EDPS

EUROPEAN DATA PROTECTION SUPERVISOR

Privacy Engineering after the GDPR: new opportunities, new challenges

Achim KLABUNDE
Adviser to the Supervisor on Technology and Data Protection
EDPS – European Data Protection Supervisor

IWPE 2020 – International Workshop on Privacy Engineering
7 September 2020 - Genova, Italy (online)

Overview

- Context: EDPS, GDPR History and Background
- PbD → DPbD
- GDPR Article 25 under the microscope
- Core concept: “State of the Art”
- Questions – to the audience
- Where do we go from here?

The EDPS

The EU’s independent data protection authority

The EDPS

The **European Data Protection Supervisor**: an independent institution responsible for ensuring the protection of personal data by the EU institutions and bodies

Wojciech Wiewiórowski
EDPS

The EDPS

1. **Supervise** data processing done by EU institutions and bodies;
2. **Advise** the EU legislator and appear before the EU courts;
3. **Monitor** new technologies with an impact on privacy;
4. **Cooperate** with other supervisory data protection authorities.

GDPR family

- Ancestors
  - 1970s: Regional and national laws in DE, FR, SE, USA
  - 1980s: Council of Europe Convention 108 (revised)
  - OECD Privacy Guidelines (revised 2013)
- Parents and Aunts
  - EU Data Protection Directive 95/46/EC
  - ePrivacy Directive 2002/58/EC (revised 2009)
  - Framework Decision 2008/977/JHA
  - Regulation 45/2001/EC
- Siblings
  - Law Enforcement Directive (EU) 2018/680
  - “EDPR” Regulation (EU) 2018/1725
  - ePrivacy Regulation (forthcoming)

GDPR changes

- Clarifications
  - Definitions
  - Existing Obligations (Consent, Transparency, Joint Controllers, International Transfers)
  - Data subject rights
  - Supervisory Authorities' Powers and Tasks
- Changes and new concepts
  - Territorial Scope
  - Accountability (principles, DPIA, DPbD, DPO, etc.)
  - Certification
  - Harmonisation: Cooperation and Consistency
  - Data breach notifications

Data Protection principles

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability
- Security
- Data subjects' rights

Lawful processing

Article 6(1): Six conditions

a) Consent for specific purposes
b) Necessary for performance of a contract
c) Legal obligation
d) Vital interests of the individual
e) Public interest
f) Legitimate interest, balanced afainst individual’s rights

Point (c) and (e) require legislation.

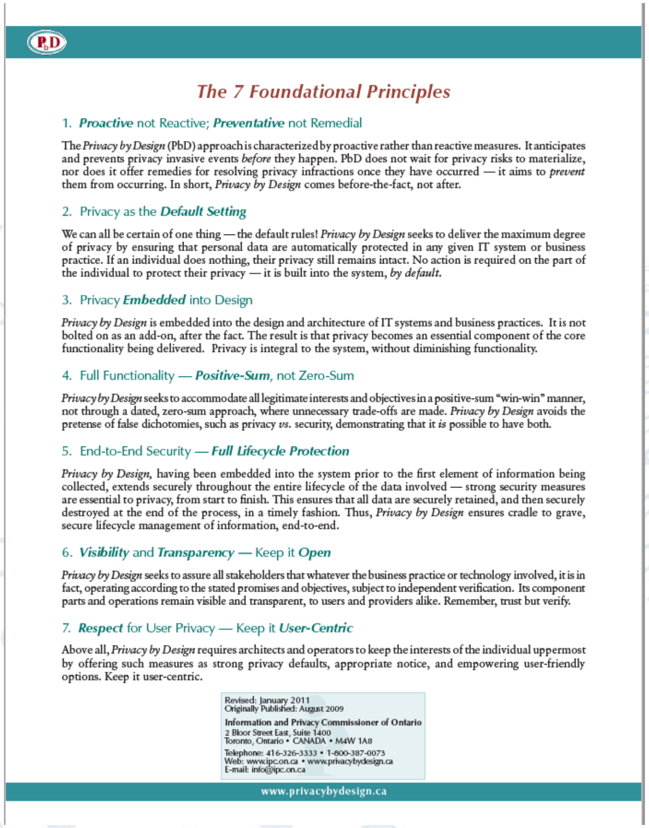
DPA powers

- Investigations
  - Order provision of information, including personal data
  - Audits and Certification Reviews
  - Access to premises
- Order compliance
  - Warnings and reprimands
  - Order changes of processing with details and deadline
  - Limit or ban processing or suspend data flows
  - Order actions towards data subjects
  - Impose fines

