AnoMed

Funded by Bundesministerium für Bildung und Forschung

Funded by the European Union
NextGenerationEU

# *Legal Aspects of Anonymization and Pseudonymization*

--

# Module 1: Overview of the GDPR

Bud P. Bruegger

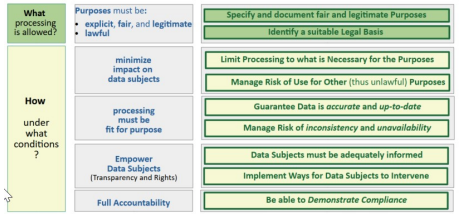
ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

# Outline Module 1

## Overview of the GDPR

- **Intro and Context**
- **Requirements of the GDPR** (Pt.of View of controllers)

- Approach: **GDPR as a Sequence of Steps:** (aka a **"map"**)




- **Structure** is useful for understanding and communicating:
  - define ***context*** or ***scope*** of a discussion (which of the risks?)
  - ***locate concepts*** "on the map" (principles, risks, ..)

# Simplifying Terminology

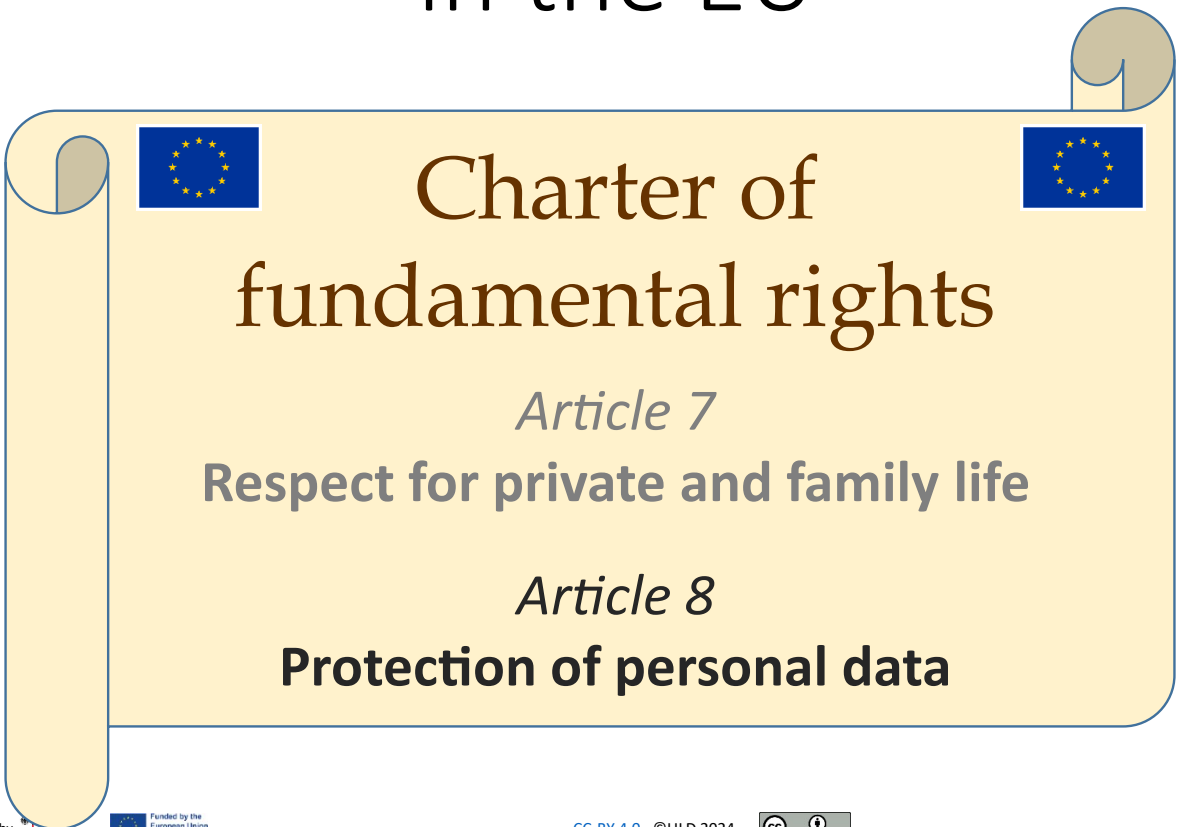
| | | |
|---|---|---|
| **processing** | → | always of **personal data** |
| **data** | → | always **personal data** |
| **use** | → | use of **personal data** |
| **Article** | → | of the **GDPR** |

etc.

