Ethikos lawyers

Making business ethical

Ethikos
200 Avenue Louise 1000 Brussels, Belgium
www.ethikos.be

Ethikos lawyers
Making business ethical

ARMA-GLA SUMMER SPOTLIGHT WORKSHOP:

"Leveraging GDPR Compliance investments with the CCPA"

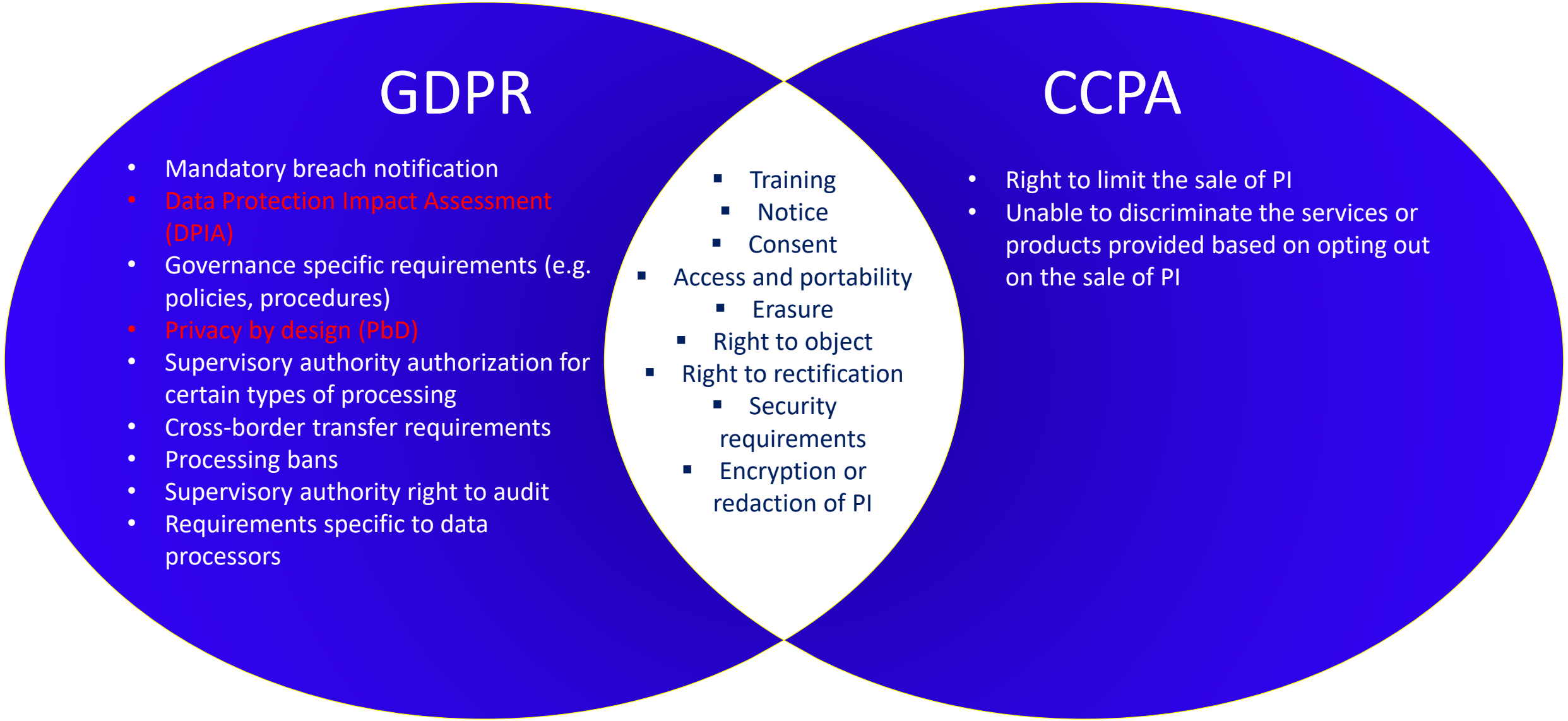
July, 31st 2019

Miguel Mairlot – Partner at Ethikos & Certified D.P.O.

