AnoMed

Funded by Bundesministerium für Bildung und Forschung

Funded by the European Union
NextGenerationEU

Legal Aspects of Anonymization and Pseudonymization

--

Module 2: Principles of the GDPR

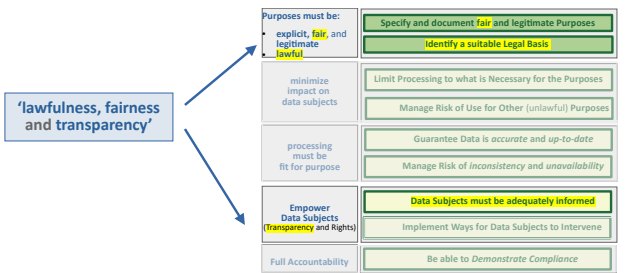
Bud P. Bruegger

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

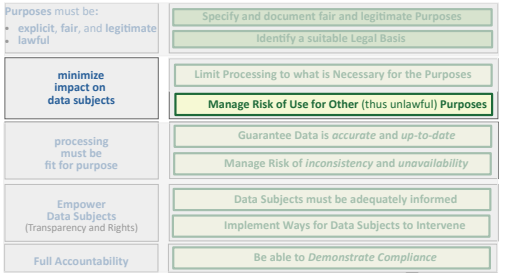
Outline Module 2

The Principles of the GDPR

- **Intro and History**
- **Definition and Mapping**



- **Risk in the GDPR**
  - which kind of Risk is AnoMed concerned with?
- **Understanding the *Risk of Use for Other Purposes***
  - in Terms of Principles

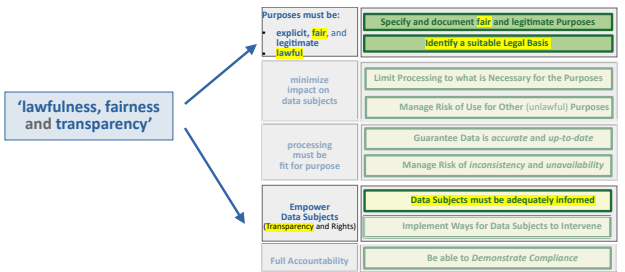


ULD for AnoMed Funded by Funded by the European Union NextGenerationEU

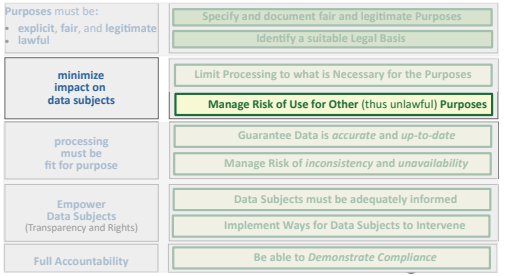
Outline Module 2

The Principles of the GDPR

- **Intro and History**
- **Definition and Mapping**



- **Risk in the GDPR**
  - which kind of Risk is AnoMed concerned with?
- **Understanding the Risk of Use for Other Purposes**
  - in Terms of Principles



Principles of Data Protection

- **Art. 5:** ***"Principles relating to processing of personal data"***

- **Art. 24:** ***"Responsibility of the controller"*** **→ what to do?**
  - "..the controller shall **implement** appropriate **technical and organisational measures**..
- **Art. 25(1):** ***"Data protection by design"*** **→ how to do it?**
  - "**implement** appropriate **technical and organisational measures**, which are designed **to implement data-protection principles**"

Principles in Art. 5

- **Description and name(s)**
  - Art 5(1)(a): ‘lawfulness, fairness and transparency’
  - Art 5(1)(b): ‘purpose limitation’
  - Art 5(1)(c): ‘data minimisation’
  - Art 5(1)(d): ‘accuracy’
  - Art 5(1)(e): ‘storage limitation’
  - Art 5(1)(f): ‘integrity and confidentiality’
  - Art 5(2): ‘accountability’

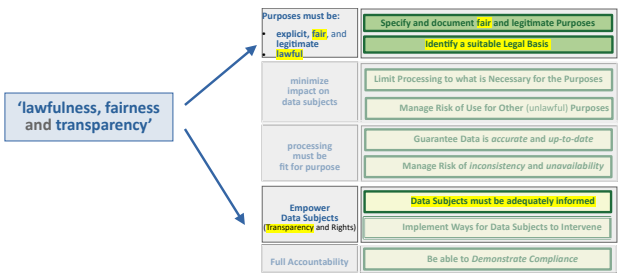
History of Principles

Council of Europe **Resolution (74) 29**	*OECD* **OECD/LEGAL/0188** *Adherents:* **all EU M.S.** except Malta and Romania	*EU* **Data Protection Directive**	*EU* **GDPR**
1974	1980	1995	2016
Lawfulness, Fairness [2.a], **Transparency** [3.a, 5.]	**Collection Limitation** & **Openness** (lawful, fair & with knowledge of data subject)	**Lawfulness, Fairness** [Art. 6(1)(a)]	**Lawfulness, Fairness** & ***Transparency*** [Art. 6(1)(a)]
Purpose Limitation [3.c]	**Purpose Specification** & **Use Limitation**	**Purpose Limitation** [Art. 6(1)(b)]	**Purpose Limitation** [Art. 5(1)(b)]
Data Minimization [2.c] (appropriate & relevant)	**Data Quality** (relevant & necessary)	**Data Minimization** [Art. 6(1)(c)] (adequate, relevant & not excessive)	**Data Minimization** [Art. 5(1)(c)] (adequate, relevant & necessary)
Accuracy [2.b]	**Data Quality** (accurate, complete, up to date)	**Accuracy** [Art. 6(1)(d)]	**Accuracy** [Art. 5(1)(d)]
Storage Limitation [4.] (storage period)	--	**Storage Limitation**[Art. 6(1)(a)] (storage period, identification)	**Storage Limitation** [Art. 5(1)(e)] (storage period, identification)
Confidentiality [6.]	**Security Safeguards**	(Art. 17: Security of Processing)	**Integrity & Confidentiality** [Art. 5(1)(f)]
--	**Individual Participation** (rights of access, erasure, rectification)	(Section V: *right of access*, Section VII: *right to object*)	(Chapter 3: *rights of the data subject*)
--	**Accountability** (privacy management, demonstrate compliance, breach notification)	**Accountability**[Art. 6(2)] (ensure compliance)	**Accountability** [Art. 5(2)] (responsible & demonstrate compliance)

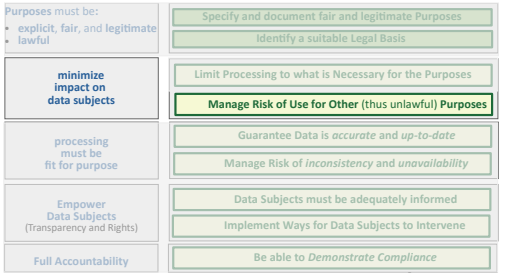
Outline Module 2

The Principles of the GDPR

- **Intro and History**
- **Definition and Mapping**



- **Risk in the GDPR**
  - which kind of Risk is AnoMed concerned with?
- **Understanding the *Risk of Use for Other Purposes***
  - in Terms of Principles



ULD for AnoMed Funded by Funded by the European Union NextGenerationEU

‘lawfulness, fairness and transparency’

- “Personal data shall be”
  - “processed **lawfully**, **fairly** and in a **transparent** manner in relation to the data subject”.

- **Lawful** is defined in **Art. 6**.
- **Fair** is not further defined.
- **Transparent** is defined in **Art. 12-14**.

