Data Protection in Research Data Management

Vasilka Stoilova

December 2023

BERD@NFDI: Consortium for Business, Economic and Related Data (BERD) in the German National Research Data Infrastructure (NFDI)

- Focus on unstructured data in economics and social sciences
- Developing a platform with various data relevant services
- Supporting researchers

Data Protection is highly relevant in all of these aspects.

Why do we need data protection?

Why do we need data protection?

Data Protection

Data Privacy

GDPR

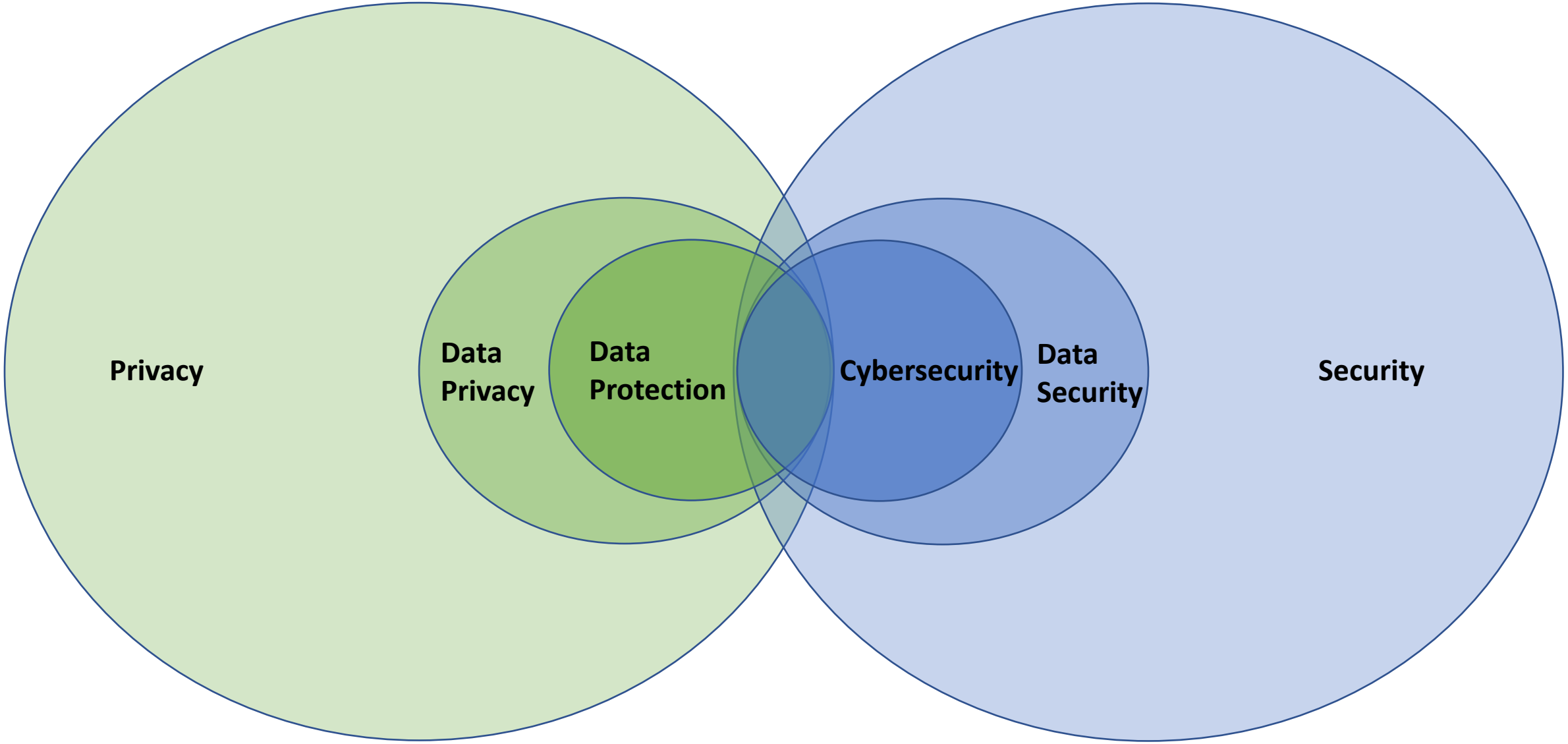
Data Security

Privacy Law

Personal Information

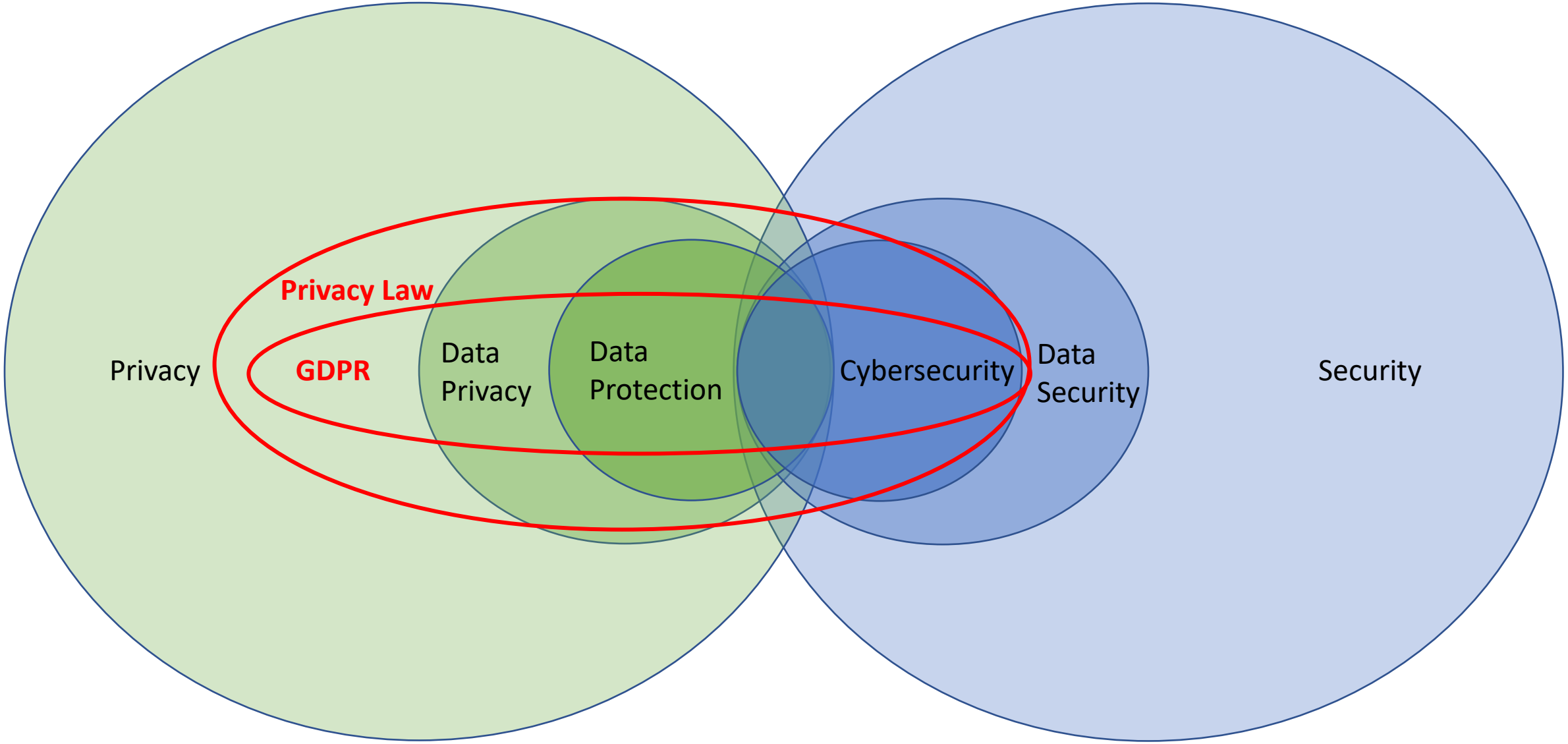
Cybersecurity

Why do we need data protection?



Source: https://securityboulevard.com/2019/11/on-the-convergence-of-data-privacy-and-data-security-part-1/

Why do we need data protection?



Source: https://securityboulevard.com/2019/11/on-the-convergence-of-data-privacy-and-data-security-part-1/

Why do we need data protection?

What is data protection?

- Data protection generally refers to the "**protection of personal data**".

Why do we need data protection?