From Privacy to Data Protection by Design

- PbD
  - Approach developed since 1995
  - High level framework
  - Difficult to enforce
- GDPR approach
  - Data protection by Design and by Default
  - DPbDD, DPbD^2
  - Based on accountability and DP principles
  - Legal obligation
  - Violation may be fined ≤ max(10 M€; 2% of turnover)
  - Certification of compliance

Privacy by Design



PbD

The 7 Foundational Principles

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (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***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — ***Positive-Sum***, not Zero-Sum

Privacy by Design 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. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.

5. End-to-End Security — ***Full Lifecycle Protection***

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. ***Visibility*** and ***Transparency*** — Keep it ***Open***

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. ***Respect*** for User Privacy — Keep it ***User-Centric***

Above all, *Privacy by Design* 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. Keep it user-centric.

Revised: January 2011
Originally Published: August 2009

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario • CANADA • M4W 1A8

Telephone: 416-326-3333 • 1-800-387-0073
Web: www.ipc.on.ca • www.privacybydesign.ca
E-mail: info@ipc.on.ca

www.privacybydesign.ca

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 5/2018

Preliminary Opinion on privacy by design

EDPS

31 May 2018

GDPR Article 25

Embed data protection principles and safeguards (article 25)

Data protection by Design

- “Implement data protection principles“
- “both at the time of the determination of the means for processing and at the time of the processing itself”

Data protection by default

- = strictest privacy settings automatically apply

GDPR Article 25, paragraph 1:

Taking into account the <u>state of the art</u>, 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 organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, 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 subjects.

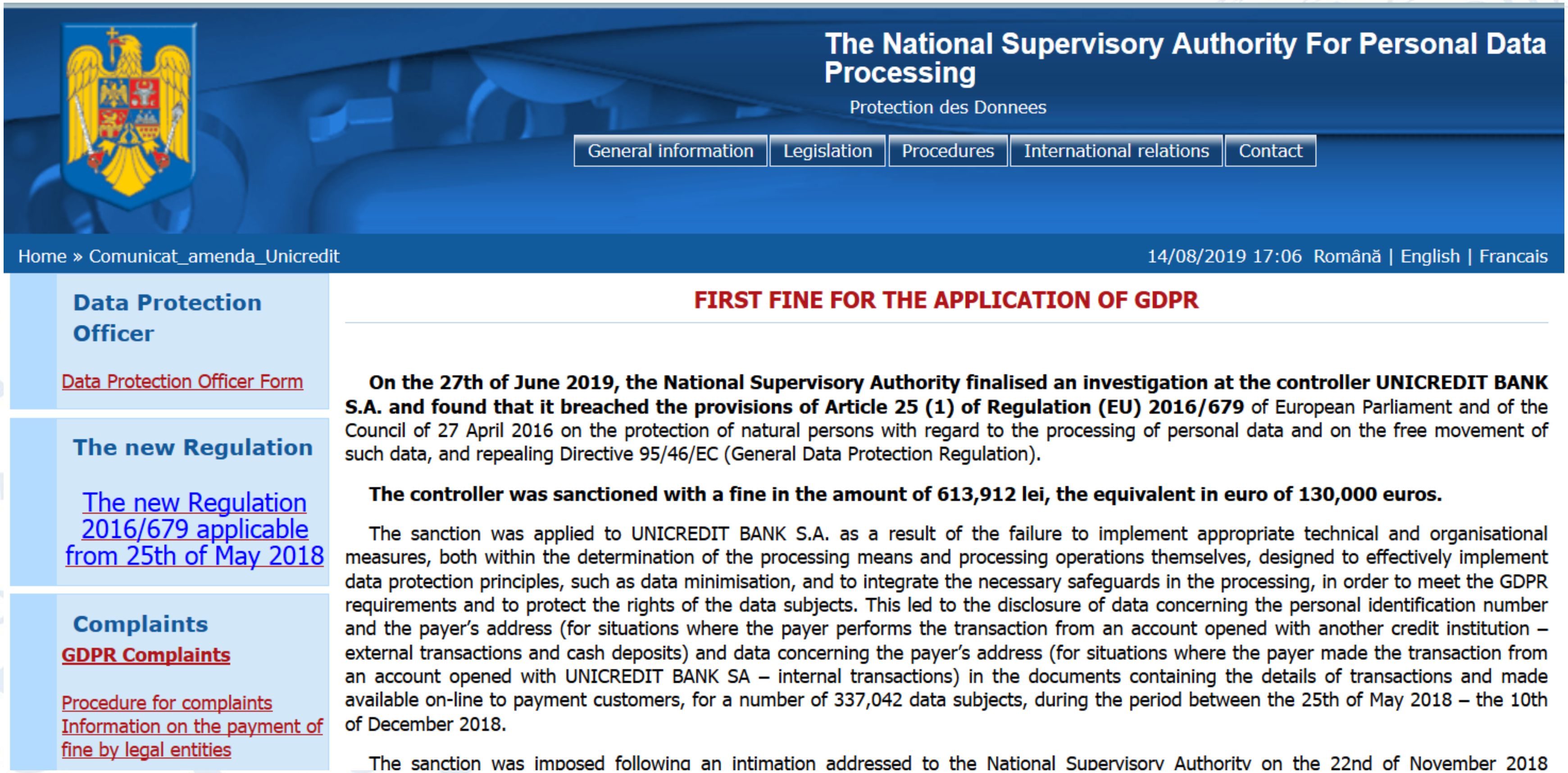
“State of the art”