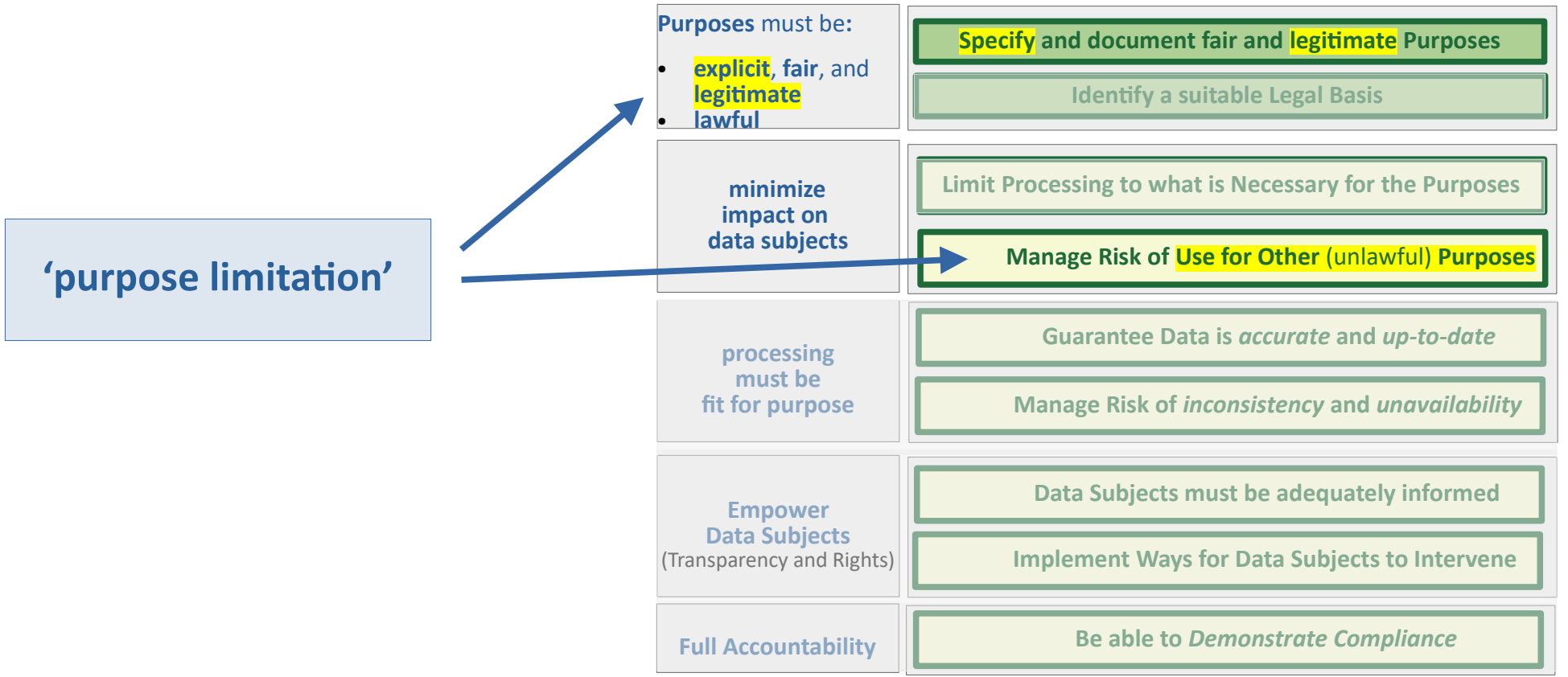
‘lawfulness, fairness and transparency’

Purposes must be: • **explicit, fair, and legitimate** • **lawful**	**Specify and document fair and legitimate Purposes** **Identify a suitable Legal Basis**
minimize impact on data subjects	Limit Processing to what is Necessary for the Purposes Manage Risk of Use for Other (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*

‘purpose limitation’

- “Personal data shall be”
  - “collected for **specified**, **explicit** and **legitimate purposes** and”
  - “**not** further **processed** in a manner that is **incompatible with those purposes.**”
  - .. what are compatible purposes ..

- 2 aspects:
  - purposes: **specified, explicit, legitimate**
  - **no** processing for **incompatible purposes**

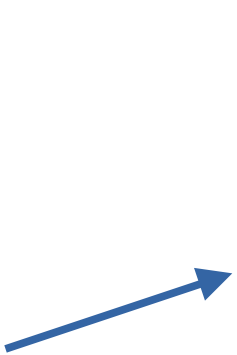


‘data minimisation’

- “Personal data shall be”
  - “**adequate**, **relevant** and **limited** to what is **necessary** in relation to the **purposes** for which they are processed.”

‘data minimisation’

less data → less impact



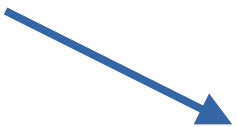
Purposes must be: • **explicit**, **fair**, and **legitimate** • **lawful**	Specify and document fair and legitimate Purposes Identify a suitable Legal Basis
minimize impact on data subjects	**Limit Processing to what is Necessary for the Purposes** **Manage Risk of Use for Other** (unlawful) **Purposes**
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*

“accuracy”

- “Personal data shall be”
  - “**accurate** and, where necessary, kept **up to date**; “
  - “every reasonable step must be taken to ensure that personal **data that are inaccurate**, having regard to the **purposes** for which they are processed, are **erased** or **rectified** without delay.”

- 2 aspects:
  - **accurate** and **up-to-date** (relative to purposes)
  - otherwise: **erased** or **rectified**

‘accuracy’



Purposes must be: • **explicit**, **fair**, and **legitimate** • **lawful**	Specify and document fair and legitimate Purposes Identify a suitable Legal Basis
minimize impact on data subjects	Limit Processing to what is Necessary for the Purposes Manage Risk of Use for Other (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*

“storage limitation”

- “Personal data shall be”
  - “**kept in a form which permits identification** of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed;“
  - “personal data may be **stored for longer periods** insofar as ...”

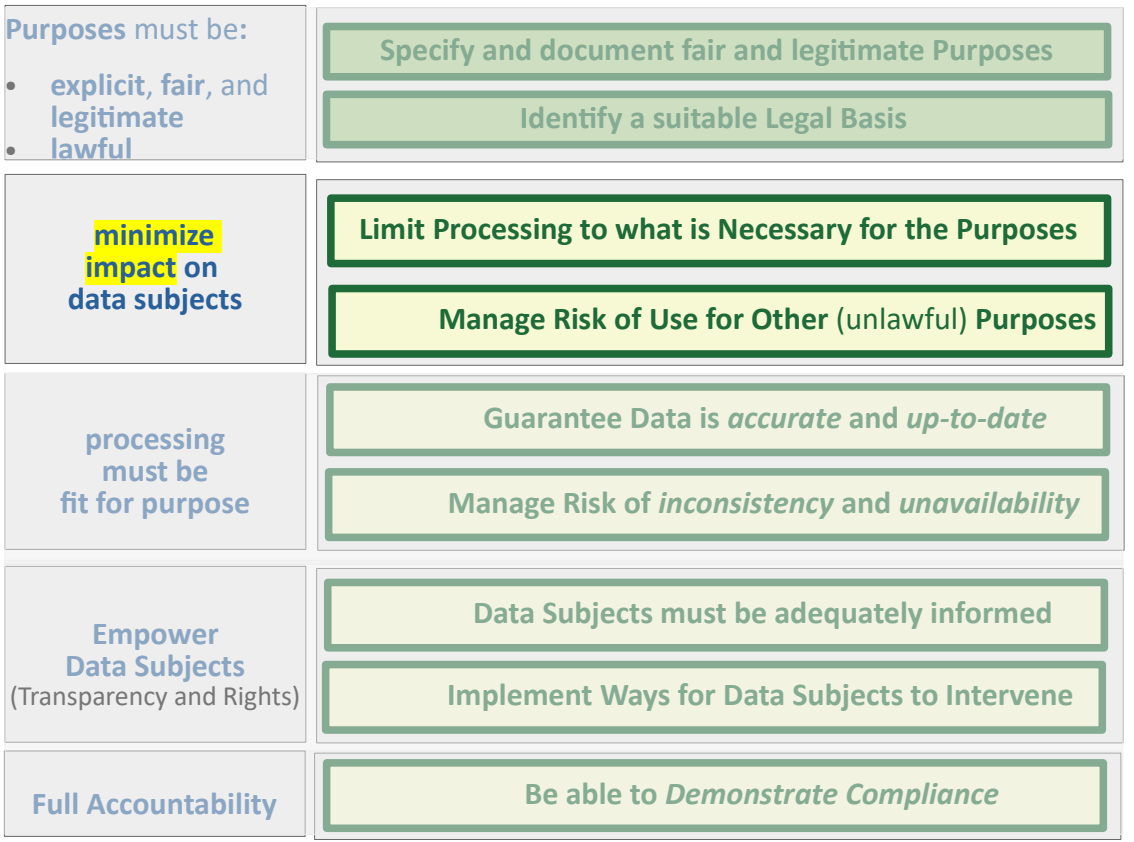
- 2 aspects:
  - **identification**
    - **pseudonymization**
    - **anonymization**
  - **storage period** **(deletion)**

‘storage limitation’

no identification → less impact

deletion → less impact

→ cannot be used for other purposes



“integrity and confidentiality”

- “Personal data shall be”
  - “processed in a manner that **ensures appropriate security** of the personal data, including protection against **unauthorised or unlawful processing** and against **accidental loss**, **destruction** or **damage**, using appropriate technical or organisational measures.”