- Data protection is important so that **data misuse** can be avoided.

What is the GDPR?

What is the GDPR?

What is the GDPR?

- The General Data Protection Regulation (GDPR) has been **directly** applicable in all EU member states since May 25, 2018.

GDPR and national regulations?

- EU member states are normally not permitted to weaken or strengthen the data protection stipulated by the General Data Protection Regulation through national regulations.
- However, the GDPR contains various opening or “escape” clauses that allow the individual Member States to regulate certain aspects of data protection on their own: e.g. Art. 9 para. 2 lit. j GDPR

GDPR

- **Data Protection**

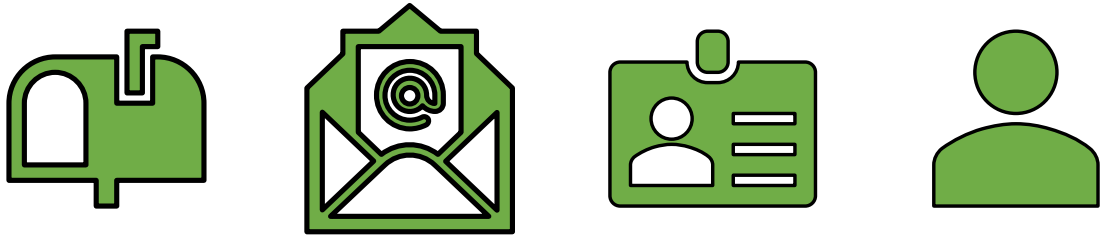
GDPR, Recital 1

…"The protection of natural persons in relation to the processing of personal data is a fundamental right."

- **Personal Data**

Art. 4 (1) GDPR

"'personal data' means any information relating to an identified or identifiable natural person[…]"



What is personal data?

- E-mail
- IP address
- Home address
- Profession
- Education Level
- Birthday
- Pet
- Favourite Colour