- Established concept in law, e.g. consumer protection and environmental law
- In data protection law already present in data security provisions
- State of the art is a dynamic concept
- For each domain, needs to be established and monitored
- Standardisation and certification may help in some areas
- GDPR ambition to trigger advancement of the state of the art (Recital 78)

What are DPAs doing?

- Enforcement
- Provide guidance on interpretation and implementation of the GDPR – individually and through the EDPB
- Exchange and cooperation with controllers, processors and suppliers
    - Identify good practices
    - Standardisation
- Cooperation with research

Enforcement


General information
Legislation
Procedures
International relations
Contact
Home » Comunicat_amenda_Unicredit
14/08/2019 17:06 Română | English | Francais

The National Supervisory Authority For Personal Data Processing

Protection des Donnees

Data Protection Officer

Data Protection Officer Form

The new Regulation

The new Regulation 2016/679 applicable from 25th of May 2018

Complaints

GDPR Complaints

Procedure for complaints

Information on the payment of fine by legal entities

FIRST FINE FOR THE APPLICATION OF GDPR

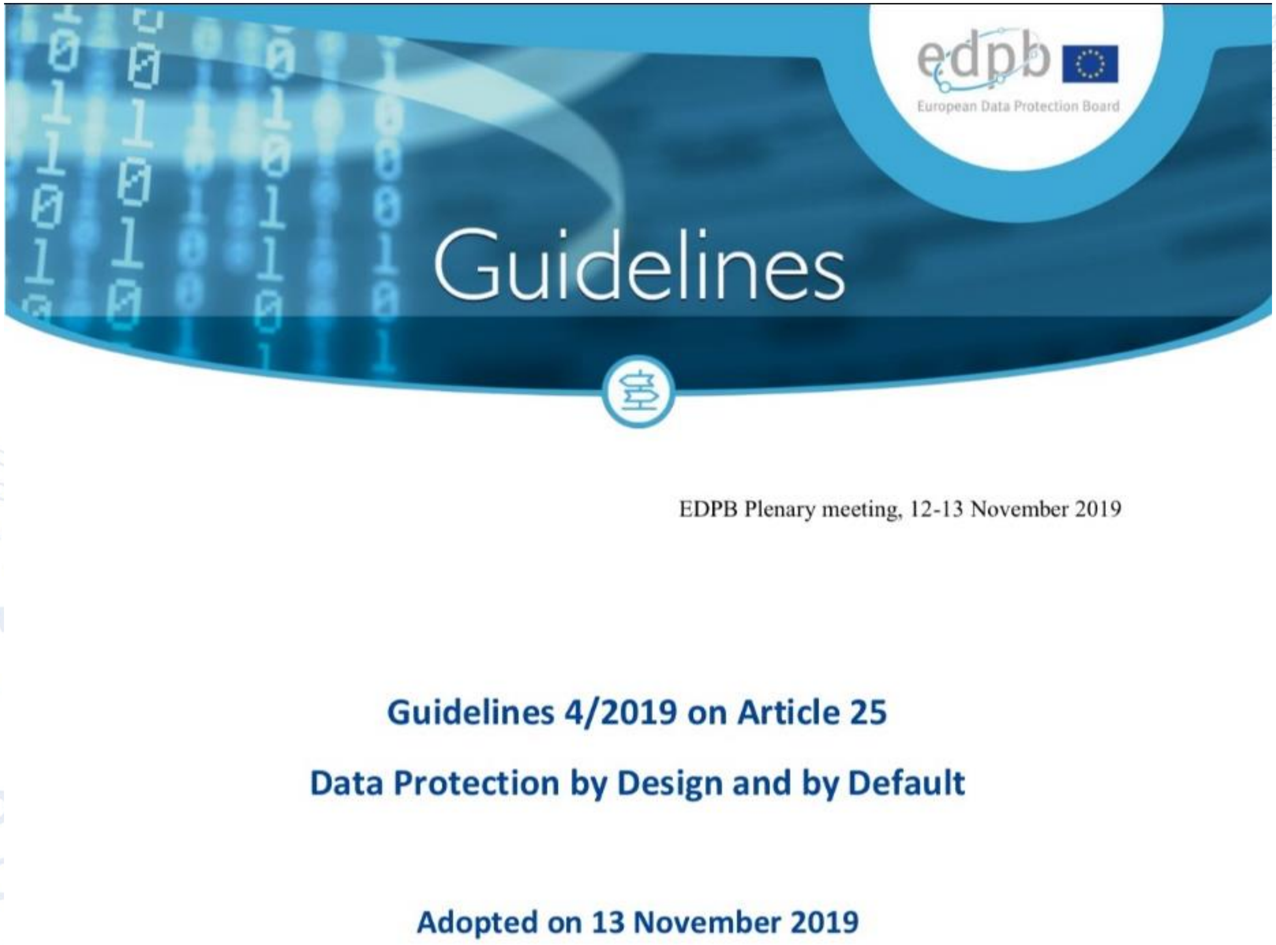
On the 27th of June 2019, the National Supervisory Authority finalised an investigation at the controller UNICREDIT BANK S.A. and found that it breached the provisions of Article 25 (1) of Regulation (EU) 2016/679 of European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The controller was sanctioned with a fine in the amount of 613,912 lei, the equivalent in euro of 130,000 euros.

The sanction was applied to UNICREDIT BANK S.A. as a result of the failure to implement appropriate technical and organisational measures, both within the determination of the processing means and processing operations themselves, designed to effectively implement data protection principles, such as data minimisation, and to integrate the necessary safeguards in the processing, in order to meet the GDPR requirements and to protect the rights of the data subjects. This led to the disclosure of data concerning the personal identification number and the payer's address (for situations where the payer performs the transaction from an account opened with another credit institution – external transactions and cash deposits) and data concerning the payer's address (for situations where the payer made the transaction from an account opened with UNICREDIT BANK SA – internal transactions) in the documents containing the details of transactions and made available on-line to payment customers, for a number of 337,042 data subjects, during the period between the 25th of May 2018 – the 10th of December 2018.

The sanction was imposed following an intimation addressed to the National Supervisory Authority on the 22nd of November 2018