- Context: **information security**
- Aspects:
  - **confidentiality**
  - **availability** (Art. 32 adds “resilience”)
  - **integrity**

‘integrity and confidentiality’

need to know disclosure

→ less impact

→ cannot be used for other purposes

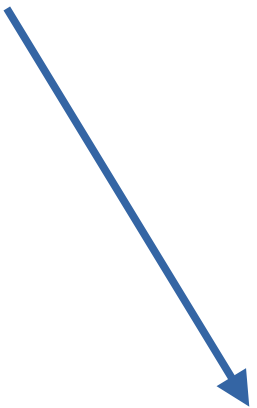
Purposes must be: • **explicit**, **fair**, and **legitimate** • **lawful**	Specify and document fair and legitimate Purposes Identify a suitable Legal Basis
minimize impact on data subjects	**Limit Processing to what is Necessary for the Purposes** **Manage Risk of Use for Other** (unlawful) **Purposes**
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*

“accountability”

- “The **controller** shall be **responsible** for, and be **able to demonstrate compliance with**, paragraph 1 ” [i.e., **the principles**]

- 2 Aspects:
  - **compliance with Principles**
  - **ability to demonstrate it**

‘accountability’



Purposes must be: • **explicit**, **fair**, and **legitimate** • **lawful**	Specify and document fair and legitimate Purposes Identify a suitable Legal Basis
minimize impact on data subjects	Limit Processing to what is Necessary for the Purposes Manage Risk of Use for Other (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***

Summary

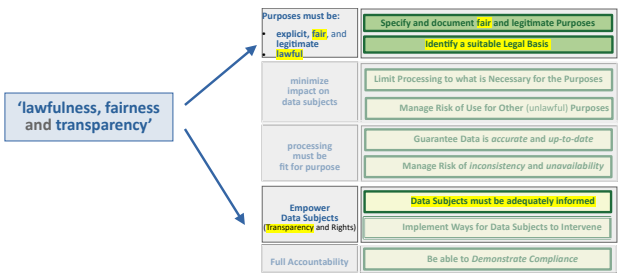
- **“Flowchart” contains all Principles**

- **Principles motivate Flowchart**
  - **but not 1:1 mapping**
  - **“untangling” necessary to create logical flow**

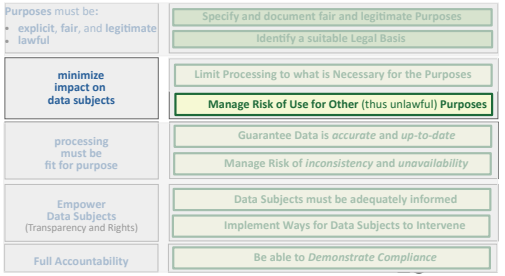
Outline Module 2

The Principles of the GDPR

- **Intro and History**
- **Definition and Mapping**



- **Risk in the GDPR**
  - which kind of Risk is AnoMed concerned with?
- **Understanding the *Risk of Use for Other Purposes***
  - in Terms of Principles



GDPR takes a risk-based approach

Art. 24 “Responsibility of the controller”

- Taking into account ... as well as the **risks of varying likelihood and severity** for the rights and freedoms of natural persons, ...

Art. 25(1) “Data protection by design”

- Taking into account ... as well as the **risks of varying likelihood and severity** for rights and freedoms of natural persons posed by the processing, ...

Art. 36(7)(c) “Data protection impact assessment”

- an **assessment of the risks** to the rights and freedoms of data subjects..

Proportionality of Risk and Protection

Risk

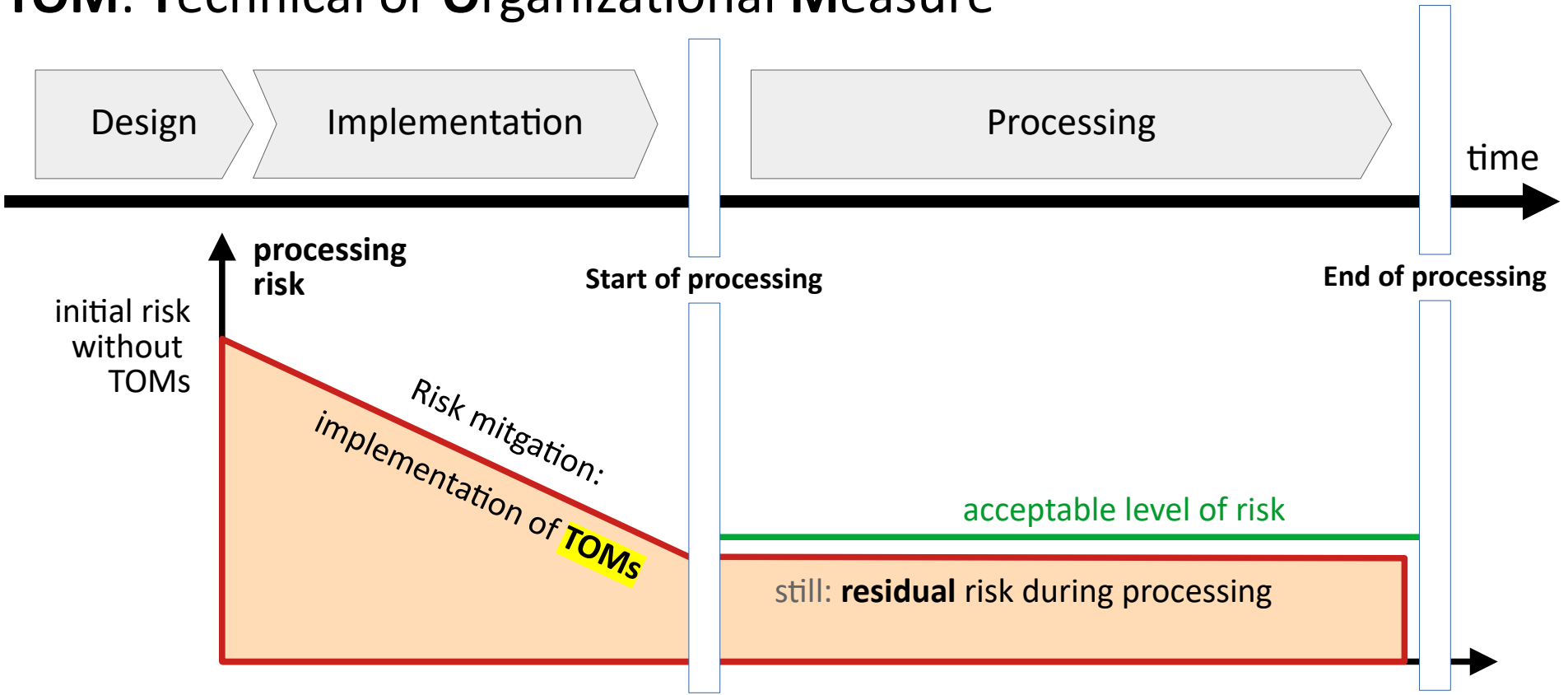
Technical and Organizational Measures

(TOMs)

(effort put into protection)

Mitigation of Risk with TOMs

TOM: **T**echnical or **O**rganizational **M**easure



Proportionality of Risk and Protection

GDPR:

