# How to implement data protection – fulfilling the (not so new) requirement of the GDPR

Dr. h.c. Marit Hansen
State Data Protection Commissioner
of Schleswig-Holstein, Germany

Hamburg, 13 September 2024

Plattform Privatheit

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

## Overview



**Schleswig-Holstein**

State of Germany

Flag

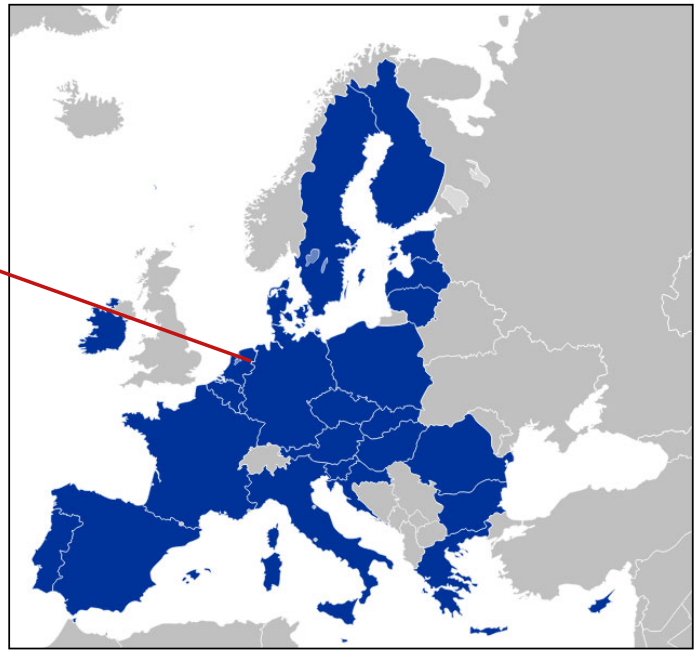
Coat of arms

Coordinates: 54°28′12″N 9°30′50″E

| | |
|---|---|
| **Country** | Germany |
| **Capital** | Kiel |
| **Government** | |
| • **Body** | Landtag of Schleswig-Holstein |
| • **Minister-President** | Daniel Günther (CDU) |
| • **Governing parties** | CDU / Greens |
| • **Bundesrat votes** | 4 (of 69) |
| **Area** | |
| • **Total** | 15,763.18 km² (6,086.20 sq mi) |

# *Setting of ULD*

- State Data Protection Authority (DPA) for both the public and private sector
- Located in Kiel, Germany



