



 **PRIPARE**

**PR**eparing Industry to **PR**ivacy-by-design by  
supporting its **AP**plication in **RE**search

# Privacy by Design

A legal perspective

Pagona Tsormpatzoudi

Katholieke Universiteit Leuven





# The goal

---

## Privacy by Design as a way to foster implementation of the data protection legal framework





# Initial approach to Privacy by Design – through technology

---

In 1995: “Privacy Enhancing Technologies: The path to anonymity”

## Privacy Enhancing Technologies:

a coherent system of ICT measures that **protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data**, all without losing functionality of the information systems (European Commission, 2007)





# Privacy by Design – through technical and organisational measures

---

## *Enforcing law through technical and organisational measures*

- Dutch Data Protection Authority: PETs should be combined with privacy management tools (informational tools to create awareness, creation of policies, compliance checks)
- Data Protection Directive 95/46/EC (legal basis):
  - Data minimisation (Article 6.1 (b) & (c))
  - Obligation to security (Article 17 & Recital 61)





# Privacy by Design in the data protection reform

## *Preparatory work of the data protection reform*

*'Users of ICT services are not in a position to take relevant security measures by themselves in order to protect their own or other persons' personal data.' (Art. 29 WP, 2009 )*

*"...a more positive solution is to design and develop ICT in a way that respects privacy and data protection.."  
(EDPS,2010)*

**Need** to provide for the principle of "privacy by design" into the data protection legal framework in different ways:

- As a general principle
- With provisions in specific legal instruments
- As a guiding principle of the Digital Agenda for Europe
- In Other EU initiatives (EDPS,2010)





# Privacy by Design during the data processing lifecycle

---

## *From Privacy by Design to Data Protection by Design: The draft general data protection regulation*

### **Data protection by design**

**Who?** The data controller

**What?** Internal policies and appropriate measures within the entire lifecycle of technology:

-technical: minimising, pseudonymising, transparency, monitoring own data, security

-organisational : data protection impact assessments, data protection officers

**Why?** To comply with the general principles of data protection and protect individuals' rights

### **Data protection by default**

**Who?** The data controller

**What?** Internal policies and appropriate measures (privacy settings 'on')

**Why?** to comply by default with the general principles of data protection (user empowerment)





# Privacy by Design during the data processing lifecycle

---

Council's report (Dec 2014)

“Having regard to **available technology** and the **cost of implementation** and taking account of *the nature, scope, context and purposes of the processing* as well as the **likelihood and severity of the risk** for rights and freedoms of individuals posed by the processing, the controllers shall implement (...) technical and organisational measures appropriate to the processing activity being carried out and its objectives, [including minimisation and pseudonymisation], in such a way that the processing will meet the requirements of this Regulation and protect the rights of (...) data subjects”.





# Privacy by Design beyond the data processing lifecycle

	<u>Who should implement data protection by design?</u>
<b>EC's proposal 2012</b>	<b>Data controller</b> to implement data protection by design (Art 23 and Rec 61)
<b>Albrecht's report 2012</b>	<b>Data controller</b> + “ <b>Data processors and producers</b> shall implement appropriate measures and procedures to ensure that their services and products allow controllers by default to meet the requirements of this Regulation..” (Art 23 2a)
<b>LIBE Committee/ EP (Mar 14)</b>	<b>Data controller -</b> “...responsibility for the products and services used by the controller or processor” (Rec 61)
<b>Council's report (Dec 14)</b>	<b>Data controller</b> + “ <b>producers</b> of the products, services and applications <b>should be encouraged</b> to take into account the right to data protection” (Rec 61)







# PRIPARE

**PR**eparing Industry to **PR**ivacy-by-design by  
supporting its **AP**plication in **RE**search

Thank you for your attention

Questions?

Website: [www.pripareproject.eu](http://www.pripareproject.eu)





# Annex

---



# Privacy by Design during the data processing lifecycle

	<u>Data protection by design and by default– recital 61</u>
<b>EC’s proposal 2012</b>	In order to ensure and demonstrate compliance with this Regulation, the controller should adopt <b>internal policies and implement appropriate measures</b> , which meet in particular the principles of data protection by design and data protection by default.
<b>Albrecht’s report/ LIBE Committee/ EP Plenary (Mar 2014)</b>	<p><b>2 definitions of data protection by design and by default</b></p> <p>The principle of data protection by design require data protection to be embedded within the entire life cycle of the technology, from the very early design stage, right through to its ultimate deployment, use and final disposal.</p> <p>The principle of data protection by default requires privacy settings on services and products which should by default comply with the general principles of data protection, such as data minimisation and purpose limitation.</p>
<b>Council’s report (Dec 14)</b>	<p><b>Non-exhaustive list of measures:</b></p> <p>The controller shall implement measures... “Such measures could consist inter alia of <b>minimising the processing of personal data, (...) pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.</b>”</p>



# Privacy by Design: An interdisciplinary concept

## In Europe

- Data Security (Directive 95/46/EC): technical and organisational measures
- PETs to be combined with privacy management tools
- Data protection by design and by default (Draft GDPR): Internal policies, technical and organisational measures

## In Canada

**The concept of Privacy by Design could be represented as a trilogy of elements (Ann Cavoukian):**