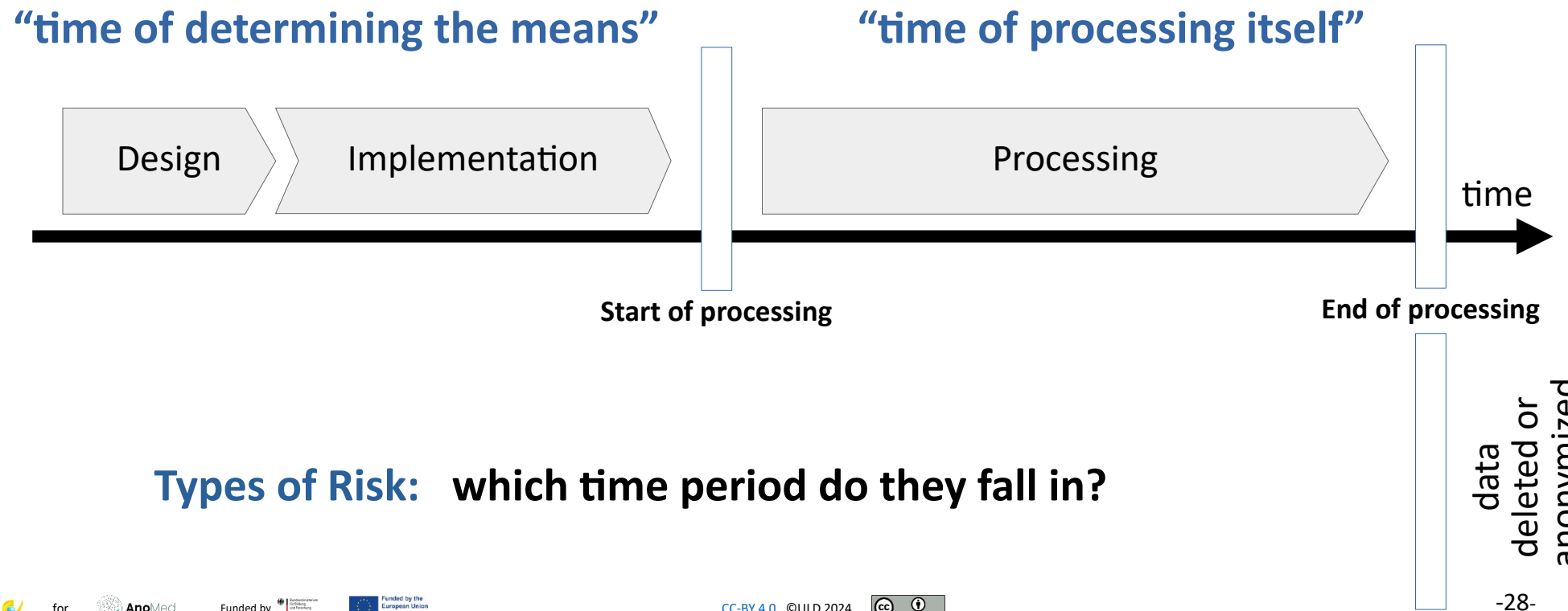
Risks to the ***rights and freedoms of natural persons***

- how does it compare to technical notion of risk? (Attacker Model, ..)

➔ distinguish **different kinds of risk**

Two Periods of Time in the GDPR

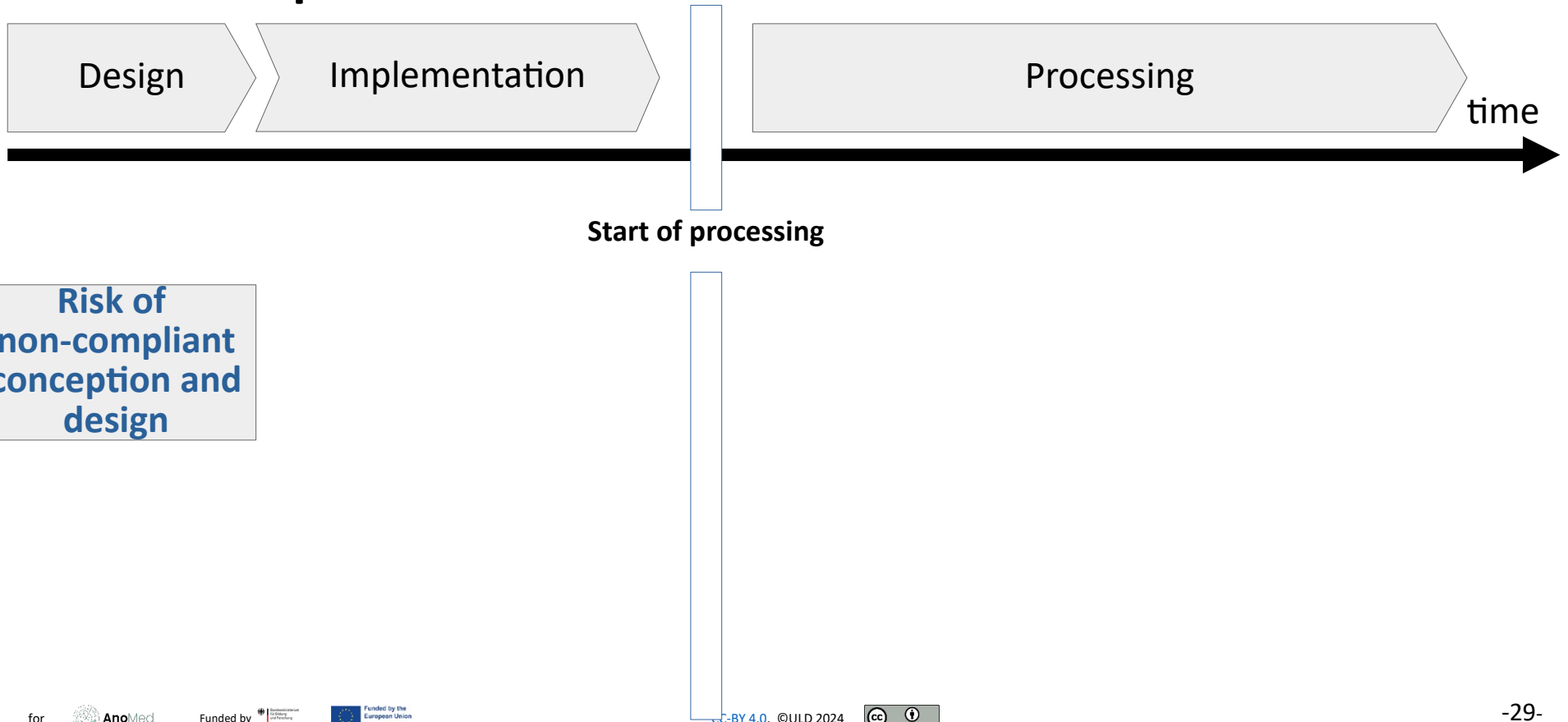
Art. 25 “data protection by design”



Types of Risk: **which time period do they fall in?**

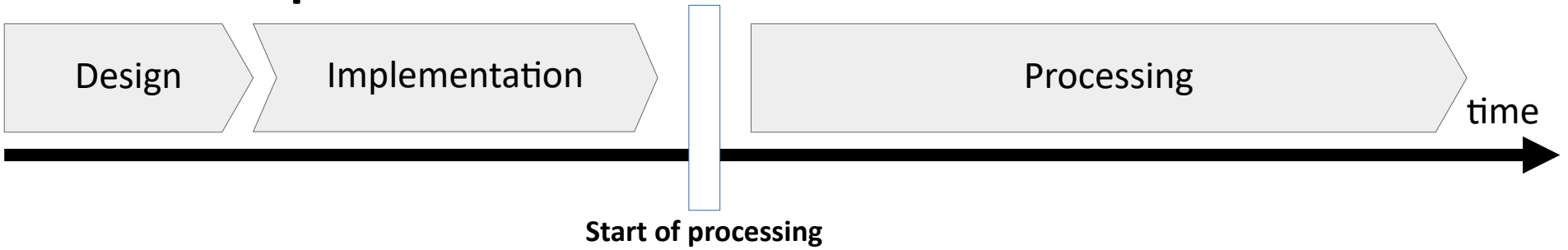
Different Kinds of Risk

Which time period does the risk refer to?



Different Kinds of Risk

Which time period does the risk refer to?



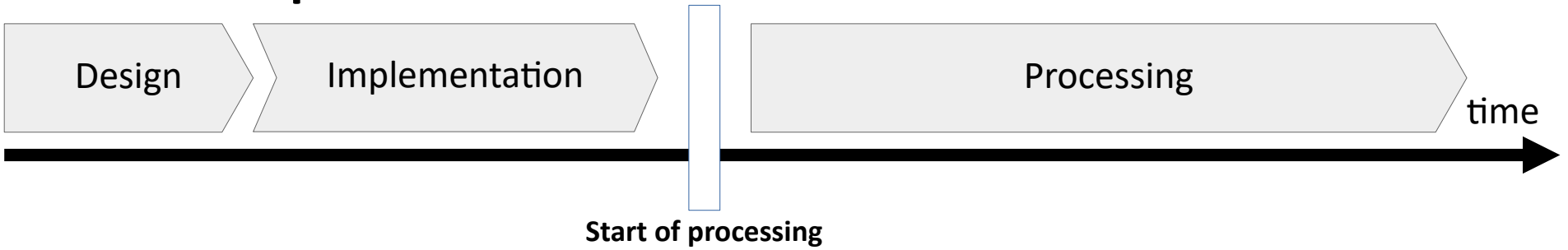
Risk of non-compliant conception and design

Risk of insufficient implementation:

- insufficient TOMs for protection
- insufficient implementation of data subject rights
- ...

