

Data Protection by Design and by Default

Marit Hansen

Data Protection Commissioner
Schleswig-Holstein, Germany

Data Protection in the Digital Era Conference
İstanbul Üniversitesi Hukuk Fakültesi
16 April 2021



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Setting of ULD

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

Schleswig-Holstein	
State of Germany	
Flag	Coat of arms
<p>Coordinates: 54°28'12"N 9°30'50"E</p>	
Country	Germany
Capital	Kiel
Government	
• Body	Landtag of Schleswig-Holstein
• Minister-President	Daniel Günther (CDU)
• Governing parties	CDU / Greens / FDP
• Bundesrat votes	4 (of 69)
Area	
• Total	15,763.18 km ² (6,086.20 sq mi)
Population (2016-12-31) ^[1]	
• Total	2,881,926
• Density	180/km ² (470/sq mi)

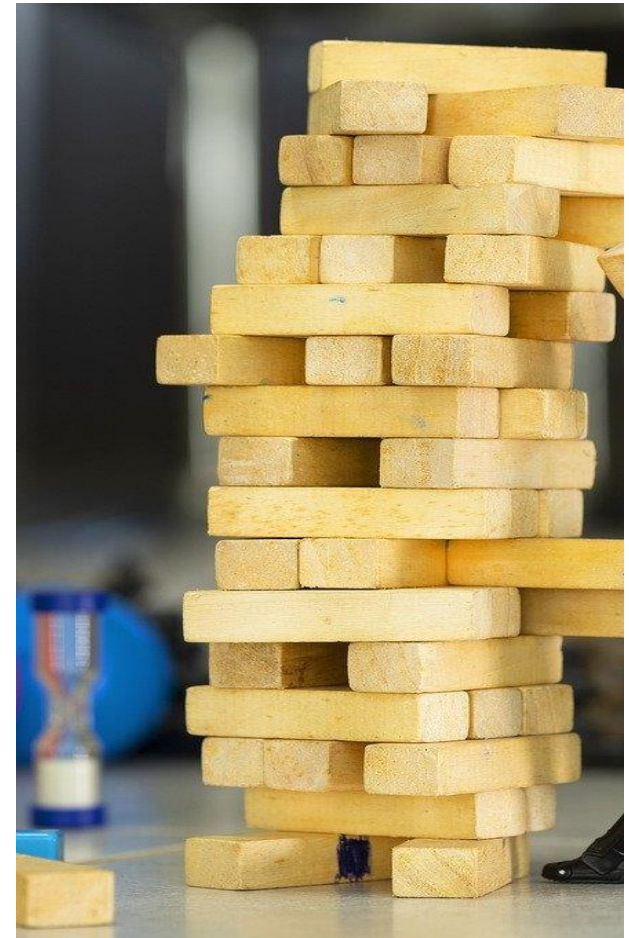
Berlin

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



Overview

- Data Protection – what's that?
- General Data Protection Regulation (GDPR) in a nutshell
- Data Protection by Design and by Default
- How to?
- Conclusion



Source: Johnny Gutierrez
via Pixabay

Imbalance
in power



data protection
necessary

Important:

Perspective of
the individual

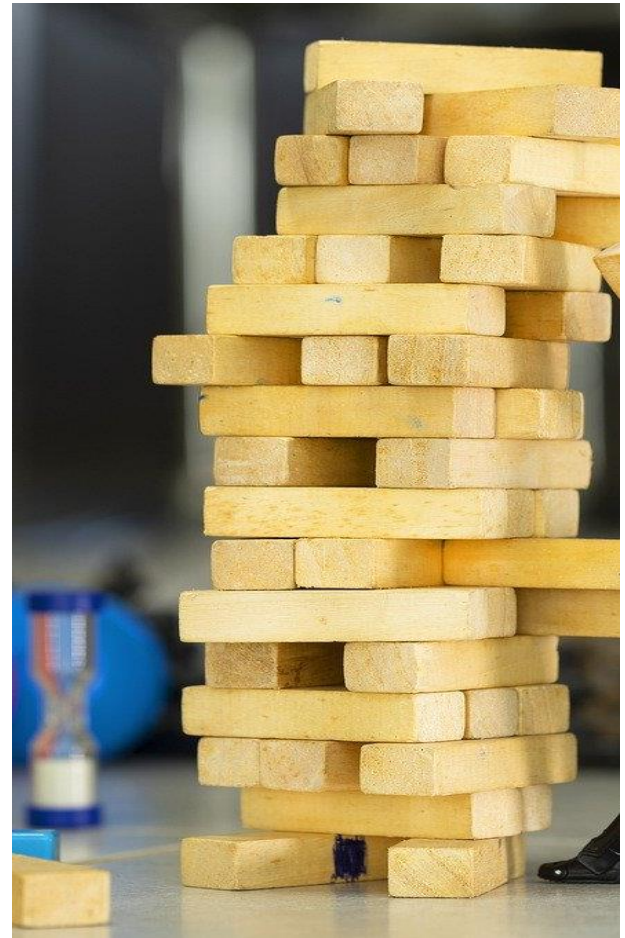
More than
security of
personal data



Source: beludise via Pixabay

Overview

- Data Protection – what's that?
- **General Data Protection Regulation (GDPR) in a nutshell**
- Data Protection by Design and by Default
- How to?
- Conclusion



Source: Johnny Gutierrez
via Pixabay

General Data Protection Regulation

- Idea: **One for All**
and
All for One
- Objective:
real harmonisation,
"level playing field"
- But:
 - 70 opening clauses
("variables" for Member States)
 - Enforcement problems,
esp. global players




https://upload.wikimedia.org/wikipedia/commons/8/85/Unus_pro_omnibus%2C_omnes_pro_uno.jpg

GDPR as "Game Changer" (?)



Source: Astryd_MAD via Pixabay

Powerful **toolbox**
if applied
appropriately

- **Market location principle** (Art. 3 GDPR) 
- **Responsibility** (Art. 24 GDPR)
- **Data protection by design** (Art. 25(1) GDPR) 
- **Data protection by default** (Art. 25(2) GDPR)
- **Security** (Art. 32 GDPR)
- **Data protection impact assessment**
(Art. 35 GDPR – "Rights and freedoms of natural persons")
- **Certification** (Art. 42+43 GDPR)
- **Fines & sanctions** by Data
Protection Commissioners (Art. 83+84 GDPR)
- **Courts**

Data Protection Principles – Art. 5 GDPR

Art. 5 GDPR – Principles relating to processing of personal data

Design requirements

(1)

- a) **Lawfulness, fairness** and transparency
- b) Purpose limitation
- c) Data minimisation
- d) Accuracy
- e) Storage limitation
- f) Integrity and confidentiality (~ security)

(2) Accountability

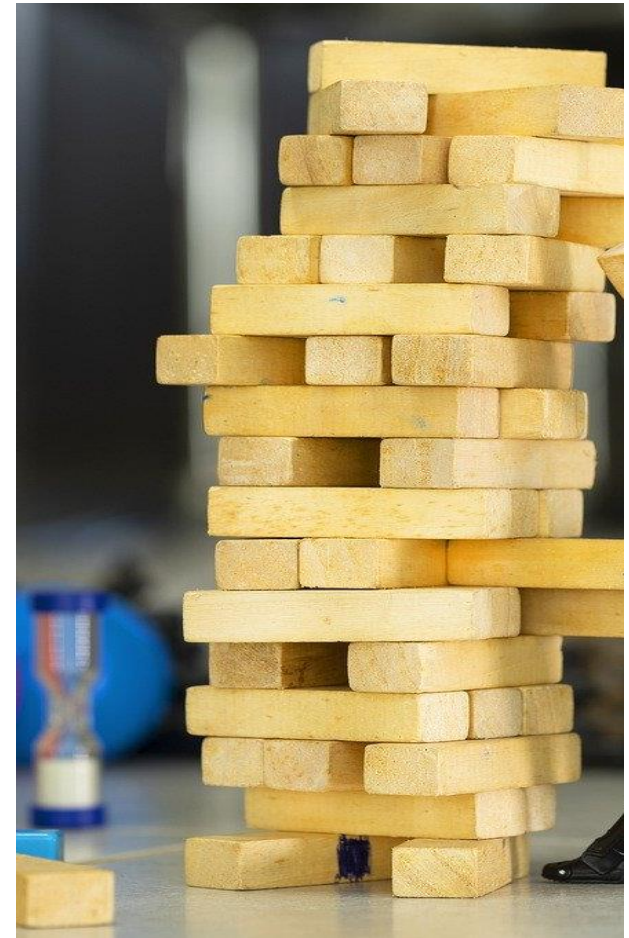
Lawfulness is precondition, e.g.:

- Consent
- Contract
- Legal basis
- Legitimate interest

Fairness as common theme

Overview

- Data Protection – what's that?
- General Data Protection Regulation (GDPR) in a nutshell
- **Data Protection by Design and by Default**
- How to?
- Conclusion



Source: Johnny Gutierrez
via Pixabay

Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers
- 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**

Art. 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**, [...] which are designed to implement data-protection principles [...], in an effective manner [...]

Data Protection by Design & by Default

- Art. 25 GDPR
- Targeted at controllers
- Producers of IT systems “should be encouraged” (Rec. 78)

Art. 25 Data Protection by Design and by Default

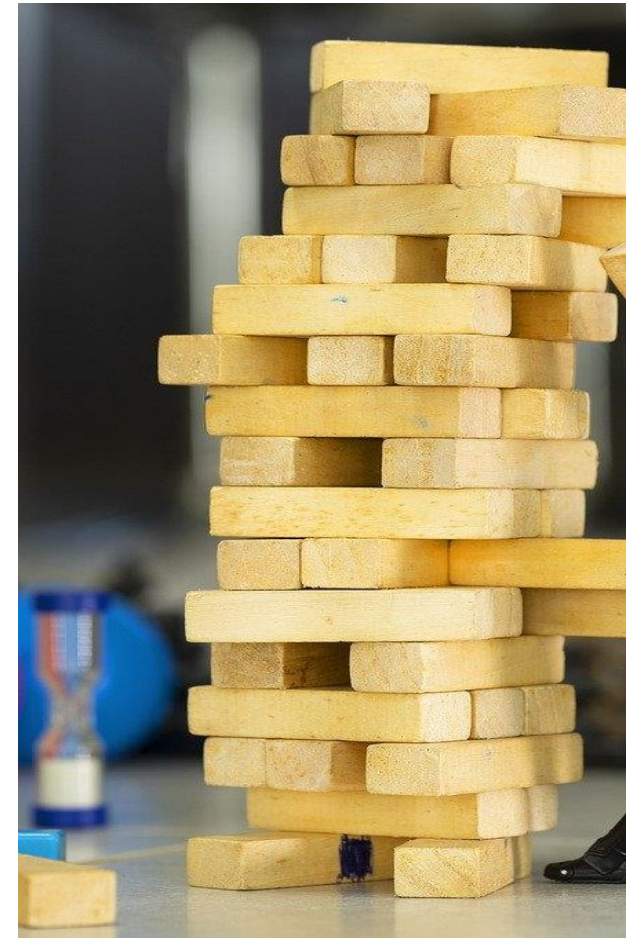
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [...]