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

Source: Kolja21 via Wikimedia

## Overview



Imbalance in power ⇨ data protection necessary

Important: Perspective of the individual

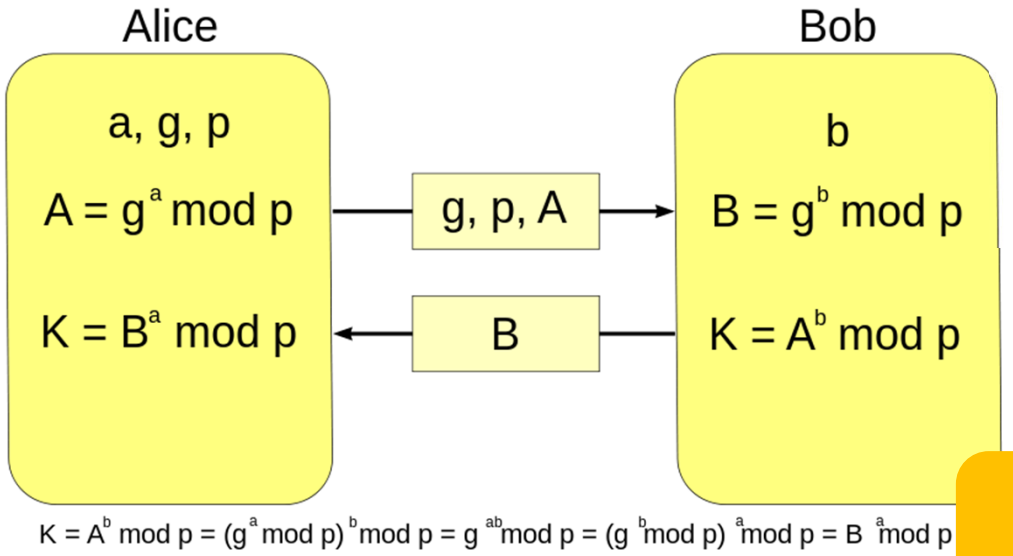
More than security of personal data


Source: beludise via Pixabay

**Overview**



# *Perspective: Alice & Bob*




$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Data processing: interference with fundamental rights

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

Data Protection: The adversary is Bob!
(At least: Bob is one of them.)

**Overview**



# *General Data Protection Regulation (GDPR)*

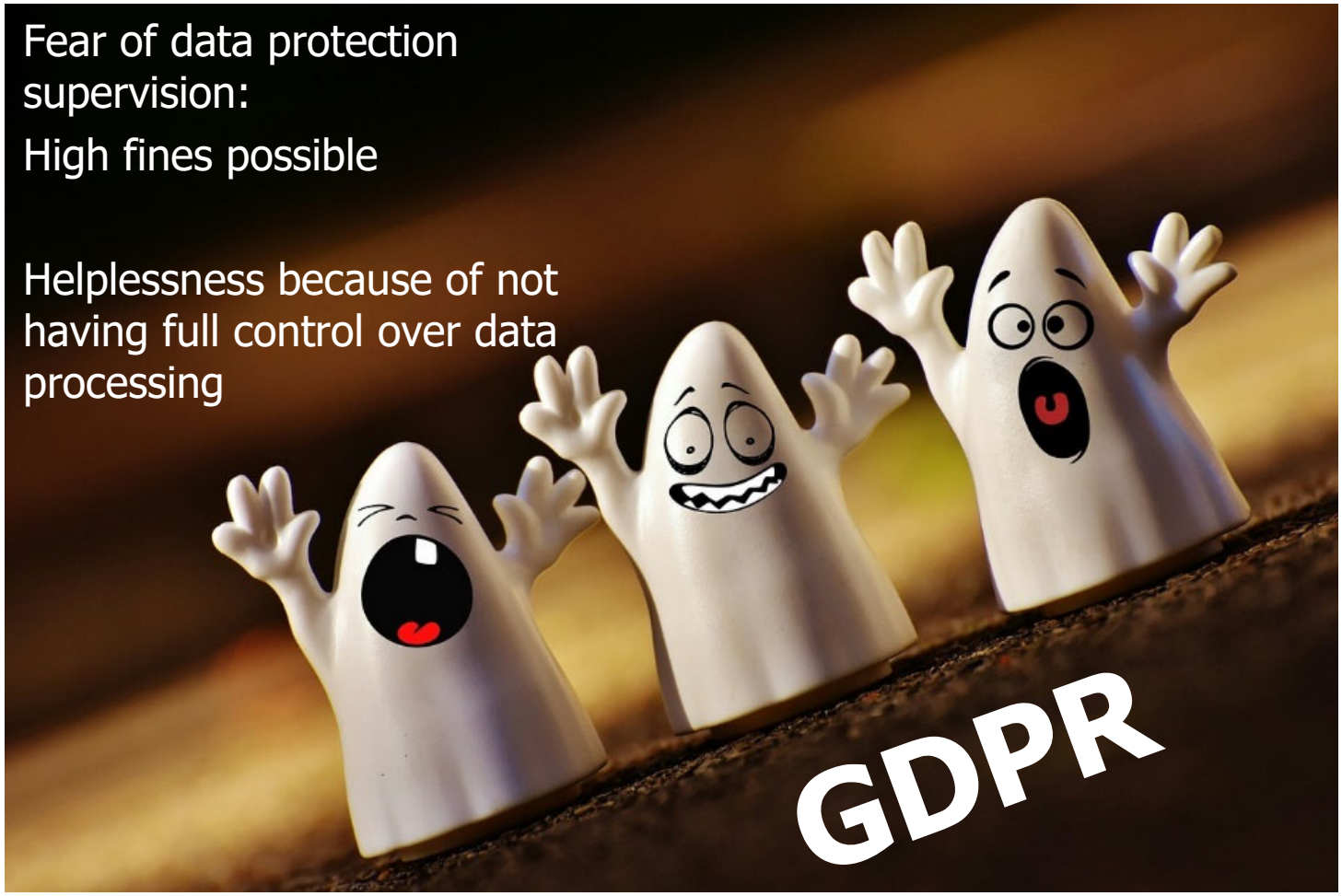
- Idea: One for All
  and
  All for One
- Objectives:
  - Real harmonisation, "level playing field"
  - Technology-neutral
- In force since May 2018


