining skills related to reviewing code and testing software in relation to security and privacy.

4.15 Cloud Privacy and Security Patterns and Best Practices

Title: *Cloud Privacy and Security Patterns and Best Practices*

Theme: Cloud privacy

Audience: Undergraduate CS students

Presentation: slides

Level: specific knowledge

Available at: https://pripare.aup.edu/node/161

Summary: The slides describe some of the known patterns and best practices most relevant to security and privacy preserving the cloud environments for cloud providers and customers. The slides also describe the characteristics of best practices and common categories privacy guidelines.

Authors: Hisain Elshaafi (WIT)

Related modules: Security and privacy patterns

Overview:

One of the emerging technology areas is cloud computing which has not been adopted fully due in part to security and privacy concerns. Addressing security and privacy issues using patterns and best practices is an important step that gives peace of mind to the providers and confidence to their consumers. The module first introduces patterns and best practices and then outlines characteristics of useful best practices. The description of some of the useful patterns and best practices that add security and privacy preserving features will provide students some important knowledge relevant to a common field of practice of their skills. Further reading resources that are listed will help students gain more detailed understanding of the listed best practices.

Learning Objectives:

- Appreciation of the need for privacy and security patterns in the field of cloud computing.
- Understanding of some known technical privacy best practices and patterns that can be applied to the cloud technologies.

4.16 Privacy Issues in Mobile Devices

Title: *Privacy Issues in Mobile Devices*

Theme: Mobile Privacy

Audience: Undergraduate CS students

Presentation: Reading list

Level: Specific knowledge

Available at: https://pripare.aup.edu/node/162

Summary:

This reading list aims to provide some pointers to useful material on privacy problems linked to mobile devices and applications as well as techniques and mechanisms to address some of those problems. The list includes privacy issues associated with usage mobile applications in healthcare (mHealth).

Authors: Hisain Elshaafi (WIT)

Overview:

Mobile devices and applications offer a wealth of features that can improve people's quality of life. However, those features can also result in degradation or loss of personal privacy particularly due to their continuous and multifaceted usage and the lack of appropriate privacy protections. The reading list selects few resources that help students understand the main privacy problems related to mobile devices, benefits of applications to users that need to be balanced with the concerns, and privacy preserving countermeasures. The material also aims to help student appreciate the existing challenges in addressing the problems and the weaknesses of the current solutions that aim to preserve privacy of mobile users.

Learning Objectives:

- Gain understanding of various privacy problems related to usage of mobile devices and applications and some of the possible solutions.

4.17 Trust and Reputation

Title:	*Trust and Reputation*
Theme:	Economic aspects
Audience:	Undergraduate and postgraduate CS students
Presentation:	Slides
Level:	Specific knowledge
Available at:	https://pripare.aup.edu/node/163

Summary: this material describes the concepts of trust, trustworthiness and reputation. It outlines the dimensions and attributes that affect trust of organisations. It also outlines the effect of privacy and security on trustworthiness, threats against trust and the aggregation of trust in service oriented computing.

Authors: Hisain Elshaafi, Jimmy McGibney and Dmiri Botvich (WIT)

Overview:

The concept of trust is multidimensional. Organisations aim to optimize their trustworthiness and reputation. Privacy and security are among the important dimensions that contribute to the aggregated level of organizational trustworthiness. The module aims to describe a variety of issues that are related to trust and understanding of its meaning as well as the relationship to privacy and security.

Essential Readings:

- H. Elshaafi, Establishment and maintenance of trustworthy composite services using multidimensional service attributes, PhD thesis, Waterford Institute of Technology, 2014

Learning Objectives:

- The module's objective is allow students to understand the role of privacy in organizational and service trustworthiness and how maintaining their customers' privacy and security can help establish and maintain their trust towards the organization.

4.18 History of Technology Related to PbD

Title: *History of Technology Related to PbD*

Theme: How Privacy issues have evolved with the evolution of technology

Audience: Students

Presentation: Slides

Level: General knowledge

Available at: https://pripare.aup.edu/node/164

Summary: This module follows the main development of information technology, roughly from the second half of the XX century to current days

Authors: Claudia Roda (AUP)

Related modules: Privacy motivation and introduction

Overview: While our understanding of privacy has evolved outside the information technology context, some important aspects of our current understanding of privacy are intrinsically related to these technologies. This module explores the evolution of information technology from the 1940 to current days and highlights the privacy issues that have developed in such context.