Different Kinds of Risk

Which time period does the risk refer to?



Risk of incompliant conception and design

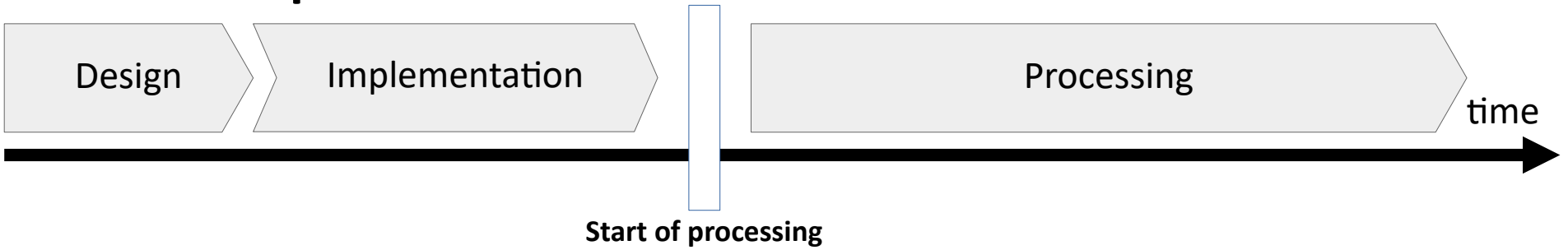
Risk of insufficient implementation:

- insufficient TOMs for protection
- insufficient implementation of data subject rights
- ...

Processing Risks

Different Kinds of Risk

Which time period does the risk refer to?



Risk of non-compliant conception and design

Risk of insufficient implementation:

- insufficient TOMs for protection
- insufficient implementation of data subject rights
- ...

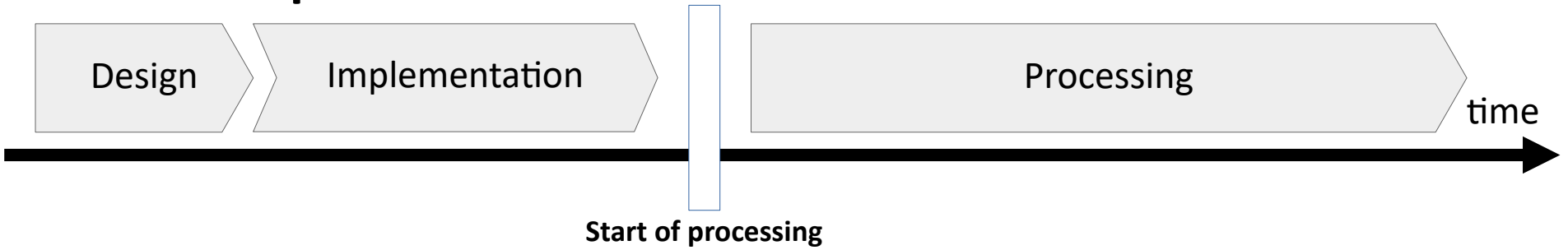
Processing Risks

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

Manage Risk of *inconsistency* and *unavailability*

Different Kinds of Risk?

Which time period does the risk refer to?



Risk of non-compliant conception and design

Risk of insufficient implementation:

- insufficient TOMs for protection
- insufficient implementation of data subject rights
- ...

Processing Risks

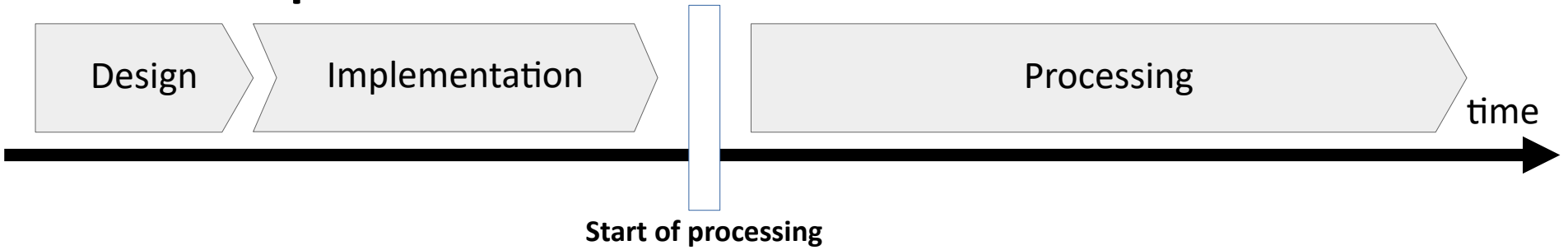
Manage Risk of Use for Other (thus unlawful) **Purposes**

information security (well understood)

Manage Risk of *inconsistency* and *unavailability*

Different Kinds of Risk?

Which time period does the risk refer to?



Risk of non-compliant conception and design

Risk of insufficient implementation:

- insufficient TOMs for protection
- insufficient implementation of data subject rights
- ...

Processing Risks

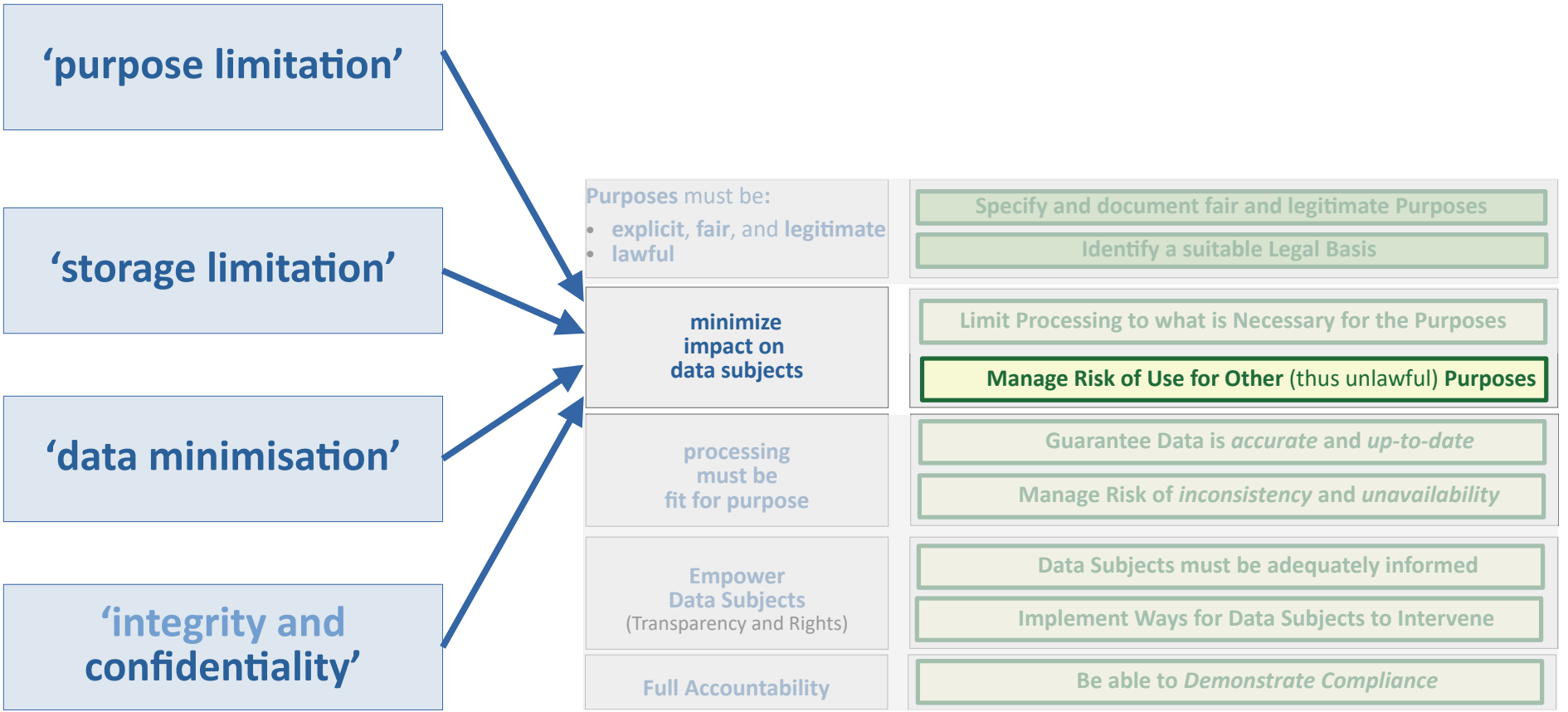
Manage Risk of Use for Other (thus unlawful) **Purposes**