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

**Overview**



# *Nightmare GDPR?*




 Source: Alexas_Fotos via Pixabay

# *GDPR as "Game Changer" (?)*

- Principle "Data Protection by Design" – but enforcement issues
  [Art. 25 GDPR]
- Fines & sanctions by Data Protection Commissioners
  [Art. 58, Art. 83 GDPR]
- Courts


Source: Astryd_MAD via Pixabay

Powerful toolbox
if applied appropriately

# *Art. 5 GDPR - Principle*

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

Common theme: Fairness

Design requirements

(1)

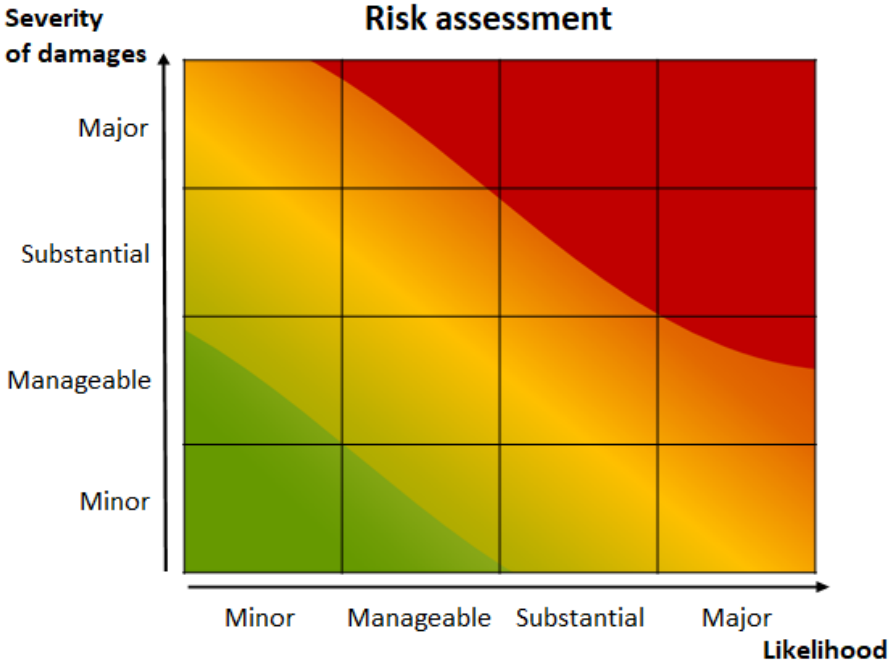
a) Lawfulness, fairness and transparency
b) Purpose limitation
c) Data minimisation
d) Accuracy
e) Storage limitation
f) Integrity and confidentiality (~ security)

(2) Accountability

**Overview**



# *Trustworthy? The GDPR's notion of risk*


Risk for the rights and freedoms of natural persons – see EU Charter of Fundamental Rights

Source: 1) Internet Meme,
2) DSK on risk (Kurzpapier Nr. 18)