GDPR

- **Personal Data**

Art. 4 (1) GDPR

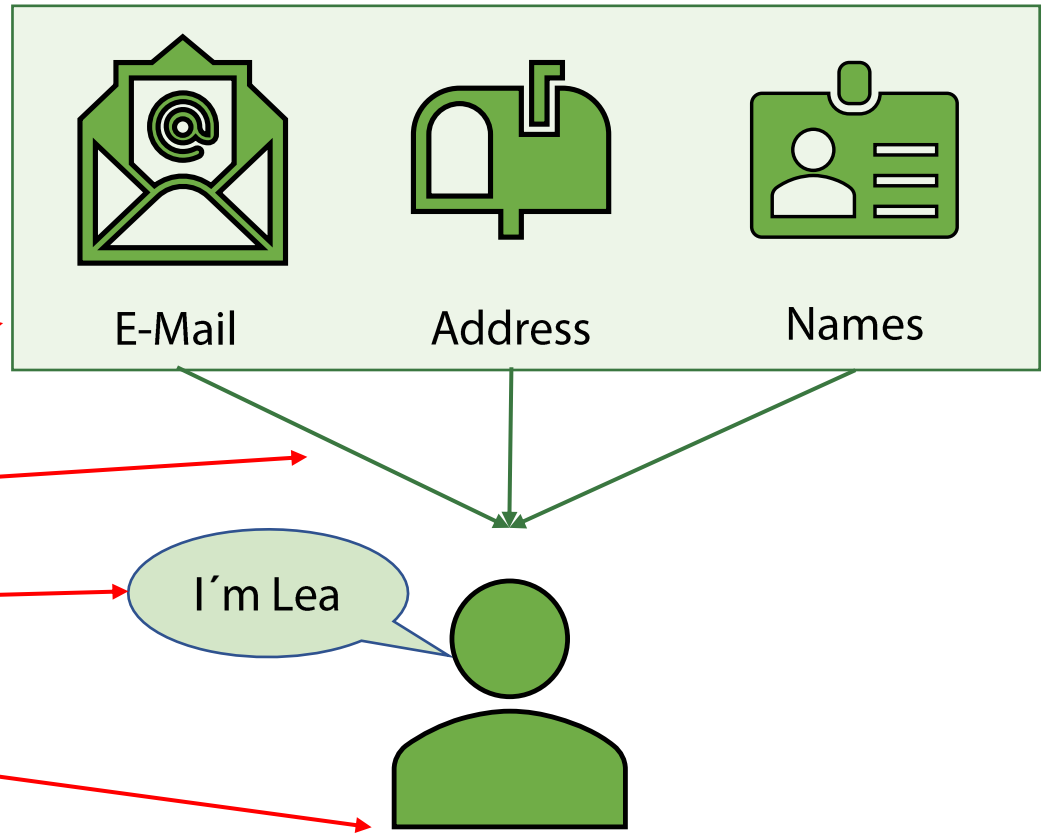
"'personal data' means

any information

relating to an identified or

identifiable

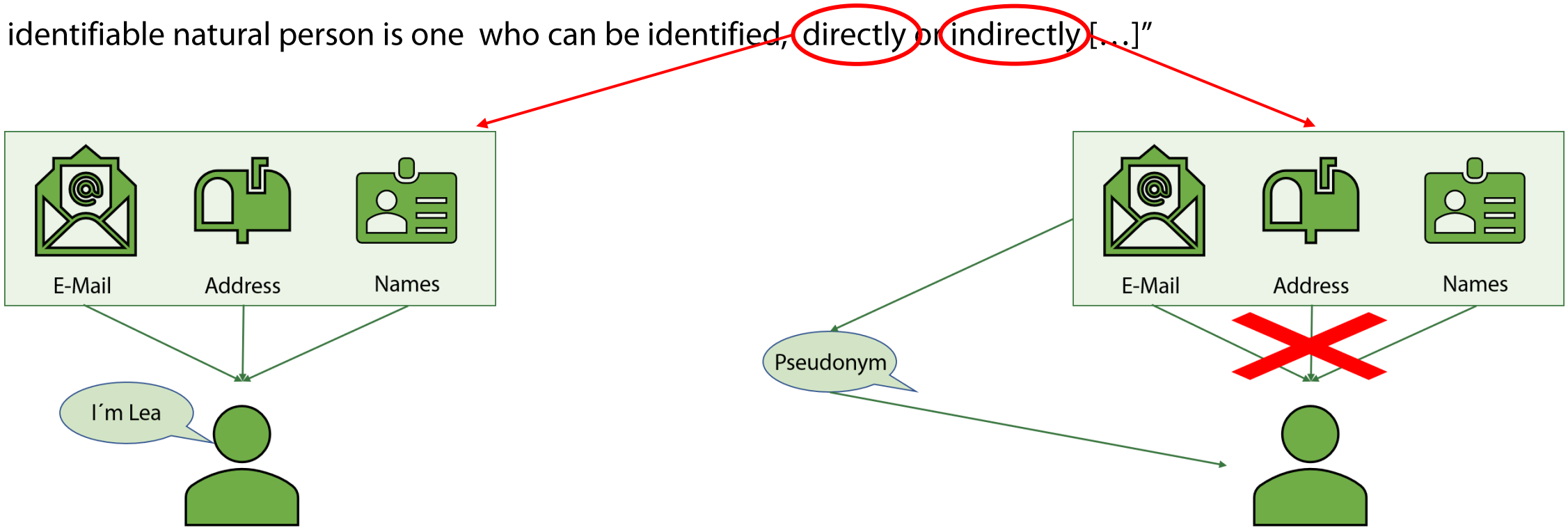
natural person[…]"



- **Identifiability**

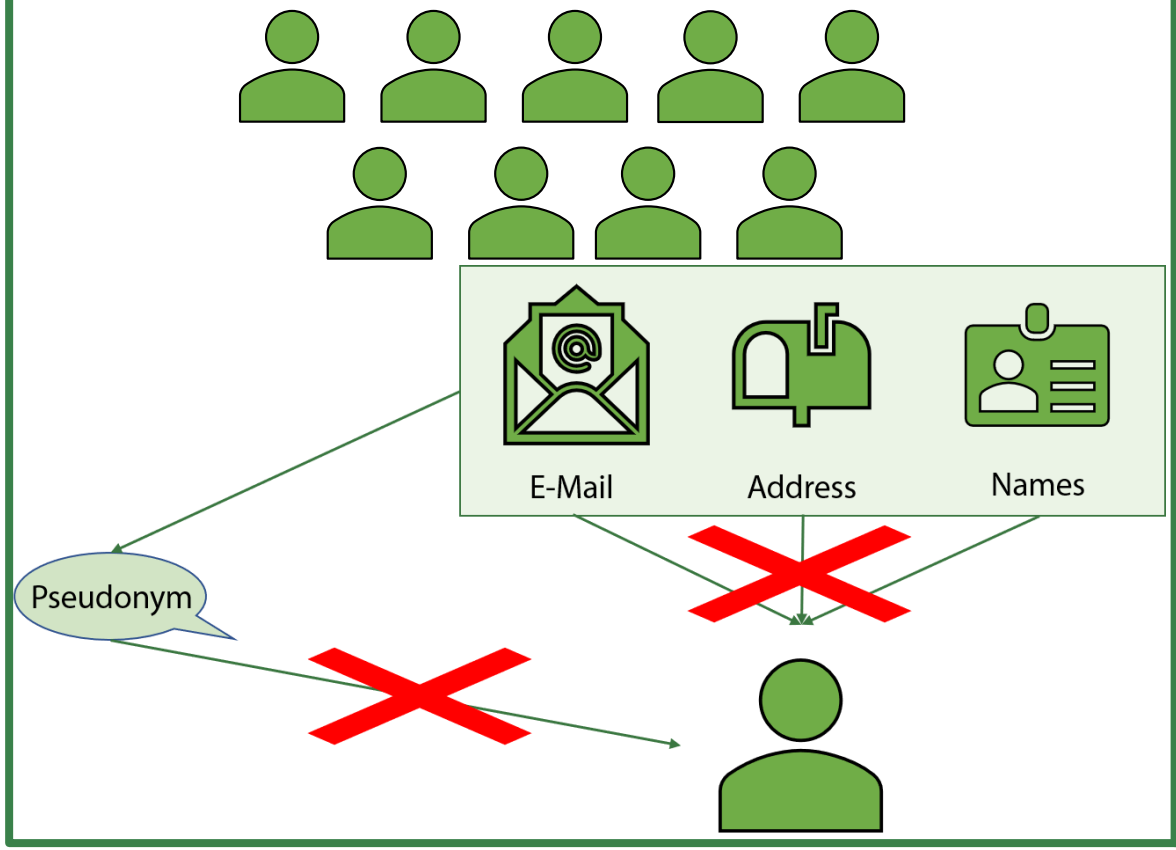
Art. 4 (1) GDPR

“an identifiable natural person is one who can be identified, directly or indirectly […]”