Ethikos lawyers
Making business ethical

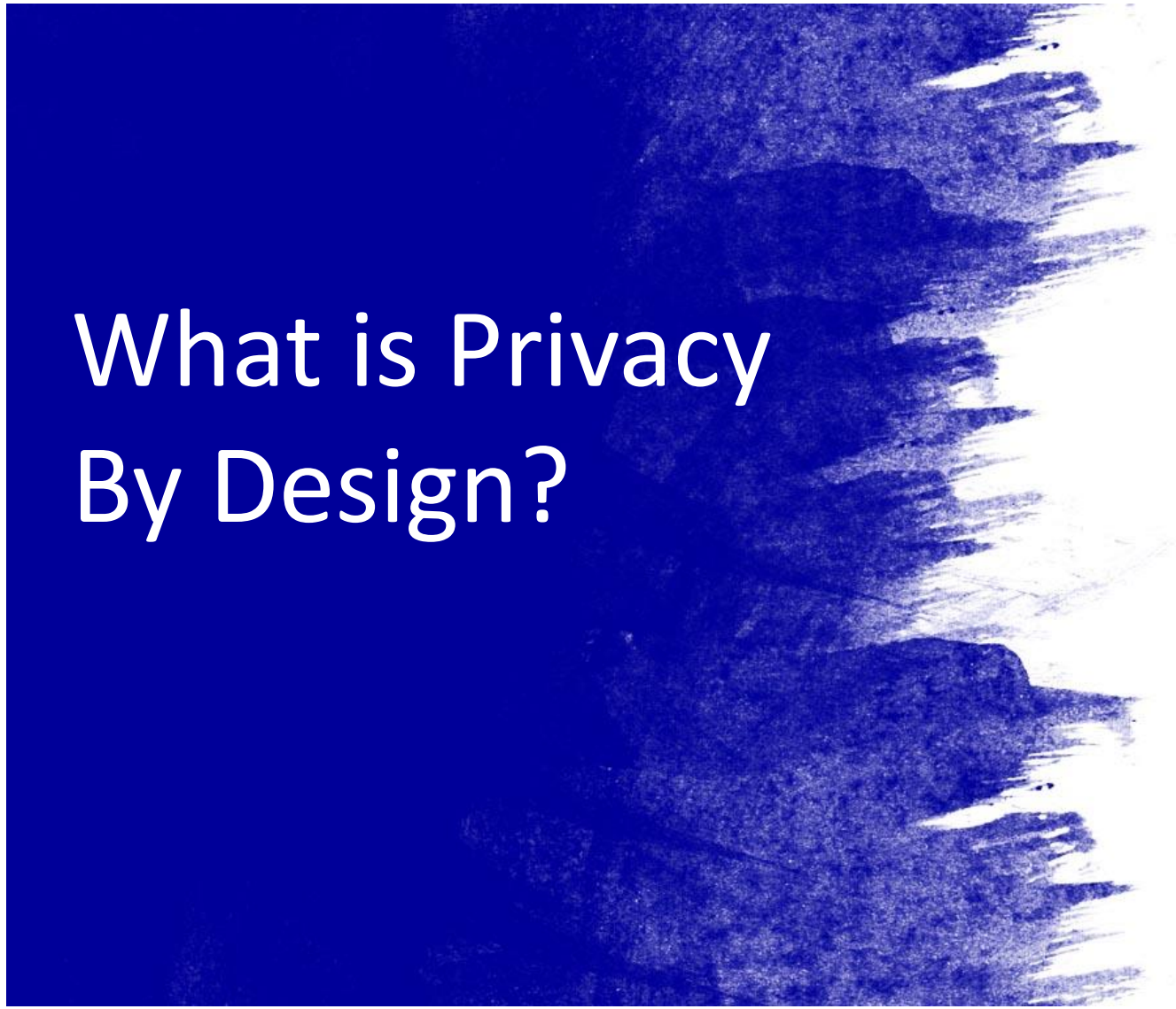
Why leveraging on GDPR compliance to prepare for the CCPA?