deserves further analysis

AnoMed: residual risk of **re-identification**

Manage Risk of *inconsistency* and *unavailability*

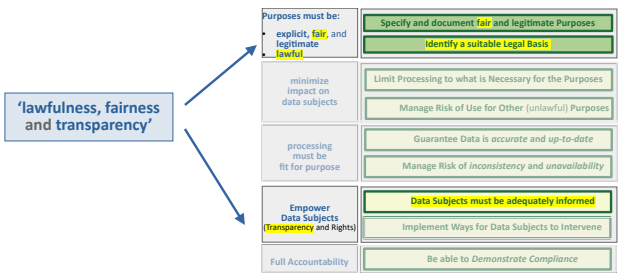
What is the Relation with Principles?



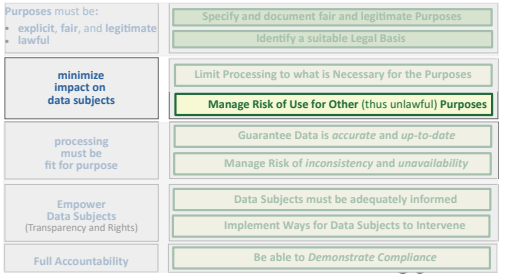
Outline Module 2

The Principles of the GDPR

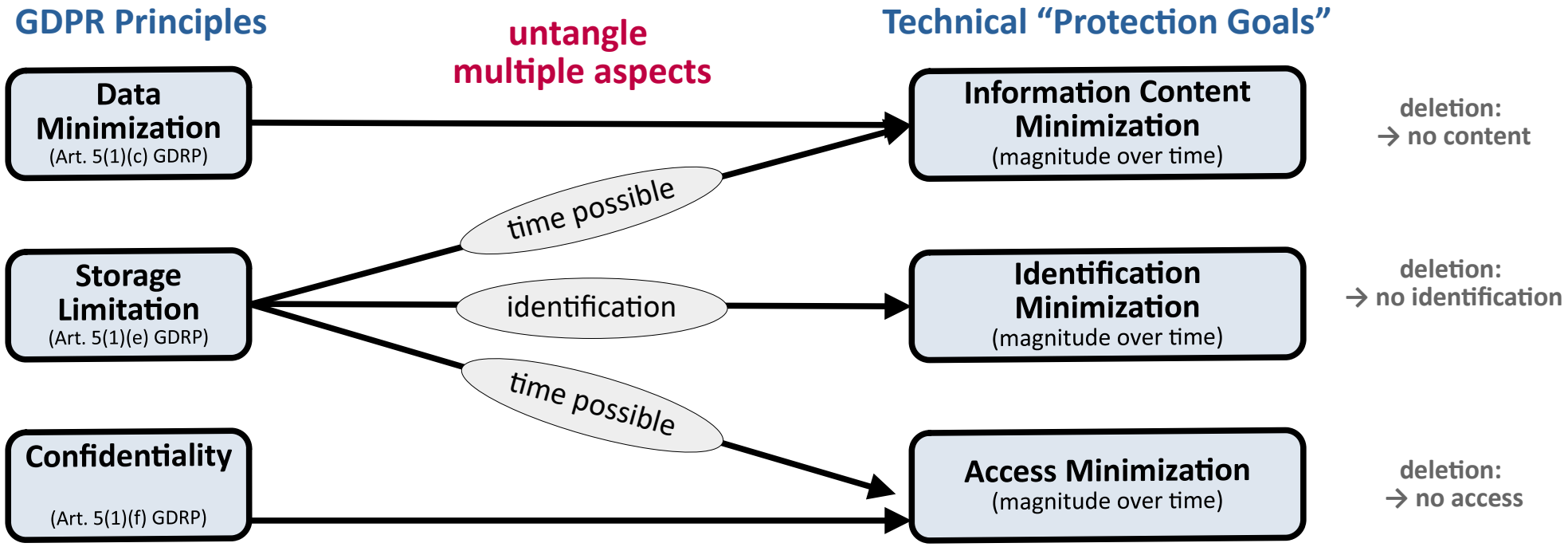
- **Intro and History**
- **Definition and Mapping**



- **Risk in the GDPR**
  - which kind of Risk is AnoMed concerned with?
- **Understanding the *Risk of Use for Other Purposes***
  - in Terms of Principles



“Untangling of Definitions: “Protection Goals”

