Data Protection by Design
- how to fulfil European demands and provide trustworthy services

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany

Datasikkerhedskonference 2017
Copenhagen, 21 March 2017

Setting of ULD

• Data Protection Authority (DPA) for both the public and private sector
• Also responsible for freedom of information

Source: en.wikipedia.org/wiki/Schleswig-Holstein
Overview

• Data Protection ↔ IT Security
• General Data Protection Regulation
• Data Protection by Design and by Default
• Standard Data Protection Model
• Conclusion

Data Protection is mainly about data

human beings with their rights

Questions to consider in system design:
• Effects on individuals?
• Effects on society?
Imbalance in power $\Rightarrow$ data protection necessary

Important: Perspective of the individual

Data protection: more than IT security

Data processing $\Rightarrow$ interference with fundamental rights

IT security: The adversary is Eve (or Mallory).

Data protection: The adversary is Bob! (Well, at least he is one of them.)
Overview

• Data Protection ↔ IT Security
• General Data Protection Regulation
• Data Protection by Design and by Default
• Standard Data Protection Model
• Conclusion

EU General Data Protection Regulation - A game changer

• Market location principle (Art. 3 GDPR)
• Data protection by design (Art. 25(1) GDPR)
• Data protection by default (Art. 25(2) GDPR)
• Data protection impact assessment (Art. 35 GDPR - “rights and freedoms of natural persons”)
• Certification (Art. 42+43 GDPR)
• Fines & sanctions (Art. 83+84 GDPR)
• Courts

Source: Johan Aulin

Powerful toolbox, but only as good as its implementation
Recital 4

The processing of personal data should be designed to serve mankind. […]
**Data Protection by Design & by Default**

- **Art. 25 GDPR**

  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, [...]

- **Targeted at controllers + data processors**

  Producers of IT systems “should be encouraged” (Rec. 78)

- **Objective:** to design systems + services from early on, for the full lifecycle ...
  
  a) ... in a data-minimising way
  
  b) ... with the most data protection-friendly pre-settings

---

**Data protection by design**

**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.
Conditions “state of the art” and “the cost of implementation”?  

Identical wording in Art. 32 “Security of processing”

Article 25

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures designed to implement data protection principles, such as data minimisation, necessary safeguards into the processing in order to meet the requirements of data subjects.

2. The controller and the processor shall implement appropriate technical and organisational security measures for the processing of personal data, the nature, scope, context of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, which shall include, in particular, measures to ensure security appropriate to the risk, the state of the art, the costs of implementation and by pretending to the nature of the data and to the categories of data subjects.

3. An approved certification mechanism pursuant to Article 50 may be used in order to determine whether the requirements set out in paragraphs 1 and 2 of this Article are met.

Article 32

Security of processing

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context of processing, and the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure security appropriate to the risk, including, in particular:

(i) the pseudonymisation and encryption of personal data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing services;

(iii) the ability to restore the availability and access to personal data in a timely manner in the event of technical incident;

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are potential to processing operations, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting on behalf of the controller or processor.

On EU level nothing new, see Data Protection Directive 95/46/EC

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and
Conditions “state of the art” and “the cost of implementation”?

_Not_ contained in Art. 24 GDPR: responsibility

**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.

2. Where proportionate in relation to processing activities, the measures for implementation of appropriate data protection policies by the controller.

3. Adherence to approved codes of conduct as referred to in Article 25 referred to in Article 42 may be used as an element by which to demonstrate controller.

In case of high risks: “State of the art” and “the cost of implementation” must not be used as excuse. (see Art. 36 Prior Consultation)

---

**Data protection by default**

**Article 25 Data protection by design and by default**

(2) 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. 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.

Related to the “purpose limitation” principle (Art. 5)

Social network clause
How? – Some hints in Recital 78

• Goal: to demonstrate compliance with the GDPR

• Adopting internal policies and implementing measures for data protection by design & by default

• Data minimisation

• Early pseudonymisation

• Transparency

• Monitoring of data processing by the data subject

• Expandable security – not “one size fits all”

• Data protection by design & by default in public tenders

• If Art. 25 (+ Art. 32) is ignored, administrative fines possible
  (Art. 83 GDPR: up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover)

Overview

• Data Protection ↔ IT Security

• General Data Protection Regulation

• Data Protection by Design and by Default

• Standard Data Protection Model

• Conclusion
Protection goals: more than IT security

Confidentiality + Unlinkability + Data minimisation

Integrity

Unlinkability

Intervenability

Transparency

Availability

classical IT security protection goals*)

*) From the data subject’s perspective

Data Protection by Design

Standard Data Protection Model

- Determination of the necessary level of protection ("normal", "high", "very high")
- Identification of risks and proper safeguards
- Protection goals as structure + for same understanding

- Model recommended by the German DPAs; suitable for
  - Supervision
  - Audits
  - Data Protection Impact Assessment
  - Data Protection by Design and by Default

- Work for 2017++: catalogues of reference protection measures
- Envisioned: repositories with info on maturity, conditions etc.
Standard Data Protection Model

To be integrated in the Data Protection Management System of the controller

Data protection by design - controller’s perspective in 2017

Minimum:

- Low-key interpretation of the legal rules
- Documentation of internal policies and measures
- Awaiting requirements of supervisory bodies
- Awareness of responsibility (CEO; at best supported by Data Protection Officer)

For “optimum” on top:

- Acting proactively
- Knowing and extending solution space
- Striving for certification
- Implementing a data protection management system for entire lifecycle
- Interacting with other actors and disciplines for improving technologies and workflows
BTW:

All translations are equivalent, aren’t they?

- [FR] Article 25: Protection des données *dès la conception* et protection des données par défaut
- [ES] Artículo 25: Protección de datos *desde el diseño* y por defecto
- [NL] Artikel 25: Gegevensbescherming door *ontwerp* en door standaardinstellingen
- [DA] Artikel 25: Databeskyttelse gennem *design* og databeskyttelse gennem standardindstillinger
- [SV] Artikel 25: *Inbyggt* dataförsvar och dataförsvar som standard
- [DE] Artikel 25: Datenschutz durch *Technikgestaltung* und durch datenschutzfreundliche Voreinstellungen

---

**Overview**

- Data Protection ↔ IT Security
- General Data Protection Regulation
- Data Protection by Design and by Default
- Standard Data Protection Model
- Conclusion
Conclusion

• Data protection by design and by default
  ▪ Demanded by the General Data Protection Regulation
  ▪ With focus on the perspective of the individuals
  ▪ Necessary for trustworthy systems

• For controllers:
  ▪ Be risk-aware
  ▪ Be compliant
  ▪ Re-think your concepts, processes & implementations
  ▪ Demand the same from your processors

• “Privacy by disaster” is not an option – get help:
  Data Protection Officers + Commissioners

Data Protection Management Systems

Tak for opmærksomheden!

Marit Hansen
ULD, Holstenstr. 98, 24103 Kiel, Germany
marit.hansen@datenschutzzentrum.de
References