# The *General Data Protection Regulation* or *GDPR* is the main data protection law of Europe

European Economic Area
(EU 27 + Norway, Iceland, Liechtenstein)

# Data Protection is a **fundamental right** in the EU



# Some History

Regulation replaces Directive

EU Directive

**Data Protection *Directive***

very similar obligations for controllers

EU Regulation

**General Data Protection *Regulation***

- Directives need **implementation in national law**
- Need for **harmonization across Member States**

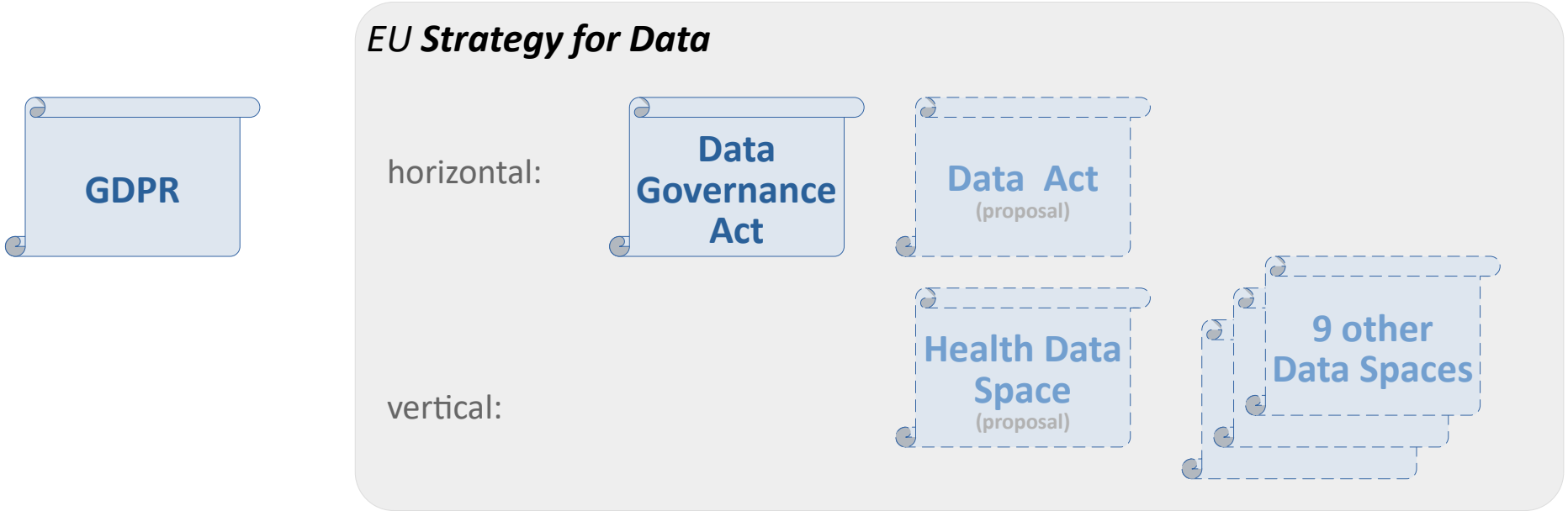
- **Directly applicable**
  No need for national implementations
- **EU harmonization foreseen**
  e.g. **E**uropean **D**ata **P**rotection **B**oard

1995 (in force)

2018 (in force)

time

# Context
## Relevant Laws



# Importance of the GDPR


**Article 1(3) DGA:**

**“In the event of a conflict** between this Regulation **and” [the GDPR] ,**

**[the GDPR] “shall prevail”.**

# Importance of the GDPR


**Article 1(3) DGA:**

**“In the event of a conflict** between this Regulation **and” [the GDPR] ,**

**[the GDPR] “shall prevail”.**

# Structure of the GDPR:
# **Legal Maxim**

**Often in the law**: *Allowed unless* (explicitly) *forbidden* (freedoms)

# Structure of the GDPR:
# Legal Maxim

**Often in the law**: *Allowed unless* (explicitly) *forbidden* (freedoms)

**GDPR**:

- **Default**: processing of Personal Data is **not permitted**
  - **unless**
    - fair, legitimate, **lawful**
    - **lawful** = "*explicitly permitted*": **fits one of six legal basis** (foreseen in Art. 6)