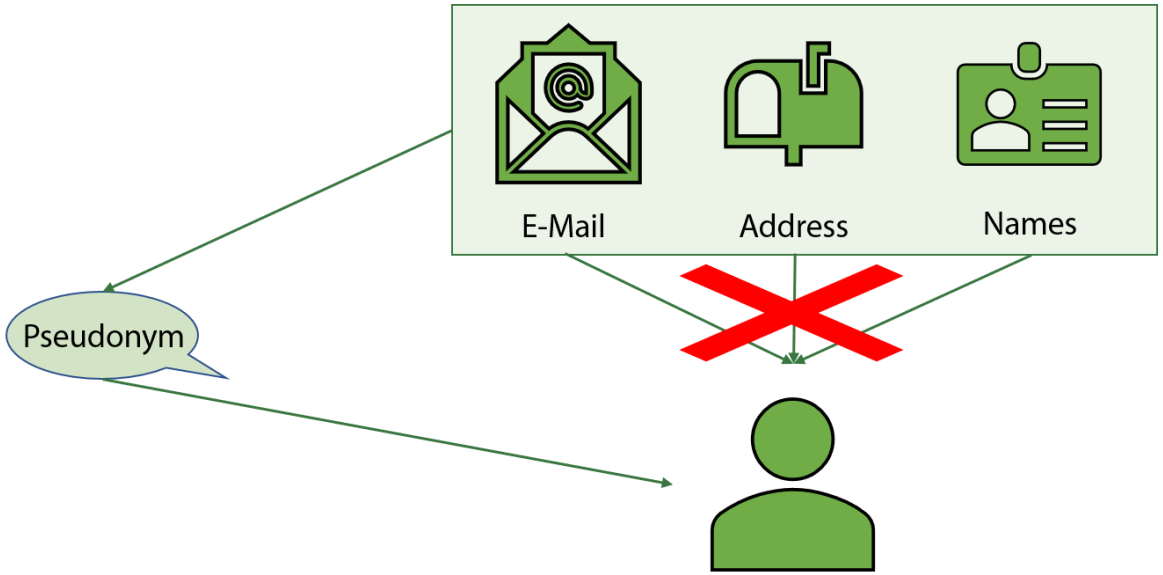


GDPR

- **Anonymised Data**



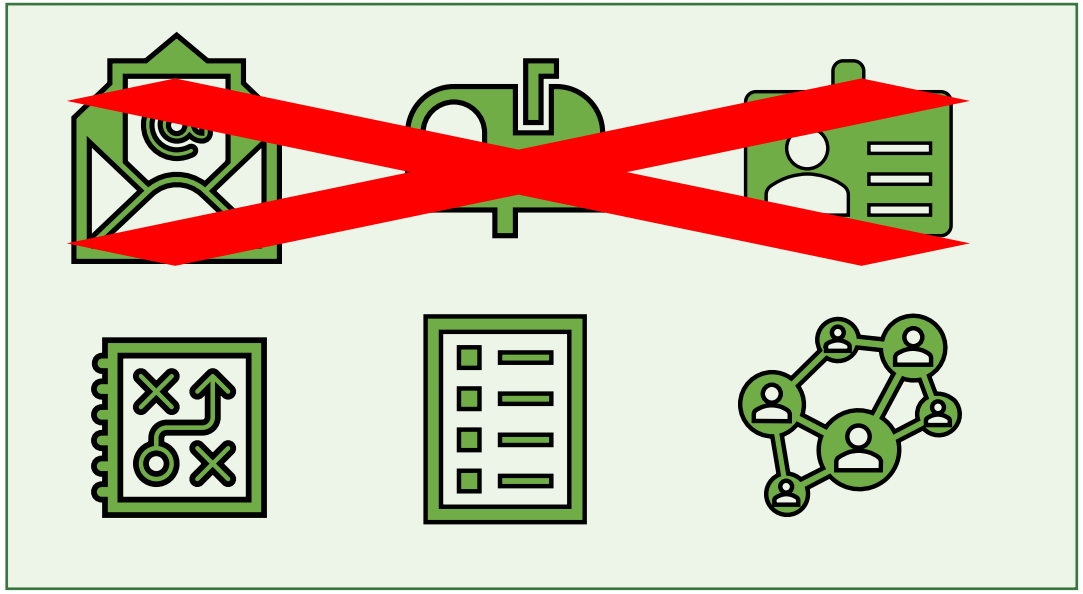
- **Pseudonymised Data**



- **Anonymous Data**

GDPR, Recital 26

Anonymous data is “information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable”



Legal basis

- **Ban subject to the possibility of authorization =** legal principle according to which a certain action is generally prohibited unless permission is expressly granted (by statutory regulations or the explicit consent of the data subject)

Art. 6 (1) GDPR

„ Processing shall be lawful only if and to the extent that at least one of the following applies:[…].“

- **consent**
- **contractual relationship**
- **compliance with a legal obligation**
- **protecting the vital interests of the data subject**
- **task carried out in the public interest**
- **legitimate interests pursued by the controller**

A legal basis is required!

What are the Data Protection Principles?

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- ➢ Lawfulness, Fairness and Transparency
- ➢ Purpose Limitation
- ➢ Data Minimization
- ➢ Accuracy
- ➢ Storage Limitation
- ➢ Integrity and Confidentiality
- ➢ Accountability

Lawfulness: Legal basis for data processing is needed:
Art. 6 GDPR (consent, contract, legal obligation, protection of vital interests of a natural person, public task done in public interest, proof of legitimate interest)
Art. 9 GDPR (further requirements for sensitive data)

Fairness: Builds on *lawfulness:*
Truthfulness and openness regarding the purposes for and the art of data collection are needed. No misuse or mishandling of the collected data.

Transparency: Closely linked to *fairness:*
Clear, understandable and honest information about the person/organization processing personal data. Data subjects must be able to comprehend the data processing.
Art. 89 GDPR allows partial derogation from the information obligations for scientific research.

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Purpose Limitation: Data is "collected for specified, explicit, and legitimate purposes" only. Clearly communicated to individuals through a privacy notice beforehand.

For each new purpose, not compatible with the original one, a new and specific consent is needed.

But scientific research is privileged, Art. 5(1)(b) GDPR:
Further processing for scientific or historical research purposes shall be considered compatible with the initial purposes.

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Data Minimization: Linked to *purpose limitation*:
Data is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Collecting only the minimum amount of data needed for the stated purposes.

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Accuracy: Data is "accurate and, where necessary, kept up to date". Inaccurate personal data in regards to the processing purposes should be "erased or rectified without delay".

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Storage Limitation: Linked to *purpose limitation*:
Data retention periods must be established, eg. a standard period after achieving the processing purposes is set, afterwards the data is anonymized.

Scientific research is privileged: longer storage periods allowed.

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- Lawfulness, Fairness and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

Integrity and Confidentiality: Keeping data secured from internal or external threats – "unauthorized or unlawful processing, accidental loss, destruction or damage using appropriate technical or organisational measures".

What are the Data Protection Principles?

- **The 7 Principles of GDPR**

Art. 5 GDPR

"'Personal data shall be[…]"

- ➢ Lawfulness, Fairness and Transparency
- ➢ Purpose Limitation
- ➢ Data Minimization
- ➢ Accuracy
- ➢ Storage Limitation
- ➢ Integrity and Confidentiality
- ➢ Accountability

Accountability: Documentation of measures and records as proof of compliance. Supervisory authorities can require this as evidence.