**Overview**



# *GDPR demands risk mitigation*

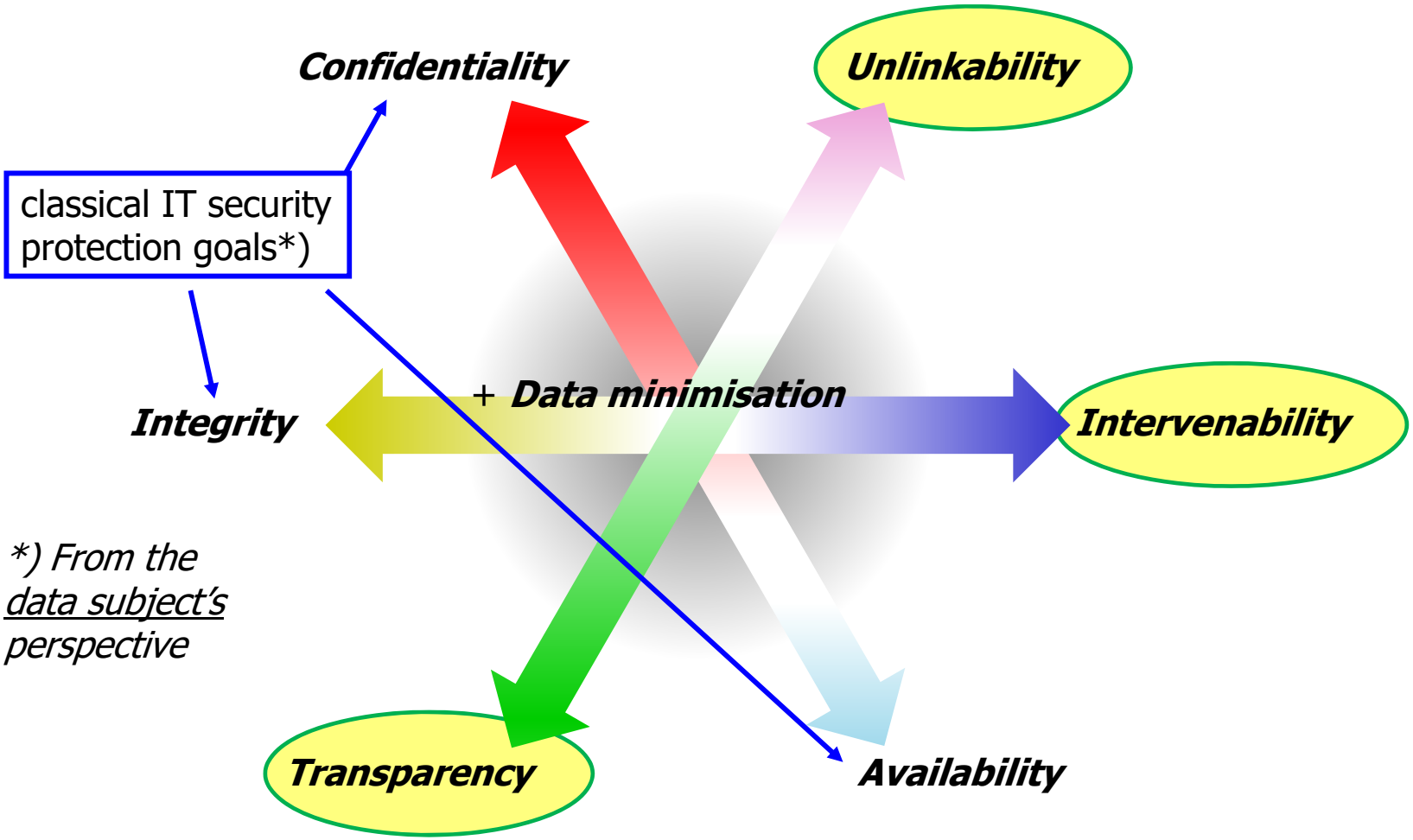
High risk – not lawful without prior risk mitigation (design, technical and organisational measures)