# Structure of the GDPR:
# Legal Maxim

**Often in the law**: *Allowed unless* (explicitly) *forbidden* (freedoms)

**GDPR**:

- **Default**: processing of Personal Data is **not permitted**
  - **unless**
    - fair, legitimate, **lawful**
    - **lawful** = "*explicitly permitted*": **fits one of six legal basis** (foreseen in Art. 6)

**Firewall**: (analogy)

- **Default Deny** (deny unless explicitly allowed)

# Structure of the GDPR:
# Legal Maxim

**Often in the law:** *Allowed unless* [illegible] (freedoms)

**GDPR:**

- **De**
  - **unles**

often used in Germany:

**“Verbot mit Erlaubnisvorbehalt”**

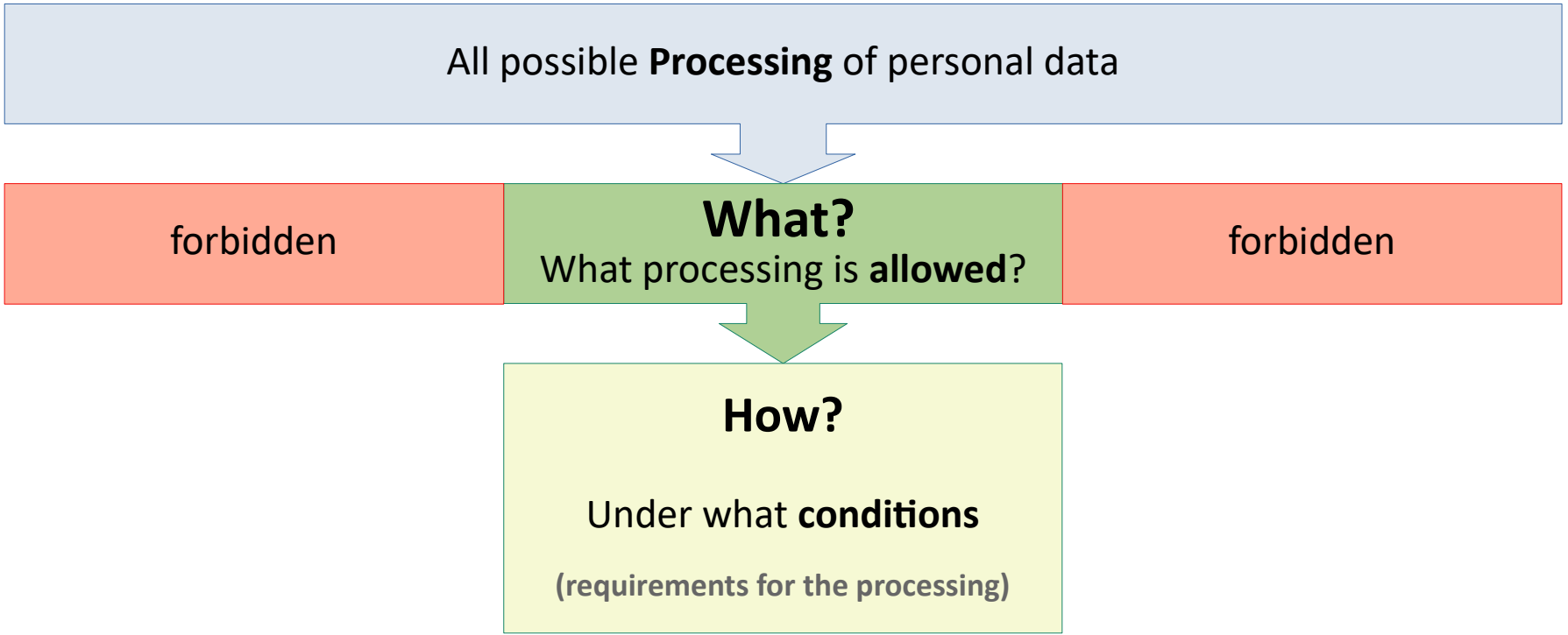
“ prohibition with the possibility of authorization”

[illegible] 6)

**Firewall:** [illegible]

- **Default Deny** [illegible] deny unless explicitly allowed)