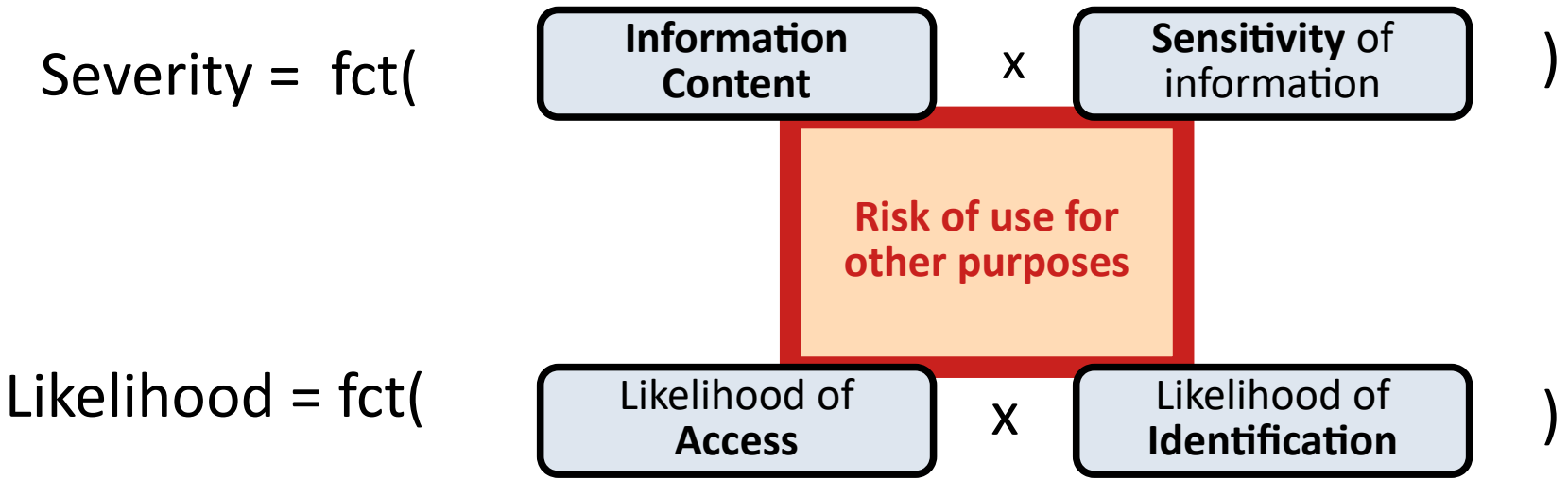


Risk

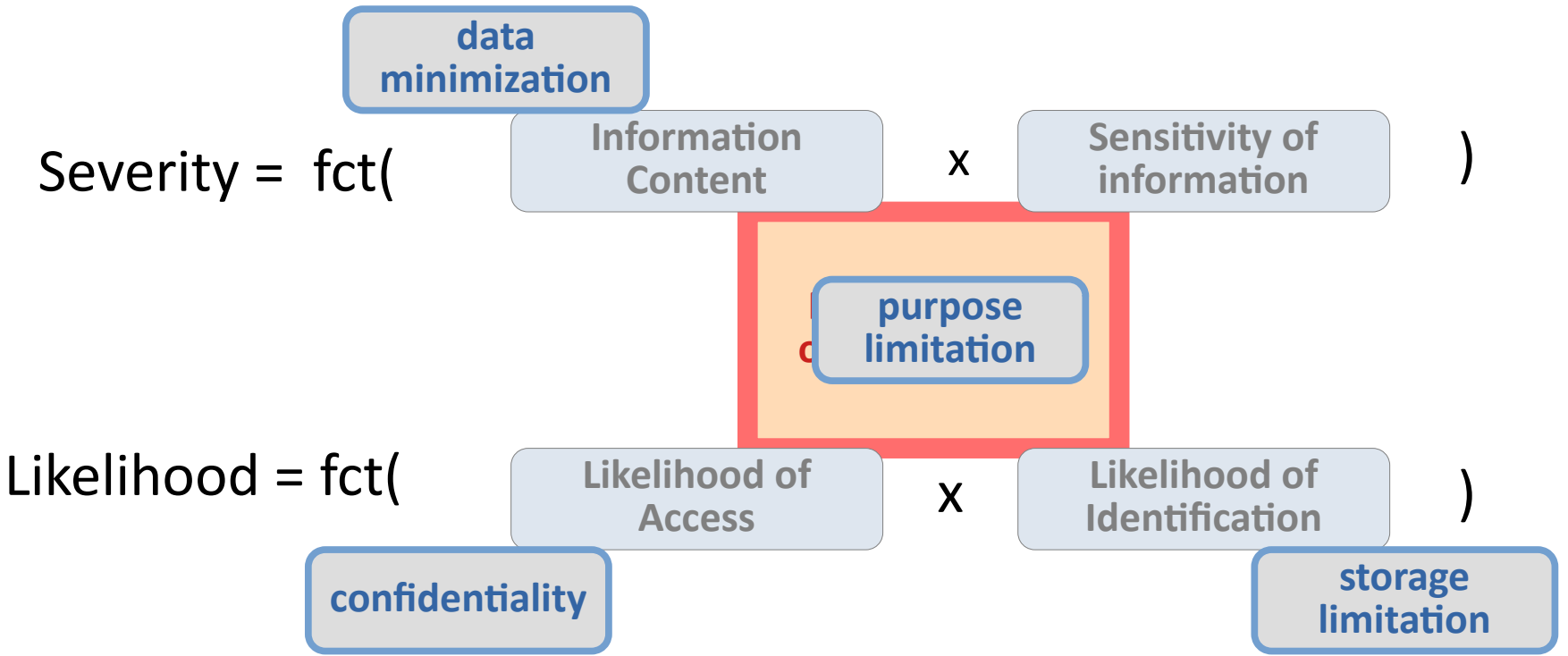
Risk = Likelihood x Severity

Risk of Use for Other Purposes

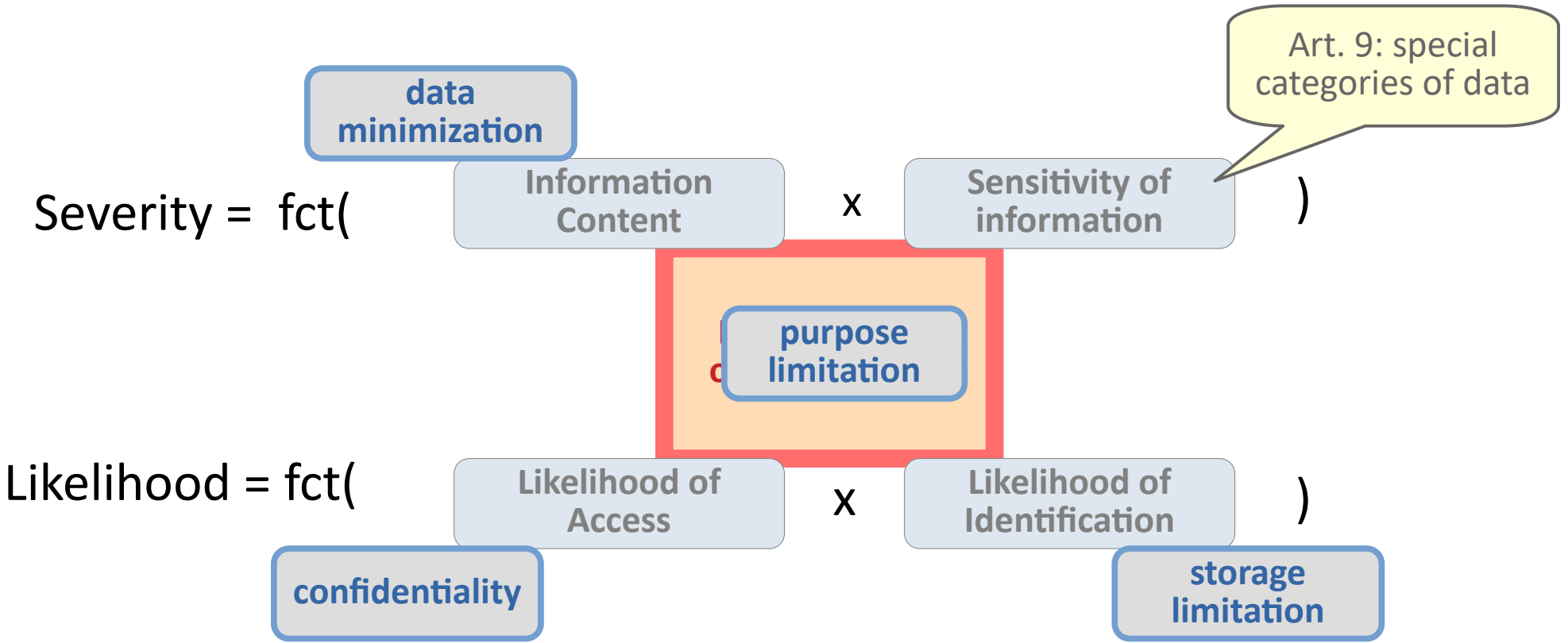
Main aspect of “purpose limitation”