Trustworthiness through appropriate built-in measures and checkability

**Overview**



# Standard Data Protection Model




https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

# *Confidentiality*

## Implementation Techniques:

- Data Encryption
  - in transit (TLS, HTTPS, SSH, …)
  - at rest (PGP, S/MIME, disk encryption …)
  - …
- Data Segregation
  - Secret Sharing, Secure Multiparty Computations
  - Onion Routing
- Access Control Enforcement

Icon: Gear Icons created by Freepik - Flaticon

**Overview**



# *Integrity*

## Implementation Techniques:

- Digital Signatures
- Hash Values
- Access Control Enforcement
- Watchdogs / Canaries

Icon: Gear Icons created by Freepik - Flaticon

**Overview**



# *Availability*

## Implementation Techniques:

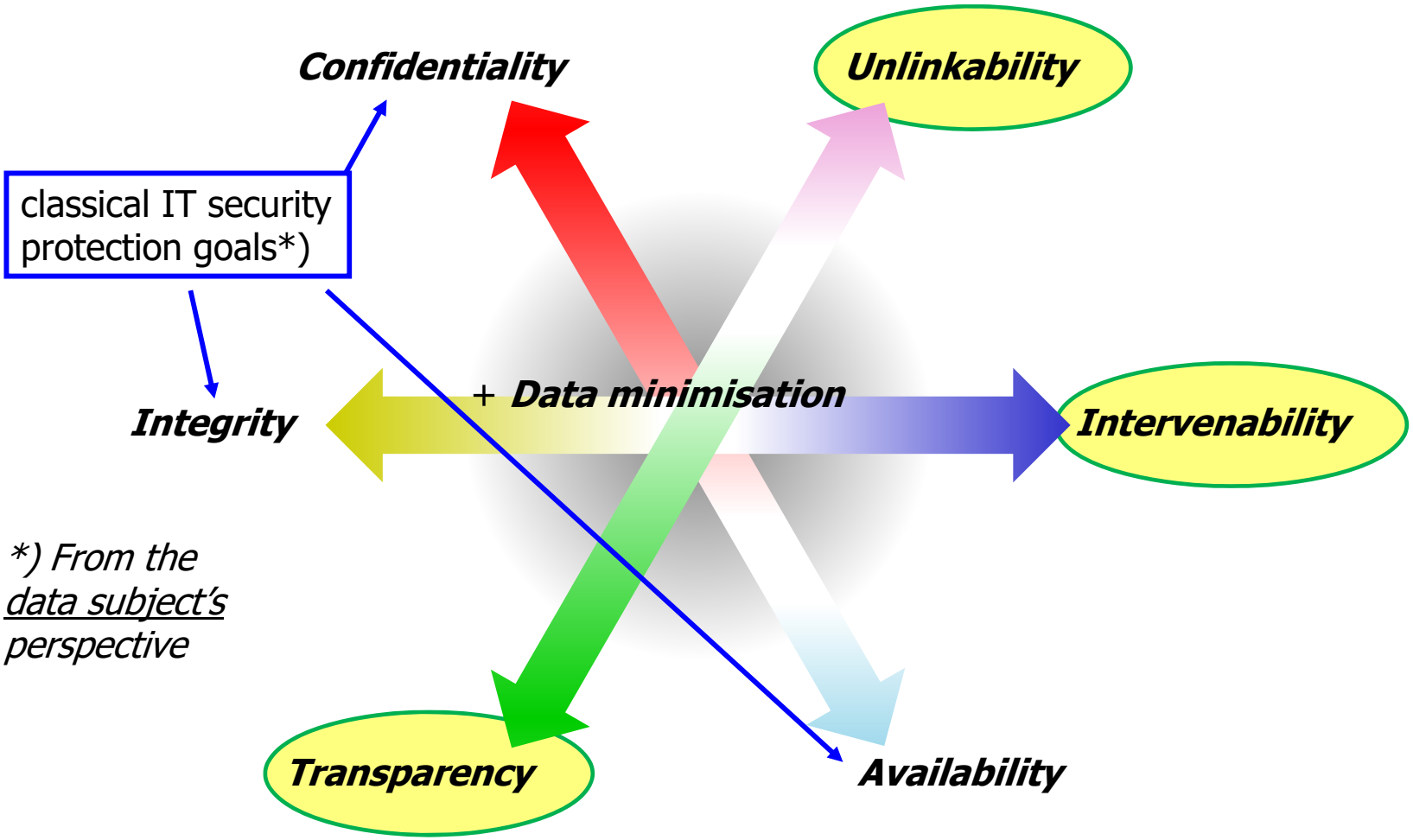
- Backups
- Load Balancers
- Redundant Components
- Avoidance of Single-Points-of-Failure
- Watchdogs / Canaries