# Basic Structure of the GDPR

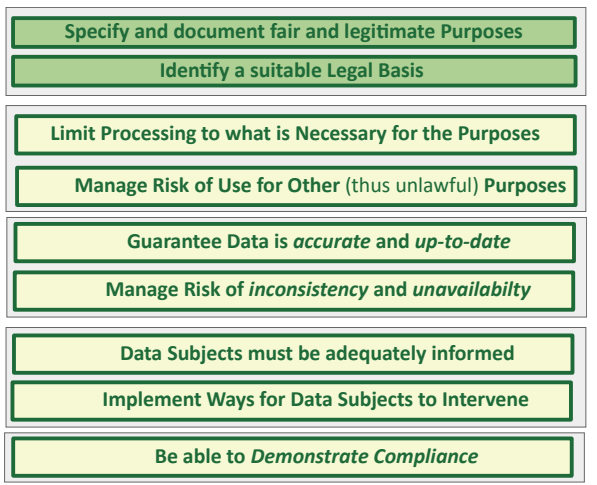


# Structure of the GDPR in more detail

- The following describes **What** and **How** in **more detail**..

# Structure of the GDPR in more detail

- The following describes **What** and **How** in **more detail**..
- ..as a flowchart



# Structure of the GDPR in more detail

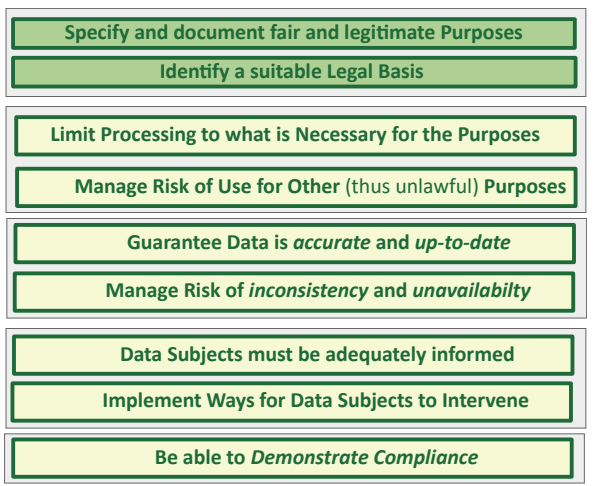
- The following describes **What** and **How** in **more detail**..
- ..as flowchart


***Disclaimer***: does **not**:

- guarantee compliance
- replace the GDPR

# Point of View

What a ***Controller*** has to do



**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**How**

under what conditions ?

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**Specify and document fair and legitimate Purposes**

**How**

under what conditions ?

**What** processing is allowed?

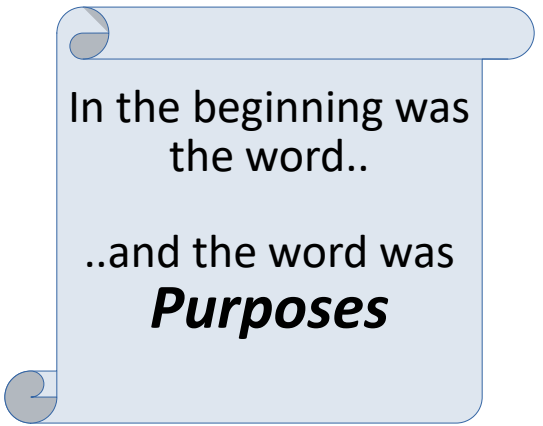
**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**Specify and document fair and legitimate Purposes**

**How**

under what conditions ?



**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**Specify and document fair and legitimate Purposes**

**How**

under what conditions ?

- **explicit**: documented in writing
- **fair**: (not well-defined)
- **legitimate:** compliant with..

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**Specify and document fair and legitimate Purposes**

**How**

under what conditions ?

- **explicit**: documented in writing
- **fair**: (not well-defined)
- **legitimate:** compliant with:
  - the **GDPR** (in letter and spirit)
  - **other laws**
  - the **values of society**
    (e.g., European **Charter of Fundamental Rights**)
  - the principles of **ethics** (e.g., **Research Ethics Commission**)

**What** processing is allowed?

**Purposes** must be:

- explicit, fair, and legitimate
- **lawful**

Specify and document fair and legitimate Purposes

**Identify a suitable Legal Basis**

**How**

under what conditions ?