Essential Readings:

Jan Holvast (2007) History of Privacy - in Karl de Leeuw and Jan Bergstra (Eds), The History of Information Security: A Comprehensive Handbook. Elsevier: 2007

Computer and Information Ethics - Stanford Encyclopedia of Philosophy – Revision October 23 2008 - http://plato.stanford.edu/entries/ethics-computer/

Terrell Ward Bynum (2000) A very short history of computer ethics http://www.cs.utexas.edu/~ear/cs349/Bynum_Short_History.html

Learning Objectives:

- Students gain a n understanding of the major milestones in the development of digital information and communication technologies
- Students are able to relate these milestones to privacy threats and privacy preserving technologies

4.19 Privacy Motivation and Introduction

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

4.20 Privacy as a Human Right

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

4.21 EU Regulation and Privacy

Title:	*EU Regulation and Privacy*
Theme:	Implementing privacy as a human right in Europe
Audience:	University students and general public
Presentation:	Ten slides, with commentary
Level:	University students in law, information technology, public policy, and the social sciences more generally, as well as the general, news-reading, adult public
Available at:	https://pripare.aup.edu/node/167

Summary: European citizens are impacted by privacy violations that occur in a digital environment. This module explains in general terms the European Union's preparations to implement stricter privacy protections by 2017.

Authors: Susan Perry **(**AUP)

Related modules: This module is a general overview of the KUL module on the EU Legal Order.

Overview: Privacy protection is essential if all EU citizens are to benefit from the Big Data economy, a sector that will be worth an estimated 3 trillion euros by 2020. This module presents an outline of the new EU regulations and the challenges that such human rights protection poses for European citizens. We conclude with a set of recommendations to embed privacy-by-design initiatives at the heart of EU data protection implementation.

Essential Readings:

Boyle, J. (2008). *The Public Domain: Enclosing the Commons of the Mind*. New Haven : Yale University Press ; Hoeren, T. (2014). Big Data and the Ownership in Data : Recent Developments in Europe, *European Intellectual Property Review*, Issue 12, pp. 751-754 ; Lessig, L. (2004). *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: Penguin. Commission Nationale de l'Informatique et des Libertés (CNIL). (2012) *Vie privée à l'horizon 2020: paroles d'experts*, Cahier Innovation & Prospective, N° 1; Rochelandet, F. (2010). *Économie des données personnelles et de la vie privée.* Paris: Éd. La Découverte, coll. Repères.

Learning Objectives:

- Participants will understand how privacy as a human right is translated into legal regulation and protection.

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

The modules presented in this section are focused on policy makers in the EU. The modules introduce privacy-by-design concepts in the context of EU policy.

Section 5.1 introduces data privacy in the European Data Protection and Privacy law and section 5.2 explains the reasons for the data protection reform.

Section 5.3 introduces the concept of Privacy by Design in two parts. The section departs from the origin of the principle and illustrates that Privacy by Design, as a concept deriving from the field of engineering, entered the European fora in the context of the discussions around Privacy Enhancing Technologies (Part 1). It further continues with its development in the European debates, including its introduction in the draft General Data Protection Regulation (Part 2). Since origin and development logically follow each other, we have organised the two topics as parts of the same section rather than treating them as separate ones. This gives the opportunity for discussing critically its evolution in the European legal order.

Section 5.4 introduces processes that are related to the implementation of Privacy by Design which consists of 3 parts. We have organised the three parts in one unit as they introduce processes that foster the implementation of Privacy by Design and refer to either technology or policy design. With regards to technology design we introduce the notions of risk assessment and Privacy Impact Assessment. We present Privacy Impact Assessment as a way to assess the impact of technologies on fundamental rights to privacy (Part 1) and exemplify that with two case studies: cloud computing and biometric processing (Part 2). With regards to policy design we illustrate that privacy should be taken into account at every stage of policy making. An important tool to that end is the policy impact assessments (Part 3).

Legal and policy stakeholder				
Subject	Module	Mode of presentation	Content	Contributing partner
Data Privacy	Basic principles on European Data Protection and Privacy Law	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	The 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	Privacy by Design - Context		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	KU Leuven

			the EDPS that stressed the importance of the data minimization principle some time ago.	
PbD,: design process	Part 1 and 2: Privacy by Design and risk assessment, examples		The module discusses PbD within the general context of data governance. 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

5.1 Basic principles of European Data Protection and Privacy Law

Title: *Basic principles of European Data Protection and Privacy Law*

Theme: Basic principles/Relevant Legislation

Audience: stakeholders with a legal background

Presentation: Slides

Level: Basic knowledge

Available at: https://pripare.aup.edu/node/169

Summary: Departing of basic notions of the European Privacy and Data Protection legal framework, this module introduces the principles laid down in the Data Protection Directive 46/1995/EC as well as relevant practical examples.

Authors: Pagona Tsormpatzoudi and Fanny Coudert

Related modules:

1 module, as descried above

Essential Readings:

- 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, 23.11.1995, p. 31–50*
- 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)
- Fundamental Rights Agency 'Handbook on Data Protection Law' (Publications Office of the European Union, Luxembourg 2014)

Learning Objectives:

- This module is addressed to audiences with legal or policy background that have no previous experience with privacy and data protection law. The aim of this module is that the attendees are able at the end of the presentation to identify in high level potential challenges that technologies pose to individuals' privacy and data protection.

5.2 The Data Protection Reform

Title: *The Data Protection Reform*

Theme: The Data Protection Reform

Audience: Stakeholders with very little knowledge on European law, data protection and privacy law

Presentation: Slides

Level: Basic Knowledge

Available at: https://pripare.aup.edu/node/170

Summary: This section introduces an introduction to the sources of European Law. The Data Protection Reform is presented in this context.