"The controller shall be responsible for, and be able to demonstrate compliance…"

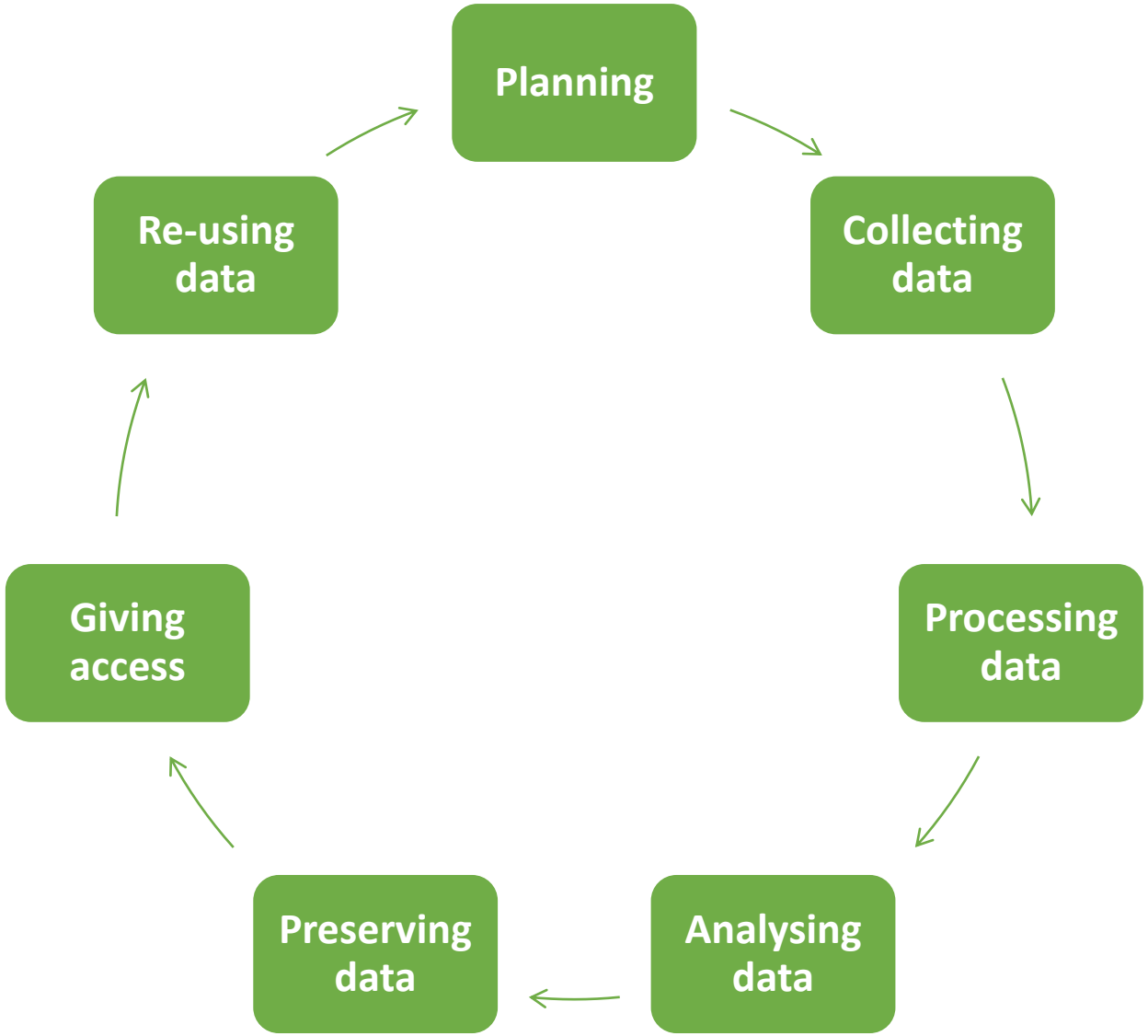
- Who is controller in scientific research?

Controllers are the primary bearers of obligations under data protection law. The factual test for controllership is who decides on the purpose and essential means of processing.

How to comply with the Data Protection Principles?

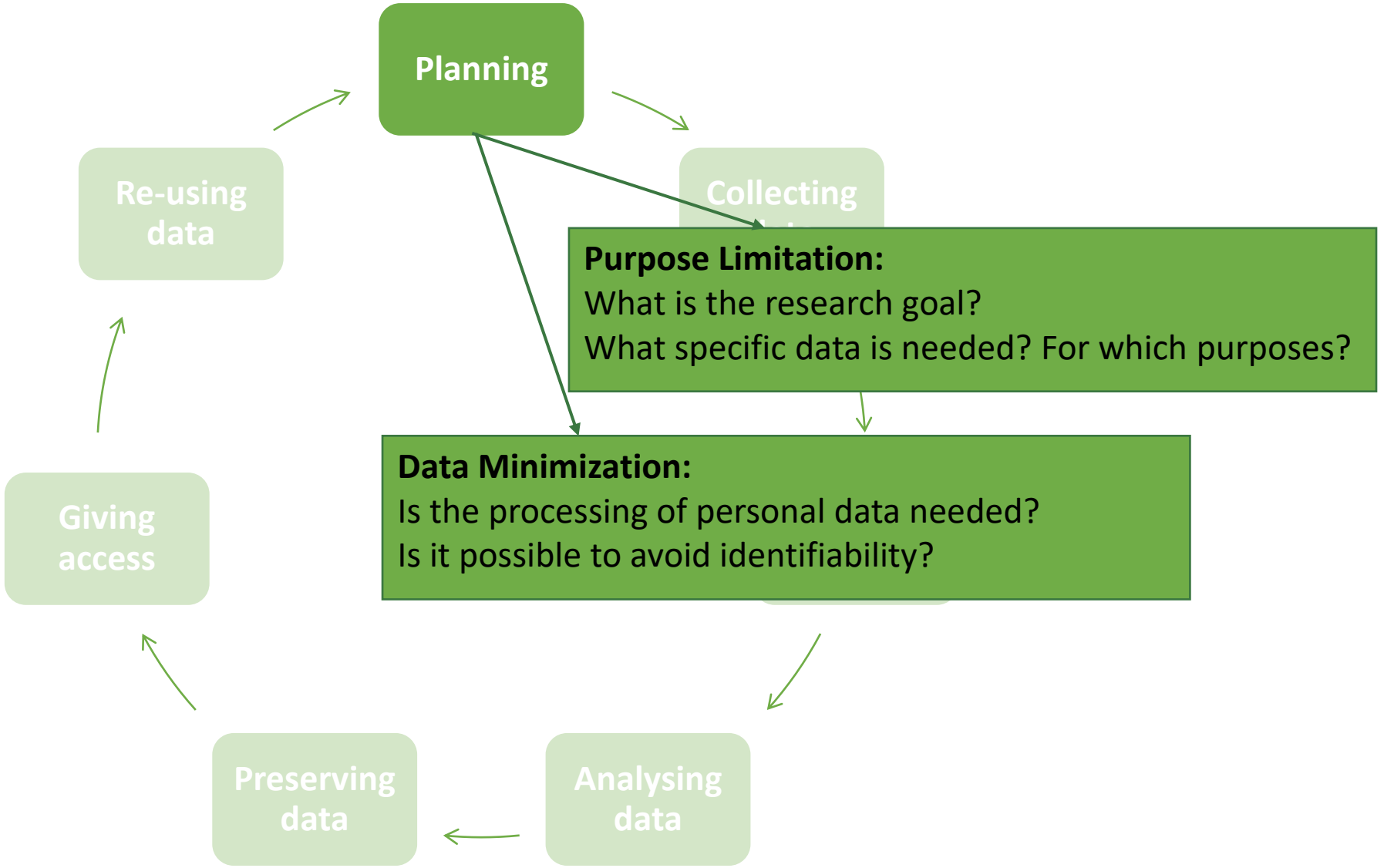
How to comply with the Data Protection Principles?

