GemTALK - How to achieve Privacy by Design and conduct DPIAs

An analysis of how key GDPR compliance can be embedded into processes and procedures

Ivana Bartoletti – Head of Data Protection, Privacy and Ethics
Beatriz Ruiz-Beato – Data Protection Officer, NEC Europe

Gemserv

Structure

- **Introduction to the Webinar**
- **Privacy by Design**
  - Introduction to Privacy by Design
  - Principles for Privacy by Design
  - Privacy by Design Process
  - Examples: Data minimisation
  - Examples: PETs
  - Examples: Security by Design
- **DPIAs**
  - Background to the DPIA process
  - Examples of DPIA assessments
  - Procedures for ongoing monitoring
- **Questions and Answers**

Introduction to Privacy by Design

- **General Requirements**
  - **Article 25** GDPR requires organisations to implement appropriate technical and organisational measures
  - **Article 35** GDPR requires an assessment on the impact of the envisaged processing to be carried out where they can cause a ***high risk to data subjects***.
  - Privacy by Design aims to implement principles – such as data minimisation and purpose limitation – through technological methods and processes.
  - **Fines of up to can be levied for up to €10,000,000 or 2% of global turnover.**

Risks to data subjects can involve:

- Unwelcome intrusion into their privacy
- The possibility for profiling
- Financial effects of decisions
- Inability to exercise right to erasure
- Possibility of unauthorised disclosure

Privacy by Design Principles

Ann Cavoukian formulated seven principles that enshrine Privacy by Design:

Proactive not reactive: A commitment to high standards and the definition of values

End-to-End Security: Ensuing data is protected throughout its lifecycle

Privacy by Default: Building collection, usage and storage limitations by default

Visibility and Transparency: Ensure accountability and openness about collection and processing

Privacy embedded into design: Carry-out and address privacy impact assessments

Respect for User Privacy: Provide for user-friendly principles and options

Full Functionality - Positive Sum, not Zero Sum: Reject Privacy trade-offs

Privacy by Design Process

1

Carry out a data mapping exercise to identify the nature, scope, context and purposes of processing – and the risks for natural persons.

2

Carrying out a cost-benefit analysis and a balancing assessment, organisations should consider:
1) what mitigating PbD measures could be involved;
2) the cost of their implementation;
3) the risks for natural persons.

3

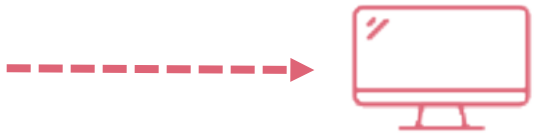
The measures should then be implemented into the systems or processes, as appropriate.

Examples: Data Minimisation

The following are examples data minimisation as incorporated in different systems and processes:

Example:
A free running app is made available to users with features including location sharing, audio and camera capture and integration with other platforms.

Example:
The marketing department of a large commercial retailer wishes to profile customers to deliver targeted advertisements.



Examples: Privacy Enhancing Technologies (PETs)

PETs are a system of ICT measures that protects privacy by eliminating or reducing personal data processing without losing functionality of the information system.

Why implement PETs?

Cost Effective

Risk Mitigation

Building Trust

Downside of PETs:

High Initial Expenditure

Struggles when implementing data subjects' rights

Constant evolvement

Examples: Privacy Enhancing Technologies (PETs)

PETs as Substitutes

Encryption Tools

Anonymisation Tools

Complementary PETs

Privacy Friendly Tools

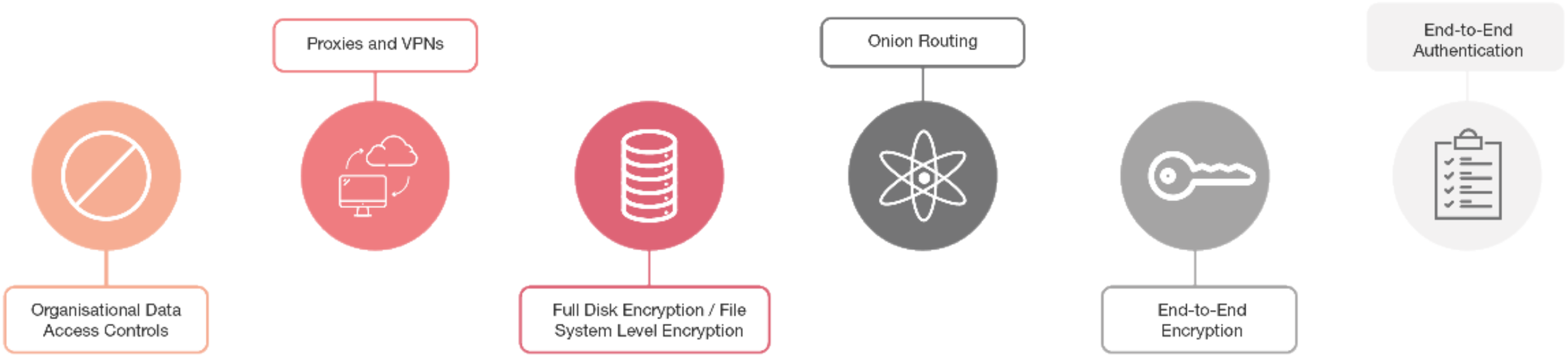
- Privacy Notice
- Consent
- Dashboards

Privacy Preserving Tools

- Cryptographic Obfuscation in Targeted Advertising

Examples: Security by Design

The following are examples of technology that can be deployed to comply with the “Security by Design” principle:



Data Protection Impact Assessments

Data Protection Impact Assessments (DPIAs)

General Requirements

- **Article 35 GDPR** provides an assessment of the risks related to certain processing activities or systems to be undertaken, i.e. where there are *high risks* to data subjects.
- **This is a higher threshold than normal Privacy by Design requirements.**
- Mandatory DPIA lists have been issued by European Supervisory Authorities.
- Privacy by Design by negotiation: the views of the data subjects

Examples of DPIA assessments

We suggest the following based on the European Supervisory Authority lists:

Processing sensitive personal data e.g. health records, criminal records, children's data

Deployment/development of new technologies or ways of using personal data

Tracking individuals through cookies, CCTV monitoring, location monitoring or employee monitoring

Decisions having a significant impact on individuals (e.g. contractual/legal benefit)

Processing likely to deprive data subjects of any of their rights

Processing on a large scale e.g. over 10,000 records and/or several jurisdictions

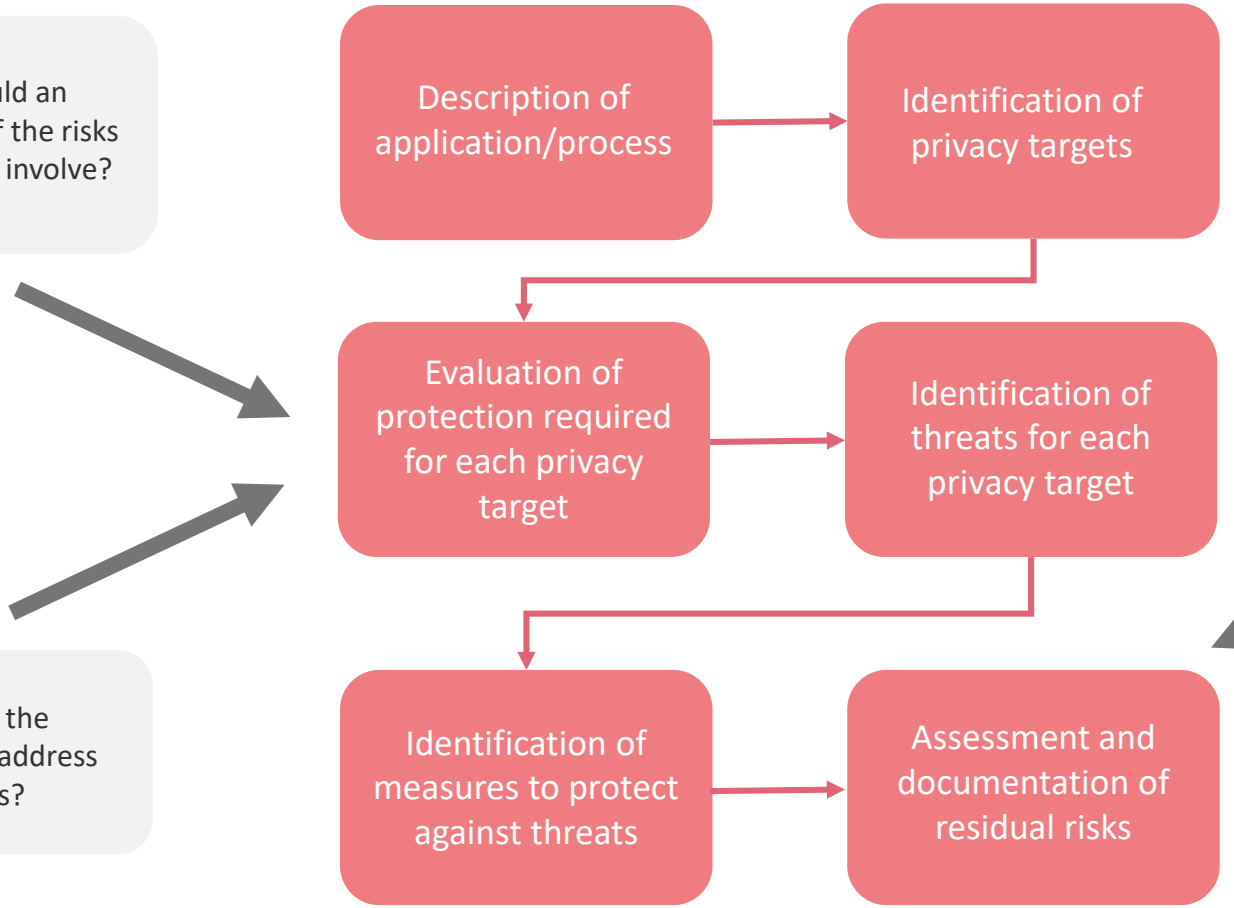
Cross-referencing of different data sets or profiling individuals

Background to the DPIA process

This explains how the DPIA process works in practice:

What would an assessment of the risks to individuals involve?

What are the measures to address the risks?



What does the consideration of 'necessity and proportionality' involve?

Ongoing Monitoring

Organisations should do the following

1.  Ensure that a risk register/action plan is carried out, with relevant responsibilities assigned

2.  Follow up on any changes to the risks or the scope of processing

3.  Collect metrics on the extent to which targets are being met and risks are being reduced

4.  Follow up with annual audits

Any Questions?

Thank you for listening

Please feel free to contact:

dataprotection@gemserv.com

Gemserv