**What** processing is allowed?

**Purposes** must be:

- explicit, fair, and legitimate
- **lawful**

Specify and document fair and legitimate Purposes

**Identify a suitable Legal Basis**

**How**

under what conditions ?

Art 6(1) defines ***lawful:***

***"Processing shall be lawful only if .. at least one of the following applies:"***

**What** processing is allowed?

**Purposes** must be:

- explicit, fair, and legitimate
- **lawful**

Specify and document fair and legitimate Purposes

**Identify a suitable Legal Basis**

**How**

under what conditions ?

Art 6(1) defines ***lawful:***

***"Processing shall be lawful only if .. at least one of the following applies:"***

exceptions to the prohibition

**What** processing is allowed?

**Purposes** must be:

- explicit, fair, and legitimate
- **lawful**

Specify and document fair and legitimate Purposes

**Identify a suitable Legal Basis**

**How**

under what conditions ?

Art 6(1) defines ***lawful:***

***"Processing shall be lawful only if .. at least one of the following applies:"***

- ***Consent*** *by data subject*
- ***Performance of a Contract*** *with the data subject*
- ***Legal Obligation***
- ***Vital Interests*** *of the data subject*
- ***Task*** *carried out* ***in the Public Interest***
- ***Legitimate Interests*** *of the* ***Controller***

**What** processing is allowed?

**Purposes** must be:

- explicit, fair, and legitimate
- **lawful**

Specify and document fair and legitimate Purposes

**Identify a suitable Legal Basis**

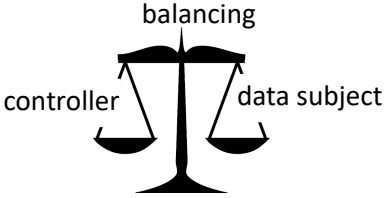
**How**

under what conditions ?

Art 6(1) defines ***lawful:***

***"Processing shall be lawful only if .. at least one of the following applies:"***

- ***Consent*** *by data subject*
- ***Performance of a Contract*** *with the data subject*
- ***Legal Obligation***
- ***Vital Interests*** *of the data subject*
- ***Task*** *carried out* ***in the Public Interest***
- ***Legitimate Interests*** *of the* ***Controller***
  - ***except where overridden by*** *the interests of the* ***data subject***
  - *→ "Balancing Test" necessary*



**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**minimize impact on data subjects**

**How**

under what conditions ?

**Specify and document fair and legitimate Purposes**

**Identify a suitable Legal Basis**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

**Limit Processing to what is Necessary for the Purposes**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

**Limit Processing to what is Necessary for the Purposes**

- **Processing for** the specified **Purposes is permitted**
- it always **impacts the Rights and Freedoms of Data Subjects**
- only what is really **necessary** is permitted

➔ Note: Central Role of **Purposes**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

**Manage Risk of Use for Other** (thus unlawful) **Purposes**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

**Manage Risk of Use for Other** (thus unlawful) **Purposes**

## Use for other Purposes:

- **Breach of Confidentiality:** Attackers can use Data
- **Authorized Personnel pursues other Purposes**
  e.g., recognize neighbor or spouse in data

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

**Manage Risk of Use for Other** (thus unlawful) **Purposes**

**Use for other Purposes:**

- **Breach of Confidentiality:** Attackers can use Data
- **Authorized Personnel pursues other Purposes**
  e.g., recognize neighbor or spouse in data

**Manage Risk:** through **Technical** and **Organizational Measures** (**TOMs**)

- **make it less likely** (likelihood)
- **reduce negative impact on data subjects** (severity)

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**Specify and document fair and legitimate Purposes**

**Identify a suitable Legal Basis**

**How**

under what conditions ?

**minimize impact on data subjects**

**Limit Processing to what is Necessary for the Purposes**

**Manage Risk of Use for Other** (thus unlawful) **Purposes**

**processing must be fit for purpose**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is ***accurate*** and ***up-to-date***

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

## Data Subjects:

**No negative consequences from *inaccurate* and *out-of-date* data**

➔ see also data subjects' *right to rectification*

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

**Manage Risk of *inconsistency* and *unavailability***

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

Manage Risk of *inconsistency* and *unavailability*

## Data Subjects:

**No negative consequences from *inconsistency* and *data loss***

➔ stated in the context *of information security*

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**Specify and document fair and legitimate Purposes**

**Identify a suitable Legal Basis**

**How**

under what conditions ?