Icon: Gear Icons created by Freepik - Flaticon

**Overview**



# Standard Data Protection Model




https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

**Overview**



## *Unlinkability*

**"The protection goal of**

## ***Unlinkability***

**is defined as the property that personal data cannot be linked across domains that are constituted by a common purpose and context."**

# *Unlinkability*

*… in other words:*

- Necessity / Need-to-Know
- Purpose Binding
- Separation of Power
- Unobservability

# *Unlinkability*

## Implementation Techniques:

- Data Avoidance / Reduction
- Access Control Enforcement
- Generalization
  - Anonymization / Pseudonymization
  - Abstraction
  - Derivation
- Separation / Isolation
- Avoidance of Identifiers

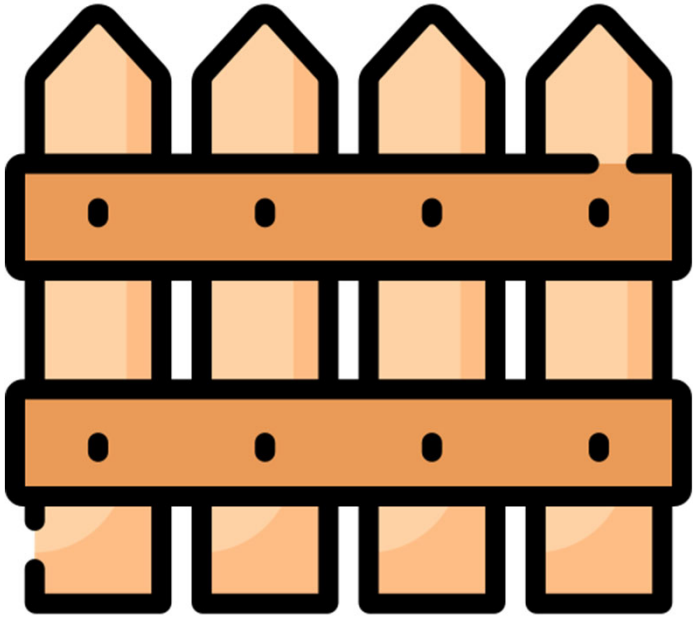
Icon: Gear Icons created by Freepik - Flaticon

**Overview**



# *Unlinkability*

Think of it as …



Icon: Fence Icons created by Freepik - Flaticon

**Overview**



# *Transparency*

**"The protection goal of**

## *Transparency*

**is defined as the property that all processing of personal data – including the legal, technical, and organizational setting – can be understood and reconstructed at any time."**

# *Transparency*

*... in other words:*

- Openness
- Accountability
- Documentation
- Reproducibility
- Notice (and Choice)
- Auditability
- Full-Disclosure

**Overview**



# *Transparency*

## Implementation Techniques:

- Logging and Reporting
- User Notifications
- Documentation
- Status Dashboards
- Privacy Policies
- Transparency Services for Personal Data
- Data Breach Notifications

Icon: Gear Icons created by Freepik - Flaticon

**Overview**



# *Transparency*

Think of it as …

Icon: Define Icons created by Freepik - Flaticon

**Overview**



# *Intervenability*

**"The protection goal of**

## ***Intervenability***

**is defined as the property that intervention is possible concerning all ongoing or planned processing of personal data."**