EDPB Guidance



edpb

European Data Protection Board

Guidelines

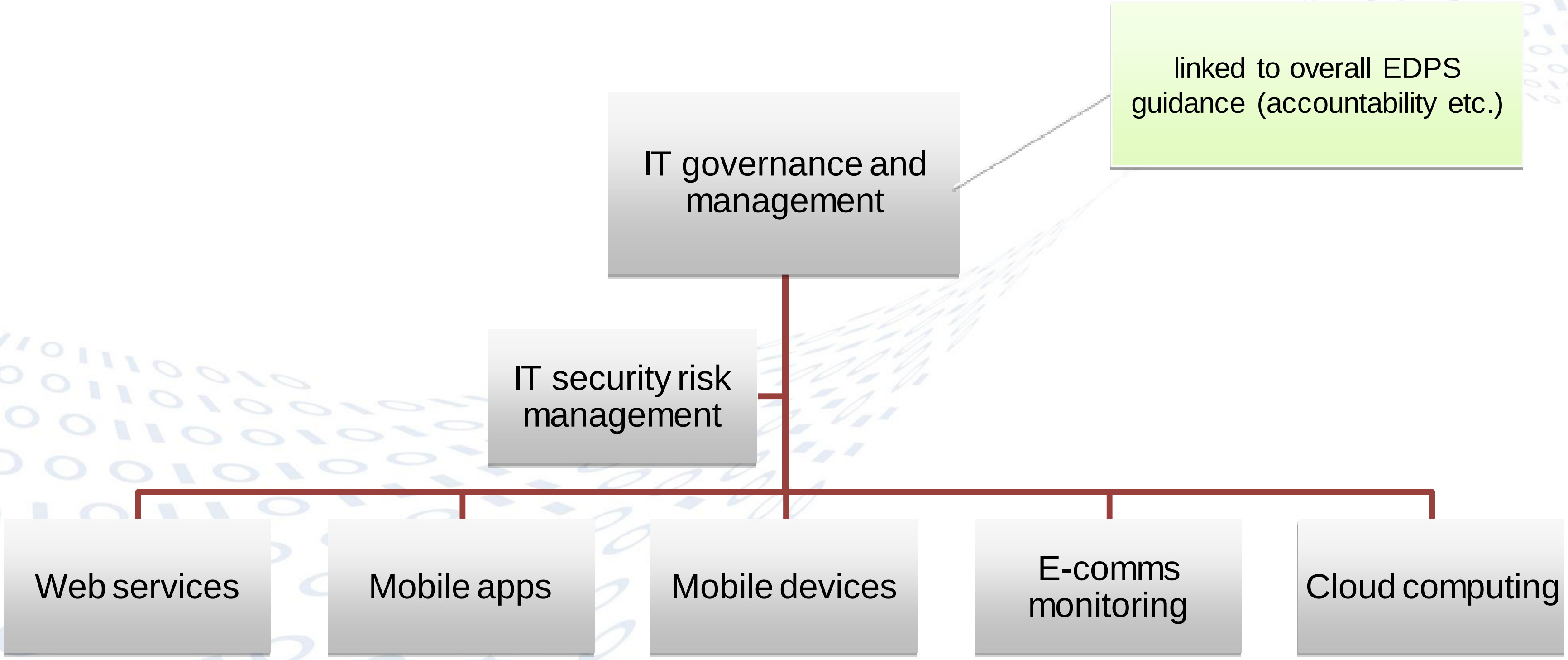
EDPB Plenary meeting, 12-13 November 2019

Guidelines 4/2019 on Article 25

Data Protection by Design and by Default

Adopted on 13 November 2019

EDPS tech intensive guidelines



IT governance and management

linked to overall EDPS guidance (accountability etc.)

IT security risk management

Web services

Mobile apps

Mobile devices

E-comms monitoring

Cloud computing

Where do we go from here?

Four questions:

- Is Privacy Engineering already sufficiently mature to satisfy the demands of the GDPR?
- What are the gaps in the portfolio of PETs and PE methodologies that need to be addressed by R&D?
- How can the public sector contribute to advancing the state of the art?
- What are the best ways to create incentives for suppliers of tools and devices to integrate DpbD in their products?

Internet Privacy Engineering Network

- Cooperation DPAs, Industry, Academia
- 2013 Snowden & IETF Reaction
- Launch September 2014
- 5 years, 6 workshops, 2 special events

2019 Workshop Rome

- Topic: “state of the art”
- Existing concepts
- Business without tracking
- Privacy engineering methodologies
- Anonymisation, pseudonymisation

Where do we go from here?

Five questions:

- Is Privacy Engineering already sufficiently mature to satisfy the demands of the GDPR?
- How to determine the start or the art so that it becomes operational for controllers, DPAs and courts?
- What are the gaps in the portfolio of PETs and PE methodologies that need to be addressed by R&D?
- How can the public sector contribute to advancing the state of the art?
- What are the best ways to create incentives for suppliers of tools and devices to integrate DpbD^2 in their products?

EDPS

thank you!

Q? A!

www.edps.europa.eu
edps@edps.europa.eu
@EU EDPS
@achimkla