**minimize impact on data subjects**

**Limit Processing to what is Necessary for the Purposes**

**Manage Risk of Use for Other** (thus unlawful) **Purposes**

**processing must be fit for purpose**

**Guarantee Data is *accurate* and *up-to-date***

**Manage Risk of *inconsistency* and *unavailability***

**Empower Data Subjects**
(Transparency and Rights)

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

Manage Risk of *inconsistency* and *unavailability*

**Empower Data Subjects**
(Transparency and Rights)

**Data Subjects must be adequately informed**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

**Specify and document fair and legitimate Purposes**

**Identify a suitable Legal Basis**

**How**

under what conditions ?

**minimize impact on data subjects**

**Limit Processing to what is Necessary for the Purposes**

**Manage Risk of Use for Other** (thus unlawful) **Purposes**

**processing must be fit for purpose**

**Guarantee Data is *accurate* and *up-to-date***

**Manage Risk of *inconsistency* and *unavailability***

**Empower Data Subjects**
(Transparency and Rights)

**Data Subjects must be adequately informed**

## Transparency:

- **Awareness of Processing**
- **Understand Processing** (opens up processing to scrutiny)
- **Know how to Intervene**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

Manage Risk of *inconsistency* and *unavailability*

**Empower Data Subjects**
(Transparency and Rights)

**Data Subjects must be adequately informed**

**Transparency:**

- **Awareness of Processing**
- **Understand Processing** (opens up processing to scrutiny)
- **Know how to Intervene**

also:
**Risk from Data Breaches**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

Manage Risk of *inconsistency* and *unavailability*

**Empower Data Subjects**
(Transparency and Rights)

Data Subjects must be adequately informed

**Implement Ways for Data Subjects to Intervene**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

Manage Risk of *inconsistency* and *unavailability*

**Empower Data Subjects**
(Transparency and Rights)

Data Subjects must be adequately informed

**Implement Ways for Data Subjects to Intervene**

## Data Subject have Rights of:

- **access**
- **rectification**
- **erasure**
- **restriction of processing**
- **objection**
- **notifications**
- **withdrawal of consent**
- **human intervention** (for automatic decision making)
- **data portability** (no lock-in)

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

Manage Risk of *inconsistency* and *unavailability*

**Empower Data Subjects**
(Transparency and Rights)

Data Subjects must be adequately informed

Implement Ways for Data Subjects to Intervene

**Full Accountability**

**What** processing is allowed?

**Purposes** must be:

- **explicit**, **fair**, and **legitimate**
- **lawful**

Specify and document fair and legitimate Purposes

Identify a suitable Legal Basis

**How**

under what conditions ?

**minimize impact on data subjects**

Limit Processing to what is Necessary for the Purposes

Manage Risk of Use for Other (thus unlawful) Purposes

**processing must be fit for purpose**

Guarantee Data is *accurate* and *up-to-date*

Manage Risk of *inconsistency* and *unavailability*

**Empower Data Subjects**
(Transparency and Rights)

Data Subjects must be adequately informed

Implement Ways for Data Subjects to Intervene

**Full Accountability**

Be able to *Demonstrate Compliance*

| | | |
|---|---|---|
| **What** processing is allowed? | **Purposes** must be:<br>• **explicit**, **fair**, and **legitimate**<br>• **lawful** | Specify and document fair and legitimate Purposes<br>Identify a suitable Legal Basis |
| **How**<br><br>under what conditions ? | **minimize impact on data subjects** | Limit Processing to what is Necessary for the Purposes<br>Manage Risk of Use for Other (thus unlawful) Purposes |
| | **processing must be fit for purpose** | Guarantee Data is *accurate* and *up-to-date*<br>Manage Risk of *inconsistency* and *unavailability* |
| | **Empower Data Subjects** (Transparency and Rights) | Data Subjects must be adequately informed<br>Implement Ways for Data Subjects to Intervene |
| | **Full Accountability** | Be able to *Demonstrate Compliance* |

- **Mostly towards Supervisory Authorities**
- **Documentation of Processing, Data Protection Impact Assessment, ..**

# Conclusions (Module 1)

- **major obligations of controllers on a single "map"**
- useful for:
  - **locate concepts** (module 2: **principles**, module 3: **risks, ...**)
  - **foster understanding** (by making **structure** explicit)
  - **support communications** (e.g., by defining a **scope**)