- 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

Overview

- Data Protection – what's that?
- General Data Protection Regulation (GDPR) in a nutshell
- Data Protection by Design and by Default
- **How to?**
- Conclusion



Source: Johnny Gutierrez
via Pixabay

Data Protection Principles – Art. 5 GDPR

Art. 5 GDPR – Principles relating to processing of personal data

Technical and organisational measures

Design requirements

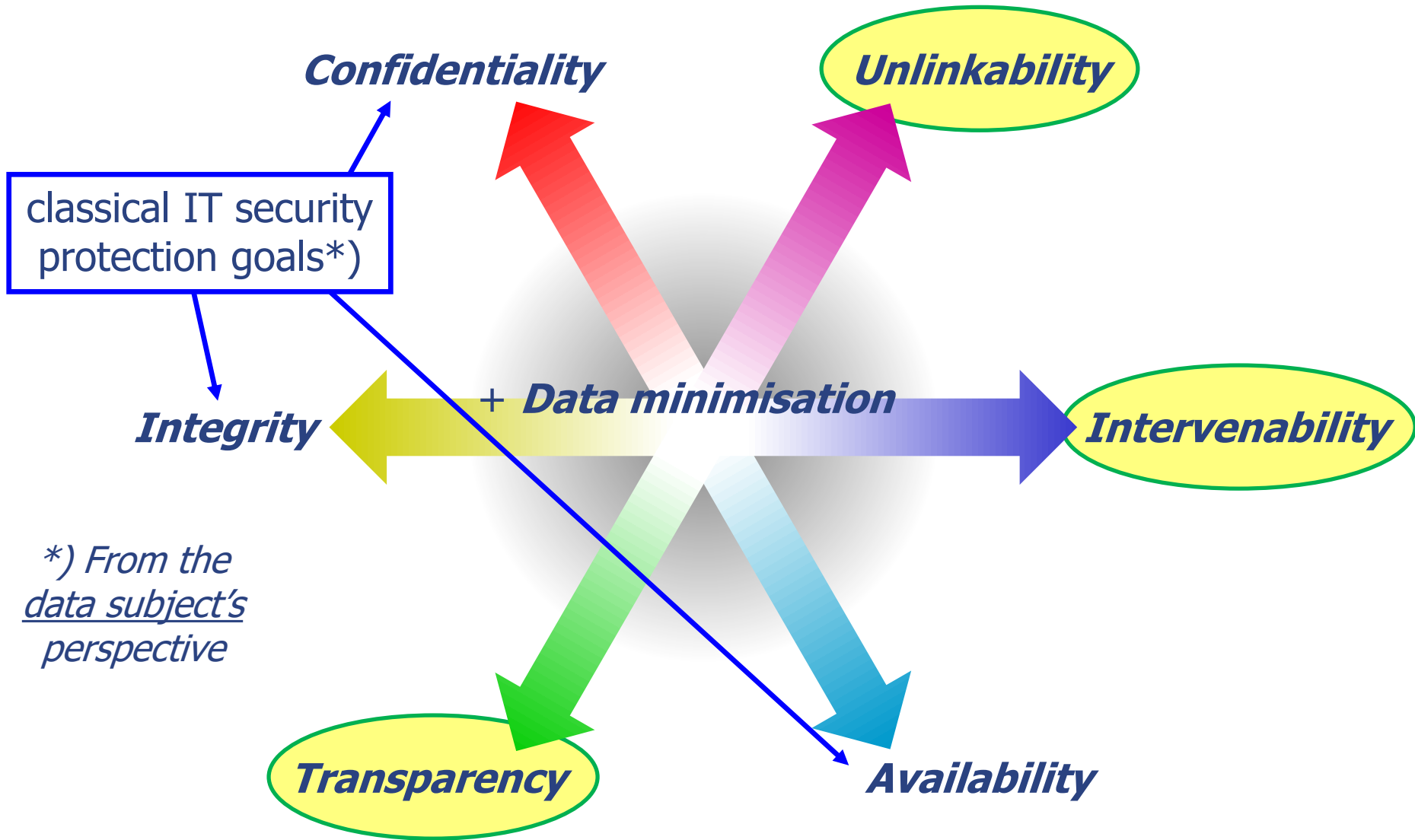
(1)

- a) Lawfulness, fairness and transparency
- b) Purpose limitation
- c) Data minimisation
- d) Accuracy
- e) Storage limitation
- f) Integrity and confidentiality (~ security)



(2) Accountability

Standard Data Protection Model



**) From the data subject's perspective*

Data minimisation + Unlinkability

Limit data collection, separation of domains, purpose binding, encryption, anonymisation, pseudonymisation



Source: ivanacoi via Pixabay



How to?