- **Research Data Lifecycle**



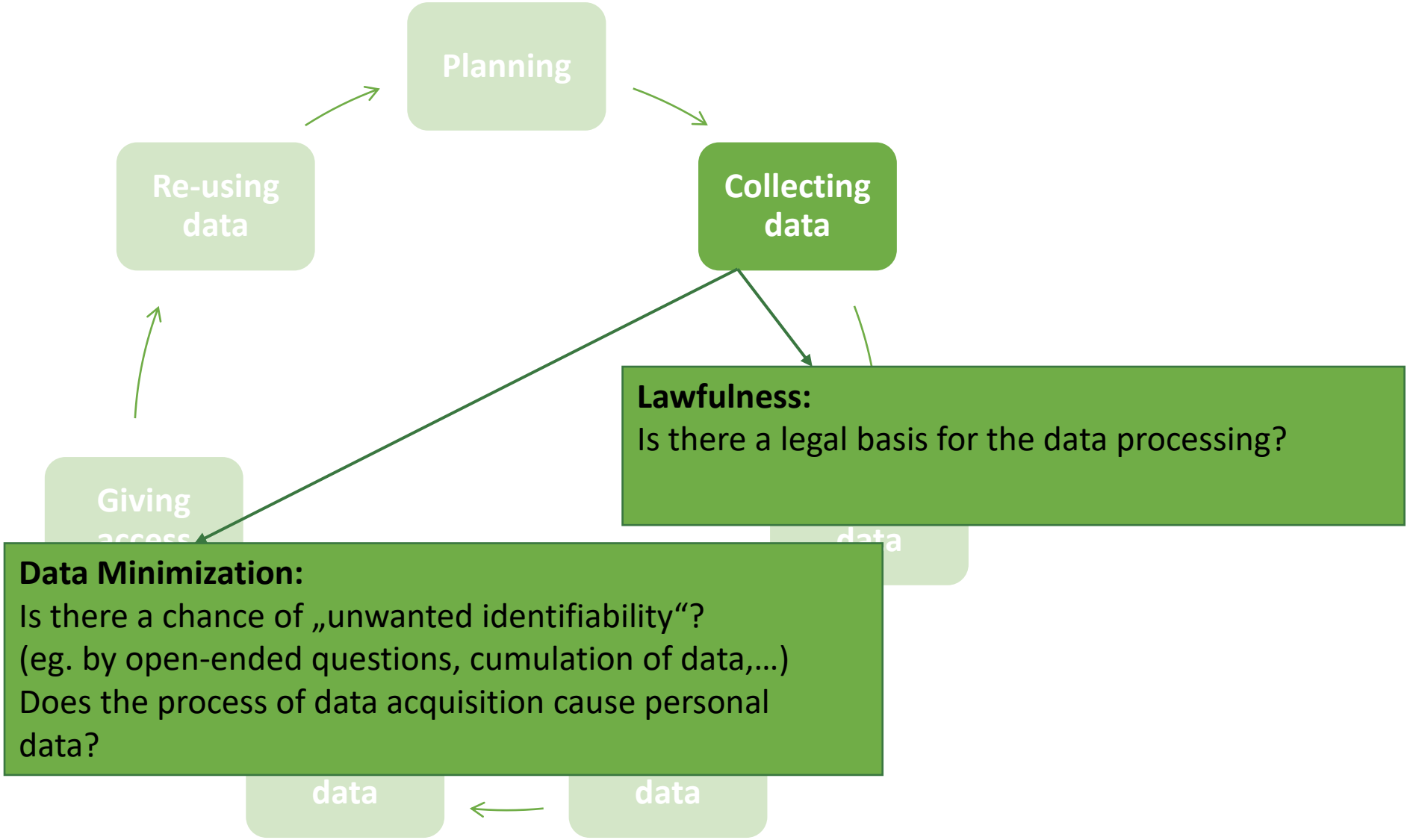
How to comply with the Data Protection Principles?

- **Research Data Lifecycle**



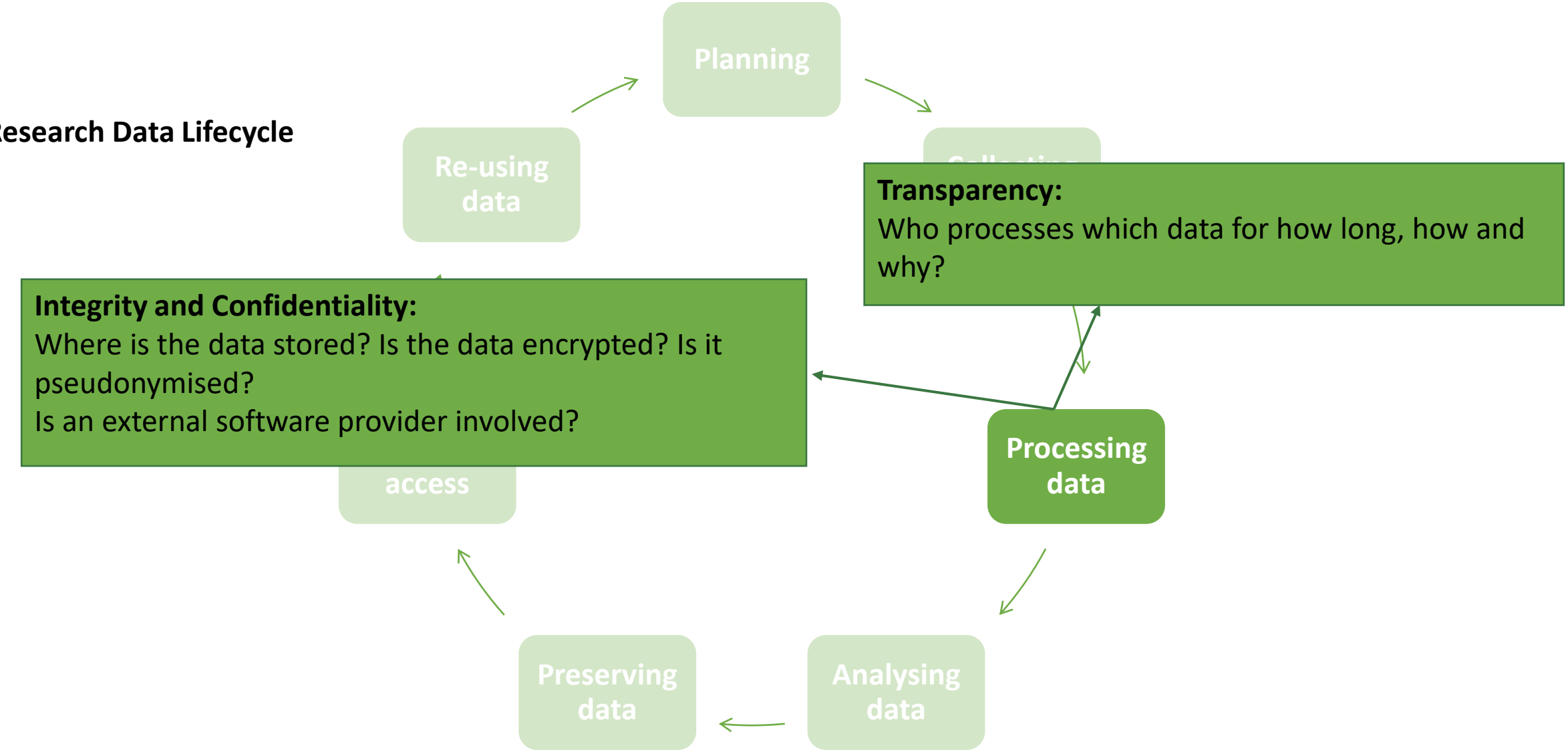
How to comply with the Data Protection Principles?