# *Intervenability*

*… in other words:*

- Self-Determination
- User Controls
- Rectification or Erasure of Data
- (Notice and) Choice
- Consent Withdrawal
- Claim Lodging / Dispute Raising
- Process Interruption

# *Intervenability*

## Implementation Techniques:

- Configuration Menu
- Help Desks
- Stop-Button for Processes
- Break-Glass / Alert Procedures
- Manual Override of Automated Decisions
- External Supervisory Authorities (DPAs)

Icon: Gear Icons created by Freepik - Flaticon

**Overview**



# *Intervenability*

Think of it as …

Icon: Remote Control Icons created by Freepik - Flaticon

# *Data minimisation – how exactly? E.g. video surveillance*

Many possible measures for data minimisation:
when, which data, for which analyses, … really necessary?

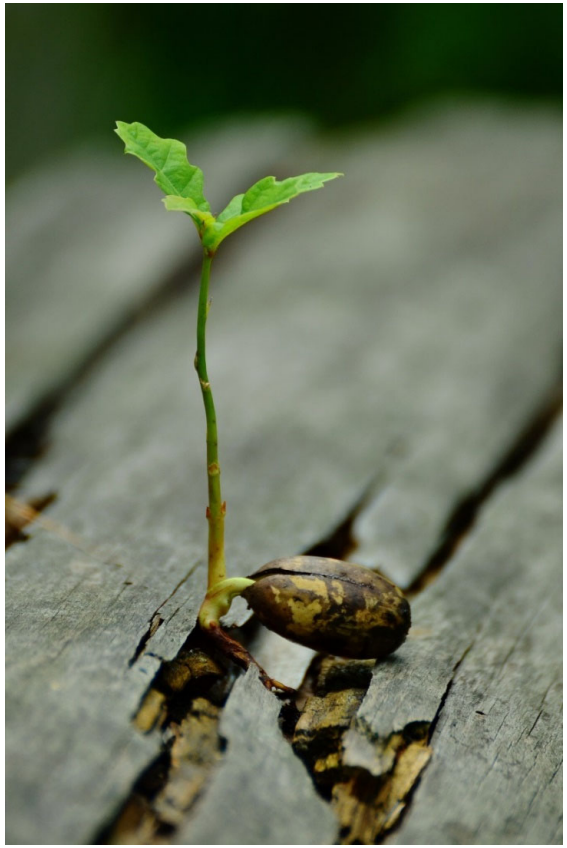

Foto: Markus Hansen

**Overview**



# *Conclusion*

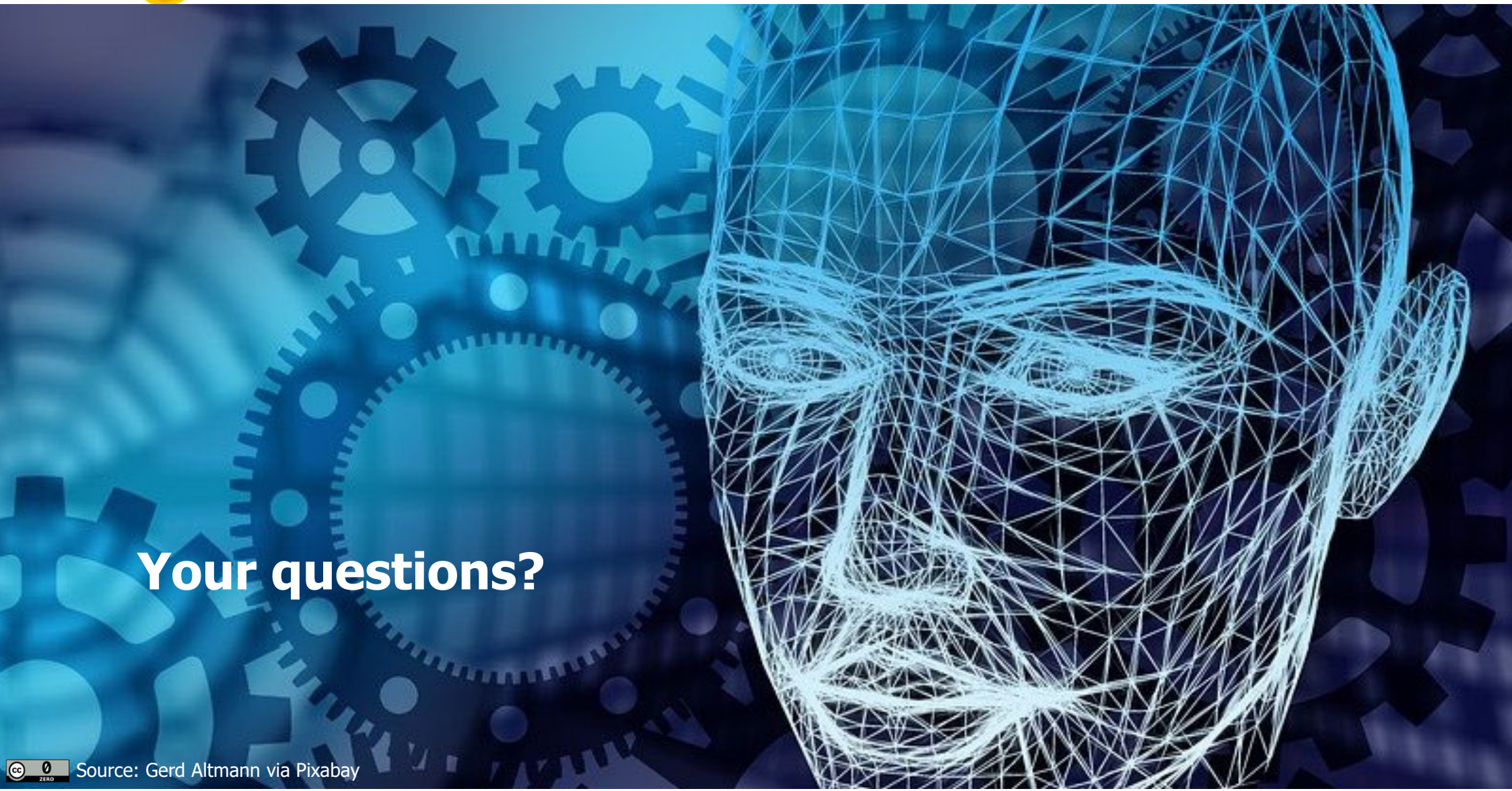
- The GDPR is there – and won't go away.
- It's all about risk mitigation
- Security: only one aspect
- Demand built-in data protection from vendors, service providers and developers
- Data Protection Authorities can help …
- … and the Standard Data Protection Model



Source: congerdesign via Pixabay

# Further Reading


- Datatilsynet: Software Development with Data Protection by Design and by Default, 2017, https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/
- DSK: SDM V3.0, 2022, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/
- EDPB: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, V2.0, 2020, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
- EDPB: Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, V2.0, 2023, https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf
- ENISA: Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, 2016, https://www.enisa.europa.eu/publications/pets
- ENISA: Engineering Personal Data Sharing, January 2023, https://www.enisa.europa.eu/publications/engineering-personal-data-sharing
- Future of Privacy Forum: Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR, 2023, https://fpf.org/resource/new-fpf-report-unlocking-data-protection-by-design-and-by-default-lessons-from-the-enforcement-of-article-25-gdpr/
- Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, IWPE, 2015, https://ieeexplore.ieee.org/ielx7/7160794/7163193/07163220.pdf
- Hoepman: Privacy Design Strategies, 2018, https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf
- Veale/Binns/Ausloos: When Data Protection by Design and Data Subject Rights Clash, in: IDPL 8 (2) 2018, 105, https://doi.org/10.1093/idpl/ipy002



# Your questions?