Ethikos lawyers
Making business ethical



Ethikos lawyers
Making business ethical

What is Privacy By Design?



Article 25 GDPR: Data Protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data protection principles such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subject.
2. The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, 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.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Privacy by Design?

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start, and should be considered for example when:

- Building new IT systems for storing or accessing personal data;
- Developing legislation, policy or strategies that have privacy implications;
- Embarking on a data sharing initiative;
- Using data for new purposes.

Data Protection Impact Assessments (DPIAs) are an integral part of taking a privacy by design approach.

The 7 principles of Privacy by design

The objectives of Privacy by Design – ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the 7 Foundational Principles.

1. **Proactive** not Reactive; **Preventive** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full functionality – **Positive-Sum**, not Zero-Sum
5. End-to-End Security – **Full Lifecycle Protection**
6. **Visibility** and **Transparency** – Keep it **Open**
7. **Respect** for User Privacy – Keep it **User-Centric**

1. Proactive not Reactive; Preventive not Remedial

PbD approach is characterized by proactive rather than reactive measures.

It anticipates and prevents privacy-invasive events before they happen.

PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring.

In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting

PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT systems or business practice.

Data subjects should get the maximum privacy protection as a baseline (safeguards to protect personal data, restricted sharing, minimized data collection, retention policies).

“The less data you have, the less damaging a breach will be”.

3. Privacy embedded into Design

Privacy should be embedded into design and architecture of IT systems and business practices.

“IT systems designers should think about privacy as a core feature of the product”.

Privacy is integral to the system, without diminishing functionality.

4. Full functionality Positive-Sum, not Zero-sum

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.

The idea here is that PbD should not compromise business goals. You can have privacy, revenue, and growth. You're not sacrificing one for the other.

Establishing a PbD culture is key to any organization subject to the GDPR.

5. End-to-End Security – Full Lifecycle Protection

PbD, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish.

“Privacy protections follow the data, wherever it goes”.

The same PbD principles apply when the data is first created, shared with others, and then finally archived. Appropriate encryption and authentication should protect the data till the very end when it finally gets deleted.

6. Visibility and Transparency – Keep it open

Information about your privacy practices should be out in the open and written in a way consumers can understand (non-legal terms).

This is the principle that helps build trust with consumers.

7. Respect for User Privacy– Keep it User-Centric

PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

Consumers own the data. The data held by an organization must be accurate, and the consumer must be given the power to make corrections.

Keep it user-centric

Ethikos lawyers
Making business ethical

How to achieve Privacy by Design?

