Implementation of Data Protection by Design and by Default: Framing guiding principles into applicable rules

Vienna - June 9, 2017

Lina Jasmontaite	@Linajasm
Irene Kamara	@kamara_irene
Stefano Leucci	@stefanoleucci
Gabriela Zanfir-Fortuna	@gabrielazanfir

Outline

- Motivation for the paper
- DPbD and its elements
- DPbDf and its elements
- Toolkits
- Practical application in three scenarios
- Concluding remarks

Data protection by design is no game changer but...

A. Cavoukian: *The 7 Foundational Principles of Privacy by Design*

Directive 95/46/EC, Article 17 & Recital 46

It is a legal obligation and not a compilation of 'vague principles'.

Working Party Article 29 and European Commission:
[t]he technological developments have strengthened the risks for individuals' privacy and data protection and to **counterbalance** these risks, the principle of 'Privacy by Design' should be introduced in the new framework: privacy and data protection should be integrated into the design of Information and Communication Technologies.

Framing
Data Protection by Design

Elements of DPbD

1. The controller… shall implement appropriate technical and organisational measures
2. Designed to implement data protection principles… and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects
3. In an effective manner
4. Taking into account:
    a. *The state of the art ... of the means for processing*
    b. *The cost of implementation*
    c. *The nature, scope, context of processing*
    d. *Purposes of processing*
    e. *Risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing*
5. At the time of the determination of the means for processing and at the time of the processing itself

1. The controller… shall implement *appropriate* technical and organisational measures

Risk-based approach

Contextual and dynamic nature

2. Designed to implement data protection principles… and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

1. The data protection principles listed in Article 5 of the GDPR;
2. The rights of the data subject and
3. The requirements of the GDPR

=

Compliance with the GDPR

3. In an effective manner

Contested

Risk management school

Recital 78 (‘How’ questions)

Broad meaning (Case C-131/13 Google v. AEPD)

The proportionality principle

4. Taking into account...

Develop knowledge about different elements of the processing

Weighing all the elements that are listed in Article 25

+

Documentation

=

Accountability

a) The state of the art … of the means for processing

- Benchmark
- Technical solutions & organizational practices
- The continuous learning or the knowledge ‘collection’ phase

b) The cost of implementation

- Going beyond the cost and benefit analysis
- The proportionality principle

c) The nature, scope and context of processing

The nature of processing activities = intrinsic characteristics of the processing
The scope of processing = amount of data, the number of data subjects involved, the organizational and technical environment where the processing activities are performed, including material and territorial scope
The context of processing activities refer to the relationship among different data processing tasks performed by the same data controller mainly referring to risks of data linkability.

d) Purposes of processing

Necessity &

data minimisation

e) Risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing

The risks related to the potential negative impact of the processing activity on data subjects' rights, freedoms and interests

5. At the time of the determination of the means for processing and at the time of the processing itself

Lifecycle

Framing
Data Protection by Default

DPbD

Data protection by design refers to the *existence of embedded safeguards and mechanisms* throughout the lifecycle of the application, service or product.

DPbDf

Data Protection by Default refers to the *activation of such safeguards as a default setting.*

Elements of the analysis

- Rationale of the Data Protection by Default principle
- Relationship of Data Protection by Design and Data Protection by Default
- Elements of Art. 25.2 GDPR

-'The controller shall implement appropriate technical and organisational measures'
-Ensuring that, 'by default, only personal data which are necessary for each specific purpose of the processing are processed'
Implementing appropriate technical and organisational measures is applicable to:

- *'the amount of personal data collected'*,
- *'the extent of their processing'*,
- *'the period of their storage' and*
- *'their accessibility' (including the goal of not making the data available to an indefinite number of persons)*

Active choosing

-More protection to the individual
-Example in the GDPR: consent Art. 6

Default rules

-Tend to ***stick***
-Example in the GDPR: Data Protection by Default Art. 25.2
-ENISA (2014)