- **Research Data Lifecycle**



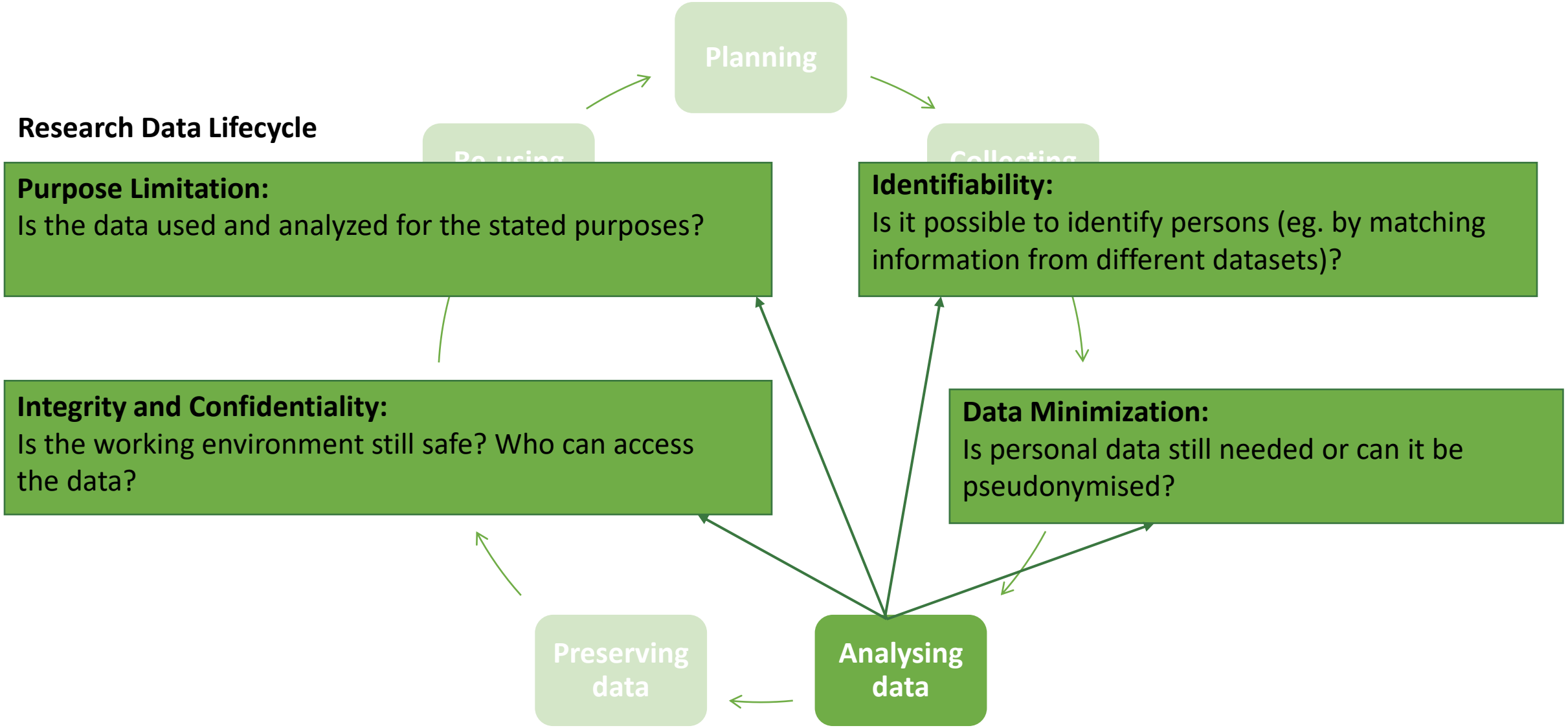
How to comply with the Data Protection Principles?

- **Research Data Lifecycle**



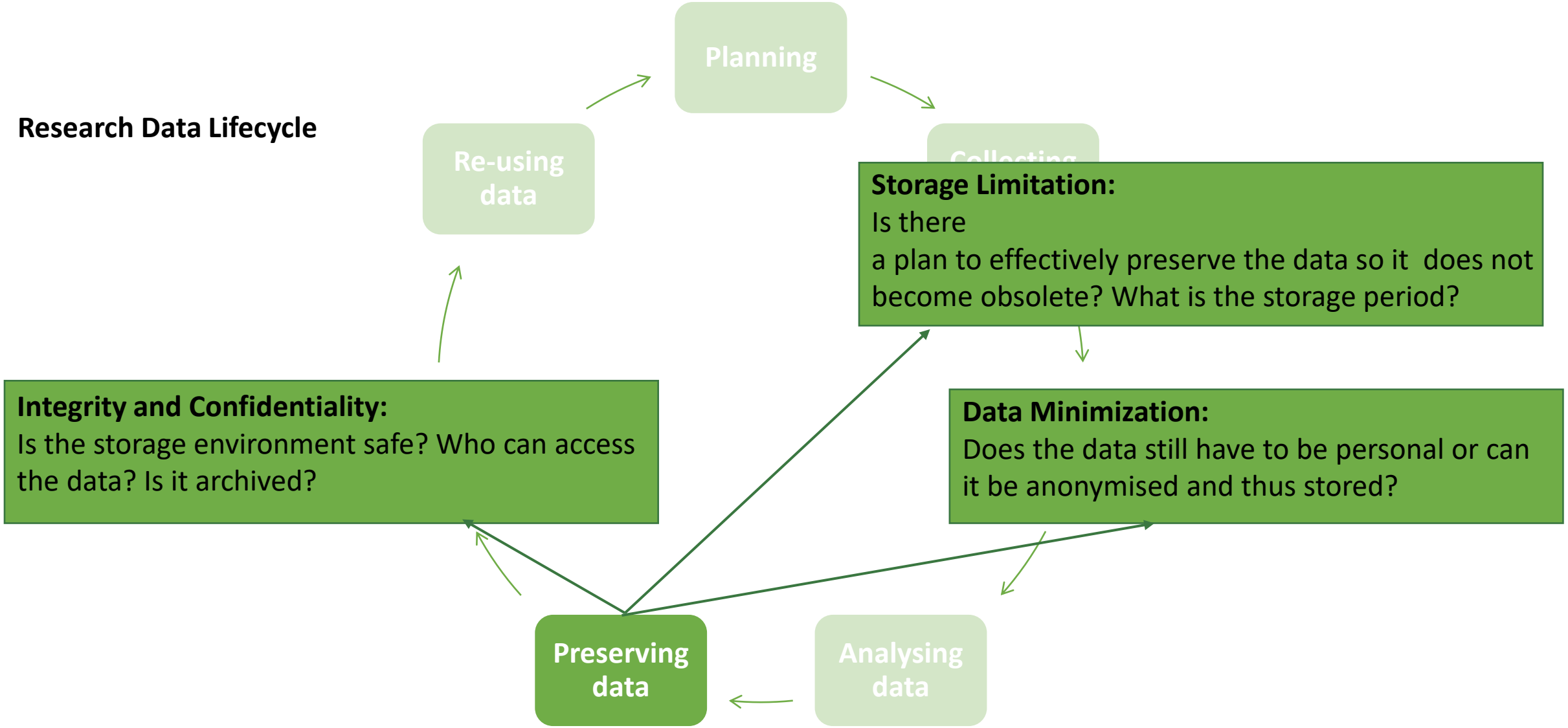
How to comply with the Data Protection Principles?