Ethikos lawyers
Making business ethical

First Step: Data Protection Impact Assessment

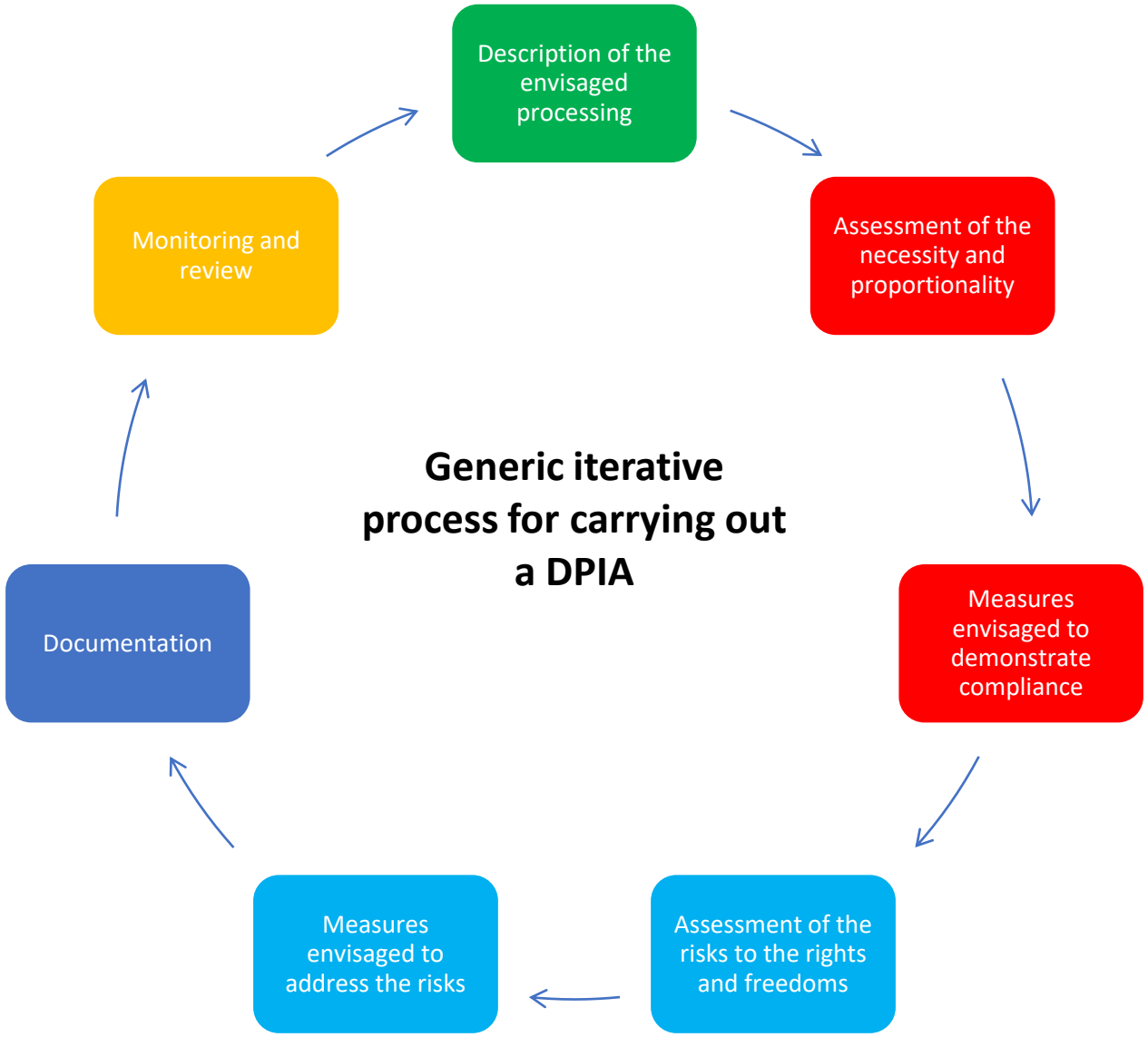
A DPIA is a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data.

DPIAs are important tools for accountability, as they help, not only to comply with the requirements of the GDPR, but also to demonstrate that appropriate measures have been taken to ensure compliance with the requirements of the GDPR.

What is the methodology to carry out a DPIA?

Different methodologies but common criteria.
The GDPR sets out the **minimum features** of DPIA (Article 35(7), and recitals 84 and 90):

- *a description of the envisaged processing operations & the purposes of the processing;*
- *an assessment of the necessity and proportionality of the processing;*
- *an assessment of the risks to the rights and freedoms of data subjects;*
- *the measures envisaged to address the risks and demonstrate compliance with the Regulation.*


Description of the envisaged processing
Assessment of the necessity and proportionality
Measures envisaged to demonstrate compliance
Assessment of the risks to the rights and freedoms
Measures envisaged to address the risks
Documentation
Monitoring and review
Generic iterative process for carrying out a DPIA

Recap: Why are PbD & DPIA relevant for an organization?

- DPIA can be used to identify and reduce the privacy risks of your projects. It can also help you to design more efficient and effective processes for handling personal data
- PbD would help organizations to achieve Knowledge AND Privacy
- PbD would make personal data compliance easier to manage also for non-experts users and mitigate the chances of data breaches
- DPIA & PbD would help to preserve organizations' reputation

Ethikos lawyers
Making business ethical

www.ethikos.be

info@ethikos.be

Ethikos
200 Avenue Louise 1000 Brussels, Belgium
www.ethikos.be