"data protection by default 'means that in the default setting the user is already protected against privacy risks' and 'this affects the choice of the designer which parts are wired-in and which are configurable"

The controller shall implement appropriate technical and organisational measures

Positive obligation of the controller

Purposes of processing

Necessity and data minimisation

- ***The amount of personal data collected***
- ***The extent of their processing***
- ***The storage period and***
- ***Their accessibility***

- Data minimisation
- Purpose limitation
- Storage limitation
- Principle of integrity and confidentiality

Interim conclusion

- Data Protection by Default **does not add new content** to the obligations of the controllers; it only affects the *timing* of compliance; that is from the very start of data processing.
- Debate **over added value** of default
- Data Protection by Default can **safeguard children, minors, elderly and other groups** that can be considered to be in a weaker position than an average (adult) individual.
- The implementation of DPbDf measures is **not an end itself**.

*DPbDf requires not only on taking measures, but also focuses on their **actual outcome**, that is, whether they protect individuals' personal data.*

Data Protection by Design Toolkit

	Time of the determination of the means for processing	Time of the processing
Taking into account		
Nature, scope, context of processing		
Purposes of processing		
Risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing		

The controller shall implement		
Appropriate **technical and organisational measures** designed to implement data protection principles ● in an effective manner ● Taking into account: ● the state of the art, ● the cost of implementation	*Which principles: only the list of principles (art. 5)?* *What kind of measures designed to enforce them?*	
Integrate the necessary **safeguards** into the processing ● ***in order to meet the requirements of this Regulation*** ● in an effective manner, ● Taking into account: ● the state of the art, ● the cost of implementation.	*Which requirements? All the GDPR requirement according to the specific context?* *What kind of safeguards?*	
Integrate the necessary **safeguards** into the processing in order to ● ***protect the rights of data subjects*** ● in an effective manner, ● taking into account: ● the state of the art, ● the cost of implementation	*Which right of data subjects?* *Should we go beyond data protection rights?*	

Data Protection by Default Toolkit

(ongoing)

	Amount of personal data collected (**data minimization**)	Extent of the processing (**purpose limitation**)	Period of the storage (**retention limitation**)	Accessibility (**principle of integrity and confidentiality**)
The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.				
Such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.				

DPbD and DPbDf in practical scenarios

Why?

- extract **specific safeguards and requirements** to be implemented in specific contexts
- generalize results with the aim of building a **common set of safeguards and measures**
- explore ways for **improving our framework**, better shaping the sequentiality
- explore the possibility to **integrate the two toolkits** in just one holistic instrument

What?

- Consumer analytics for advertising purposes
- mHealth applications in the insurance sector
- People search engine

Concluding remarks

DPbD and DPbDf constitute a meta-requirement system

DPbD and DPbDf require implementing already existing obligations resulting from intrinsic features of personal data processing, strengthening and further reinforcing the long established data protection principles and obligations (accountability included!)

Conclusion

- Even though a few requirements might be generalized, most them are contextual and depend on the circumstances of the processing.
- The pivot of the requirement is the ***specific privacy risk assessment*** that has to be performed both at the time of the determination of the means for processing and at the time of the processing itself (proportionality and appropriateness)
- Revisions in the ***logic*** involved in any automatic personal data processing activities are often required for the aim of designing systems and processes truly able to serve mankind (helping accountability!)
- Controller and processor can implement the two principles for gaining ***competitive advantage*** for a more comprehensive and meaningful protection of data subjects.

Next steps

- Many elements still need further guidance (risk-based approach!)
- Future works will try to build up a ***step-by-step methodology*** for considering different aspects, parameters and requirements that has to be translated into specific system and process requirements.
- We believe that this research has to be conducted with a ***domain-dependent approach*** because of the clear need to consider peculiarities and risks involved in processing activities.

Thank you!

Questions and remarks are welcome

@Linajasm
@kamara_irene
@StefanoLeucci
@gabrielazanfir