- **Research Data Lifecycle**



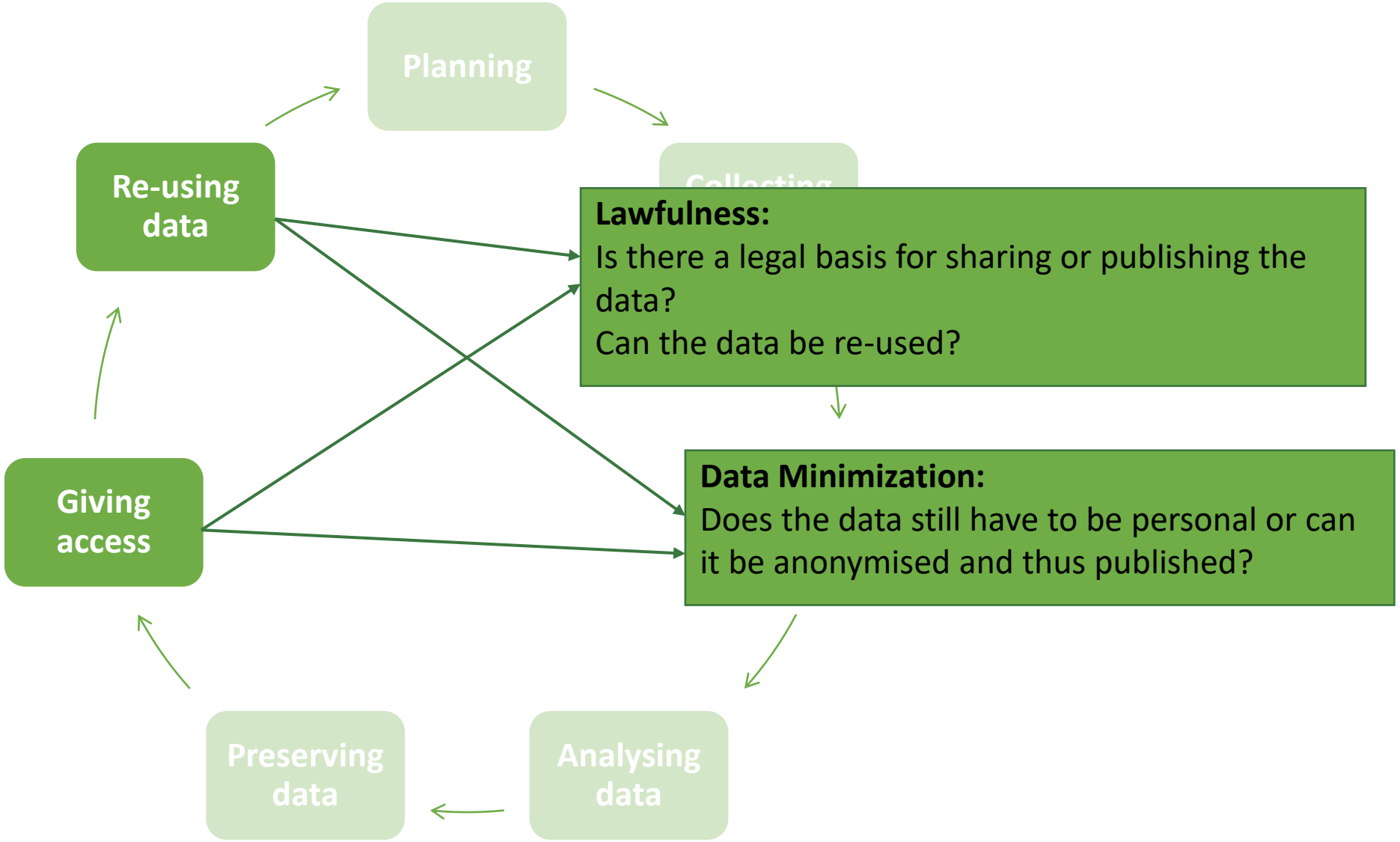
How to comply with the Data Protection Principles?

- **Research Data Lifecycle**



How to comply with the Data Protection Principles?

- **Research Data Lifecycle**



Main Take Aways

Main Take Aways

- **Data privacy, data security and data protection are intertwined.**
- **All three combined define data management strategies and are at the core of privacy laws.**
- **GDPR has set out to balance research with the rights and interests of individuals.**
- **For this reason, it has set 7 Data Protection or GDPR principles to ensure this balance.**

Main Take Aways

Following the 7 Data Protection Principles, researchers should:

- **Make sure they have a legal basis for collecting and processing personal data**
- **Avoid personal data, if it is not needed**
- **Process, analyze and store personal data in a safe environment**
- **Be aware of unwanted identifiability**
- **Regularly check if the data can be pseudonymised or anonymised**

Thank you!

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 460037581

Links and further information

https://www.berd-nfdi.de/

https://www.berd-nfdi.de/newsletter-en/

Overview of iVA:

https://www.berd-nfdi.de/servicestools/legal-questions-in-data-science/

iVA1: https://www.berd-nfdi.de/iva1/

iVA2: https://www.berd-nfdi.de/iva2/

iVA3 (in German): https://www.berd-nfdi.de/iva3/

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – 460037581

iVA: interactive Virtual Assistant

Applicability of the GDPR

iVA1 shows you if the General Data Protection Regulation (GDPR) applies to your research data.

Start here (DE)

Start here (ENG)

Consent as legal basis

iVA2 helps you identify what you have to keep in mind to get a lawful consent for data processing.

Start here (DE)

Start here (ENG)

Research relevant legal bases

iVA3 guides you through the process of determining whether data processing in the context of your research project meets a federal or state legal basis.

Start here (DE)

Is privacy law non-transparent and incomprehensible?
Not necessarily.

https://www.berd-nfdi.de/servicestools/legal-questions-in-data-science/