Authors: Pagona Tsormpatzoudi and Fanny Coudert (KU Leuven)

Essential Readings:

- European Commission. "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 4.11.2010 COM." 2010.

Learning Objectives:

- The learning objective of this module is to provide basic knowledge on European law as well as an understanding of the main motivations and expected outcomes of the data protection reform.

5.3 Privacy by Design - Context

Title: *Privacy by Design - Context*

Theme: Privacy by Design

Audience: Stakeholders with knowledge on data protection law

Presentation: Slides

Level: Advanced Knowledge

Available at: https://pripare.aup.edu/node/171

Summary: This section introduces the origins and development of the principle 'Privacy/data Protection by Design in Europe. Departing from the idea that Privacy by Design is a concept underlying in the existing legal framework, it has been made explicit in order to foster its implementation. It further tries to convey the message that Privacy by Design has been growing from a concept referring to technical and organisational measures to measures that affect the whole ecosystem around data processing. The module consists of two parts: Part 1: How did the concept develop? And Part 2: How is the concept implemented in the draft regulation?

Authors: Pagona Tsormpatzoudi and Fanny Coudert (KU Leuven)

Related modules:

Essential Readings:

- Recital 61 and Article 23 of the draft Regulation – Recommended to comparatively study the first draft of the proposed General Data Protection Regulation and subsequent proposed amendments by the European Parliament and the Council.

Learning Objectives:

- The learning objective for the audience is at the end of the lecture to be able to explain the origin, logic and content of Privacy/Data Protection by Design and critically discuss its introduction in the draft Regulation.

5.4 Privacy by Design and Risk Assessment

Title: *Privacy by Design and Risk Assessment*

Theme: Privacy-by-Design

Audience: Stakeholders with knowledge on privacy and data protection law

Presentation: Slides

Level: Advanced Knowledge

Available at: https://pripare.aup.edu/node/173

Summary: This section presents the concept of Privacy Impact Assessment as a risk assessment methodology and a way to implement Privacy by Design in line with its introduction in the draft General Data Protection Regulation. The module discusses two cases studies (cloud computing and biometric processing for border control) in order to exemplify main elements of Privacy Impact Assessment and concludes that PIA constitutes an appropriate way to handle from a legal perspective privacy and data protection risks. The module consists of 3 parts, two of which are included in the section: Part 1: Privacy Impact Assessment: A way to assess impact on fundamental rights and Part 2: Case studies.

Authors: Pagona Tsormpatzoudi **(**KU Leuven)

Related modules:

Essential Readings:

- Article 33 of the draft Regulation, Council of the European Union. "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) 15395/14 2012/0011 (COD), Brussels, 19 December 2014.

Learning Objectives:

- The learning objective of the module is to provide an introduction to the notion of PIA as well as the way it has been introduced in the draft Regulation. Further, it is expected that the attendees at the end of the class will be able follow legal reasoning in a systematic way based on the main elements of Privacy Impact Assessment.

5.5 How Do Legal Principles Affect Policy Making?

Title: *How Do Legal Principles Affect Policy Making?*

Theme: Privacy by Design - process

Audience: Stakeholders with legal or policy background and knowledge of privacy and data protection law (policy makers)

Presentation: Slides

Level: Advanced Knowledge

Available at: https://pripare.aup.edu/node/175

Summary: This section introduces privacy by design as a concept to be taken into account in policy making processes. It illustrates that impact assessments that policy makers conduct before initiating law making processes should systematically consider privacy and data protection. The case of the European anti-money laundering legal framework is used as an example. The module corresponds to Part 3 of section 5.4.

Authors: Pagona Tsormpatzoudi **(**KU Leuven)

Related modules:

Essential Readings:

- European Commission. "Impact Assessement - Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, incl. terrorist financing SWD(2013) 21." Commission Staff Working Document, Strassbourg, 2013.
- European Commission. "Impact Assessment Guidelines SEC(2009) 92." 2009.

Learning Objectives:

- The learning objective of this module is to illustrate the importance to consider privacy and data protection in policy making and in particular in policy impact assessments.

6 Conclusions

This document, together with the collection of the educational material available online, achieve the objectives that we had set out to pursue within this work-package at the beginning of the project. The formal[1] and informal feedback we have received about the modules has helped us fine tune them and encourages us that they will form a solid basis for continuing the development of knowledge tools supporting a risk management culture and the widespread application of Privacy by Design concepts, techniques and methodologies.

As already mentioned in deliverable 4.2 we believe that the adoption, development and effectiveness of these knowledge tools could be further strengthened by providing translations in several languages so to remove language barriers. Given the fast pace of evolution of the technologies that may represent a threat to privacy, a method for the adaptation of the modules should be devised in order to ensure their 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.

[1] Please see Deliverable 3.2 for a report on the feedback received about the modules used during the Privacy by Design workshop for selected FP7 projects.