Interactive Workshop on Data Protection Impact Assessment

A Hands-On Tour of the GDPR’s Most Practical Tool

IFIP Summer School 2017

Felix Bieker, Michael Friedewald and Marit Hansen
Workshop Structure

• Short Introduction to DPIA
• The Standard Data Protection Model and Risk Analysis
• Data Subject Participation
• Hands-On: Two Cases for Analysis
  ▪ Group discussions
  ▪ Presentation & Discussion
The General Data Protection Regulation

- Applicable May 2018
- Obligations for controllers:

**Article 24**

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
The General Data Protection Regulation

- Applicable May 2018
- Obligations for controllers:

Article 32

Security of processing

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
The General Data Protection Regulation

- Applicable May 2018
- Obligations for controllers:

\[\text{Article 24}\]

Responsibility of the controller

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate \textit{technical and organisational measures} to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
The General Data Protection Regulation

• Applicable May 2018
• Obligations for controllers:

Article 25

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 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.
The General Data Protection Regulation

• Applicable May 2018
• Obligations for controllers:

Article 33

Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
The General Data Protection Regulation

- Applicable May 2018
- Obligations for controllers:

**Article 30**

Records of processing activities

1. Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
The General Data Protection Regulation

- Applicable May 2018
- Obligations for controllers:

**Article 35**

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
The General Data Protection Regulation

• Applicable May 2018
• Obligations for controllers:

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
What is a Data Protection Impact Assessment?

- Tool to implement controller obligations
- Starts before processing
- Continues over entire life cycle
- Ensures compliance
- Enables transparency for
  - Controller
  - Users
  - DPAs
- Analyses risks for rights and freedoms of individuals
- Mitigates these risks with technical and organizational measures
1. Preparation Phase

2. Execution Phase

3. Implementation Phase

4. Review Phase
1. Preparation Phase

Initiation by Data Protection Management

(Further) development of a personal data processing procedure

Decision to implement a DPIA or change in circumstances since last DPIA

1. Preparation phase

1.1 Relevance threshold: Is a DPIA necessary?

1.2 Projecting the assessment

1.3 Description of target of evaluation and purposes of processing

1.4 Identification of actors and persons concerned

1.5 Identification of relevant legal bases
2. Execution Phase

2.1 Identification of evaluation criteria based on protection goals

2.2 Identification of potential attackers, their motives and objectives

2.3 Determination of the level of interference and level of protection

2.4 Evaluation of the risk

Catalogue of reference safeguards

2.5 Identification of appropriate safeguards

2.6 Documentation of evaluation results (including residual risk analysis)

DPIA report

End of a DPIA cycle

Positive end result?

Fail

Prior consultation (Art. 36 GDPR)

Pass

Abstention from processing operation
3. Implementation Phase
4. Review Phase

3. Implementation phase

- 3.3 Implementation of safeguards
- 3.3 Testing and documentation of the effectiveness of the safeguards
- 3.5 Demonstration of compliance with GDPR
- 3.6 Approval of processing operations

4. Review phase

- 4.1 Continuous review of DPIA
- 4.2 Supervision of DPIA results
- 4.3 Independent auditing of DPIA results
The Standard Data Protection Model

• Requirements of data protection
  → Six protection goals
    (+ data minimisation as general requirement)

• Three components:
  Data, IT systems and processes

• Three protection levels for data
  (data subject’s perspective)

• Work in progress: catalogue of reference protection measures

Criteria: Six Protection Goals

- Confidentiality
- Integrity
- Transparency
- Availability
- Unlinkability
- Intervenability
- Data Minimisation

*) From the data subject’s perspective

Classic IT security goals*)
Art. 5 para. 1 “Personal data shall be:

(a) processed (…) in a transparent manner in relation to the data subject (‘transparency’);

(b) collected for specified, explicit and legitimate purposes (…) (‘purpose limitation’);

(c) (…) limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) (…) Personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(f) (…) integrity and confidentiality”.

Implicitly: Availability
Risk Evaluation

- **Risk = Impact x Probability**
  \[ R = \sum_{k=1}^{n} I_k \times p(I_k) \]

- Proper assessment is paramount

Recital 76 “The **likelihood and severity of the risk to the rights and freedoms** of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk”
Examples for risks

• Risk to the rights and freedoms of natural persons …
• … which could lead to physical, material or non-material damage
  ▪ Discrimination
  ▪ Identity theft / fraud
  ▪ Financial loss
  ▪ Damage to reputation
  ▪ Significant economic or social disadvantage
  ▪ Deprivation of data subject’s rights
  ▪ Prevention from exercising control over personal data
Protection Goals and Measures

- Data Minimisation (e.g. reduction of data/identifiability)
- Confidentiality (e.g. encryption, access control)
- Integrity, Authenticity (e.g. access control, digital signatures)
- Availability (e.g. redundancy, back-up)
- Unlinkability (e.g. separation, isolation, division of powers)
- Transparency, Auditability (e.g. logging, control of SysAdmin, documentation, user manuals, information and notification of users, access)
- Intervenability (e.g. rectification, erasure, complaint handling, change management, off-switch to deactivate/stop processing)
Data Protection Impact Assessment

Stakeholder consultation

Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research
12th IFIP Summerschool Privacy and Identity Management
04 September, Ispra, Italy
(9) Where **appropriate**, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

No criteria, when involvement is appropriate...

Backdoor to avoid involvement of people affected? Especially in sensitive areas
Consultation of affected people is always useful!

- Different views and assessment of risks
  - Early identification of expectations, priorities of users
  - Unexpected solutions
- Increases the quality of results
  - Minimises unexpected and uncontrollable rejection by potential users
- Legitimises the DPIA
Views of the data subject

Who is affected? Who else has interests?

- Data subjects are in the focus of DPIA
- ... but in different roles (citizens, consumers, employees, ...)
- Employees of manufacturers/operators (can be attackers at the same time!)
- Third parties, which are not directly involved in the data processing (bystanders, intelligence services)

If the data subject is not available

- Consult “their representatives”: consumer protection organisations, works council, civil rights groups, ...
- Absolute minimum: Involve units that know the customers (sales, maintenance, etc.) – this is no consultation in the strict sense!!!
The consultation process

Adequate involvement of these groups?

- Participatory (TA) methods (focus groups, citizens conference...) available, but
- How to deal with business and corporate secrets?
- How to assess immature or even embryonic systems?
- How to address complexity of technology vs. understanding of laypeople?
- Consultation fatigue

Success factors

- Clear commitment by the management to consider results
- Early timing, sufficient time and resources
- Avoid bias in selection of stakeholder (representatives)
- Good communication (about the features of the system to be assessed; between the participants; about the results of the consultation).
michael.friedewald@isi.fraunhofer.de
@MFriedewald / @ForumPrivatheit
www.forum-privatheit.de
Hands-On

• Discuss the cases in groups
  ▪ Identify risks for individuals
  ▪ Assess risks

• Time for discussion approx. 20 Mins.
• Presentation of results approx. 10 Mins.
• Further discussions
Thank you for your attention!

Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein
marit.hansen@datenschutzzentrum.de

Felix Bieker, LL.M. (Edinburgh)
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
fbieker@datenschutzzentrum.de