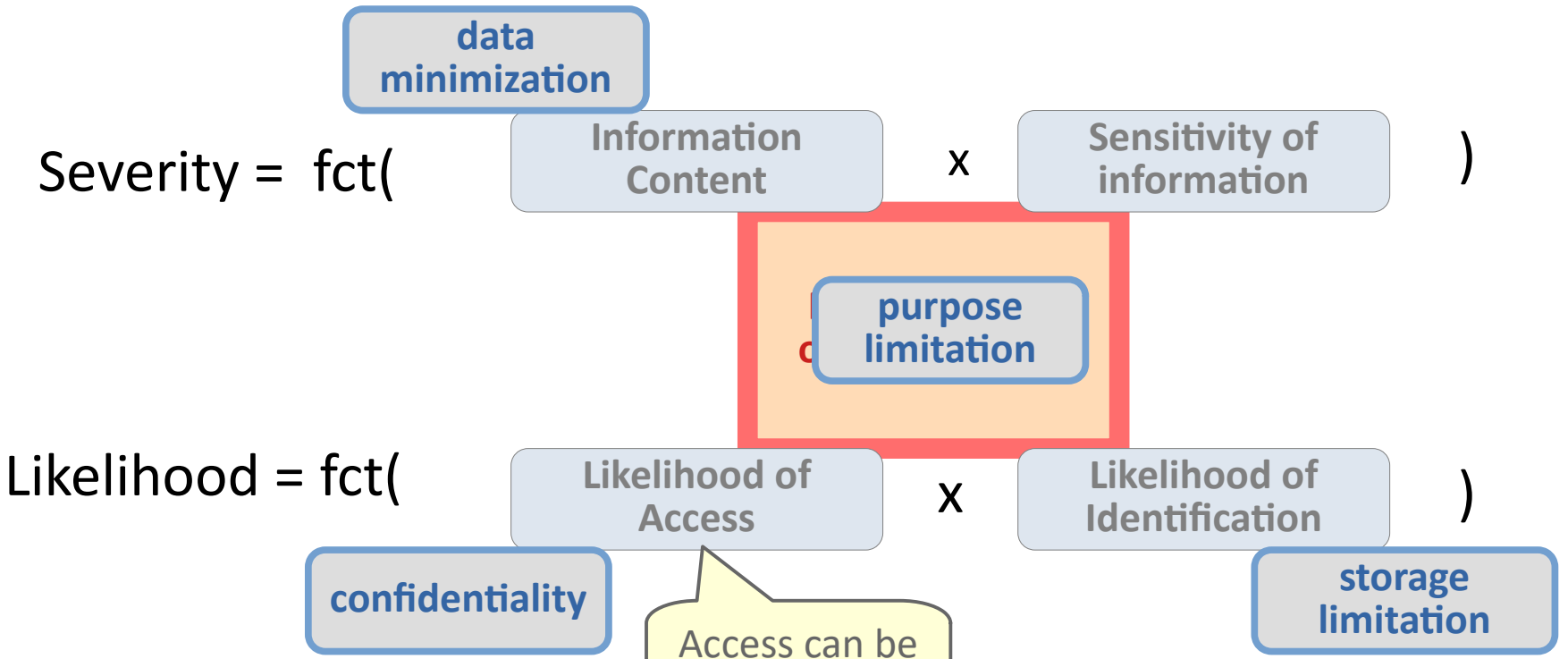
Risk of Use for Other Purposes



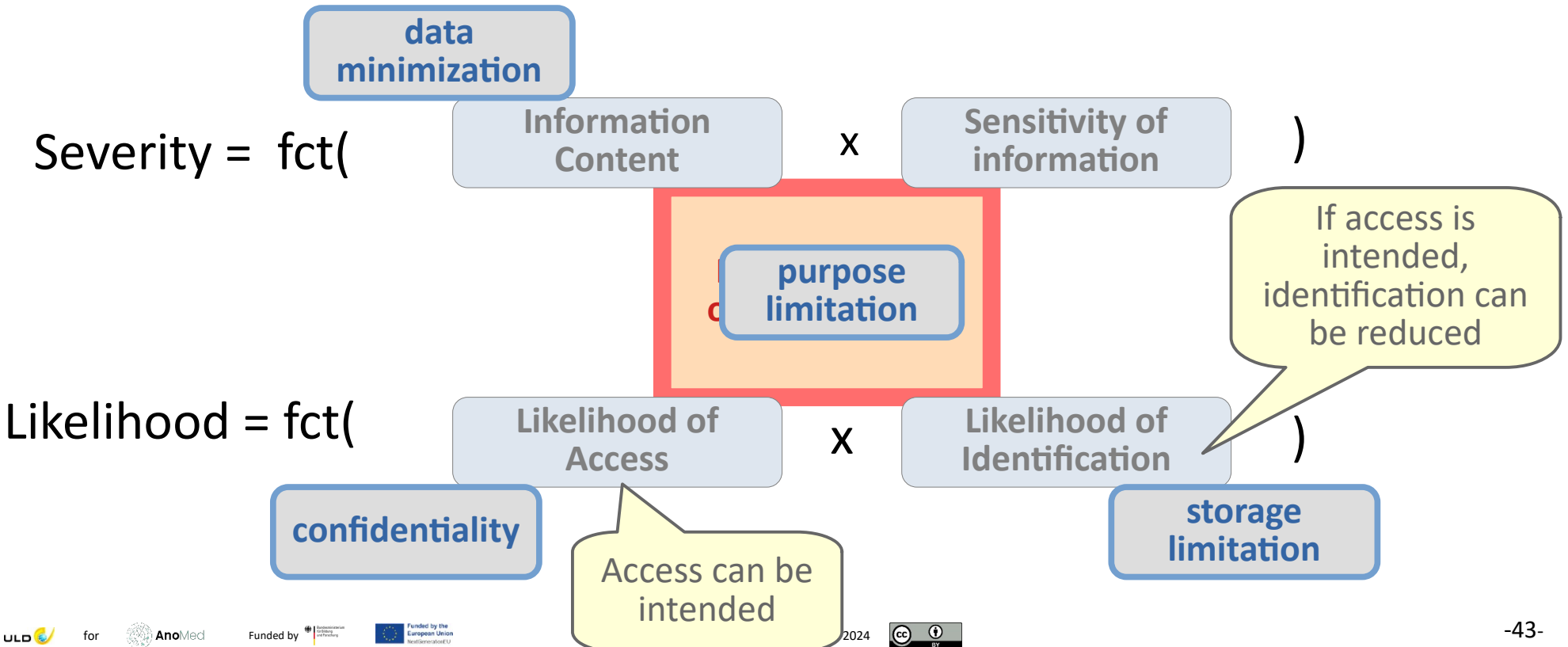
Risk of Use for Other Purposes



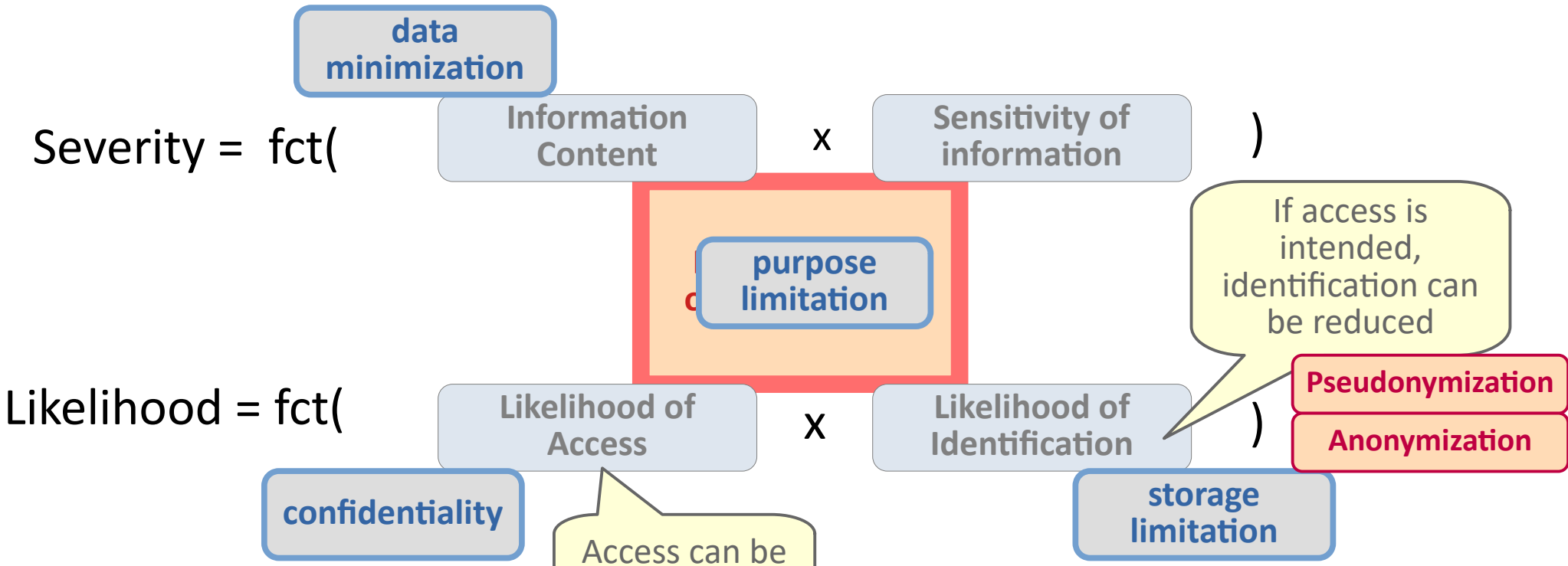
Risk of Use for Other Purposes



Risk of Use for Other Purposes



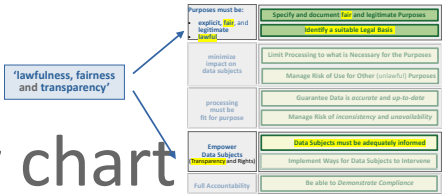
Risk of Use for Other Purposes



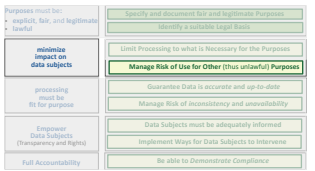
Conclusions Module 2

Principles are central to the GDPR

- They have a **long History** (many since 1974)
- **Looked at all Principles..**
- ..and where they fit in the flow chart



- Several Principles are related to the ***Risk of Use for Other Purposes***



- Briefly looked at **Risk in the GDPR**
- **Analysed how 4 principles relate to this Risk**