Scrutinise the processing, check "starting point" defaults

Transparency

DELETING FROM EMP

Goal: comprehensibility & auditability

Source: geralt via Pixabay



E.g. help desk, deactivation, rectification, objection, legal redress, no automated decisions/reversal of decisions, liability ...

Please, help me!



Source: geralt via Pixabay



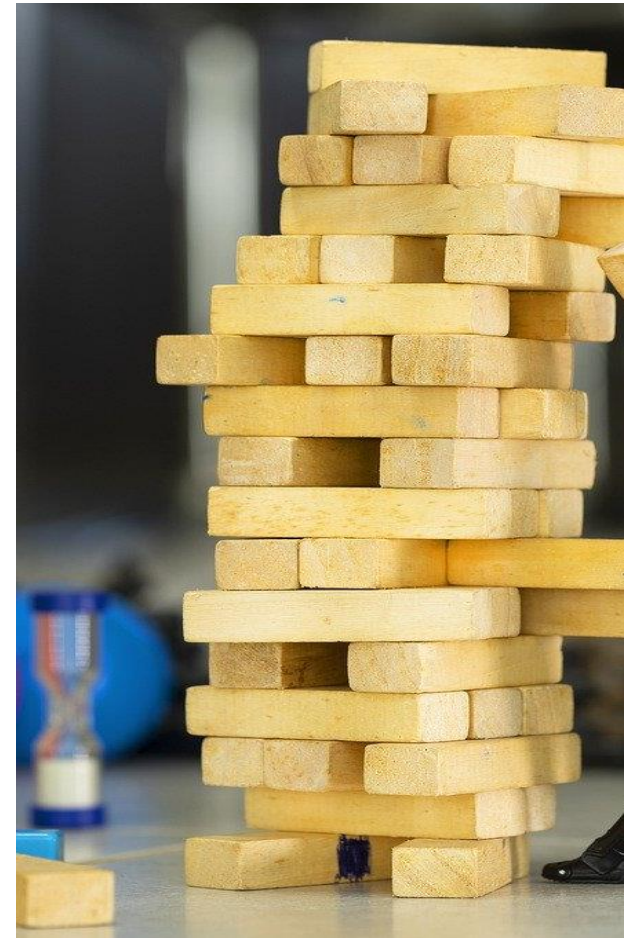
Intervenability

Main goals:

- **Fairness**
- Mitigating the **risk** for the rights and freedoms of natural persons

Overview

- Data Protection – what's that?
- General Data Protection Regulation (GDPR) in a nutshell
- Data Protection by Design
- Data Protection by Default
- **Conclusion**



Source: Johnny Gutierrez
via Pixabay

Challenge: Building sustainable & resilient systems without undesired side effects



Source: Johnny Gutierrez via Pixabay

Conclusion

- Data protection by design and by default
 - Demanded by the GDPR
 - Thereby to be demanded by controllers
- Sanctions because of infringing Art. 25 GDPR are still rare
- Ongoing work
 - Not a standard, yet
 - Developers need help and examples for good solutions



Source: congerdesign via Pixabay

Further information

- Datatilsynet (Norwegian Data Protection Authority):
Software development with Data Protection by Design and by Default, 28.11.2017,
<https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/>
- Jaap-Henk Hoepman: Privacy Design Strategies (The Little Blue Book), 2018-2019,
<https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>
- European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 20.11.2019,
https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en
- Standard Data Protection Model: A method for Data Protection advising and controlling on the basis of uniform protection goals, 2020 (last revision: V 2.0b),
https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf
- European Union Agency for Cybersecurity (ENISA) on Data Protection:
<https://www.enisa.europa.eu/topics/data-protection>