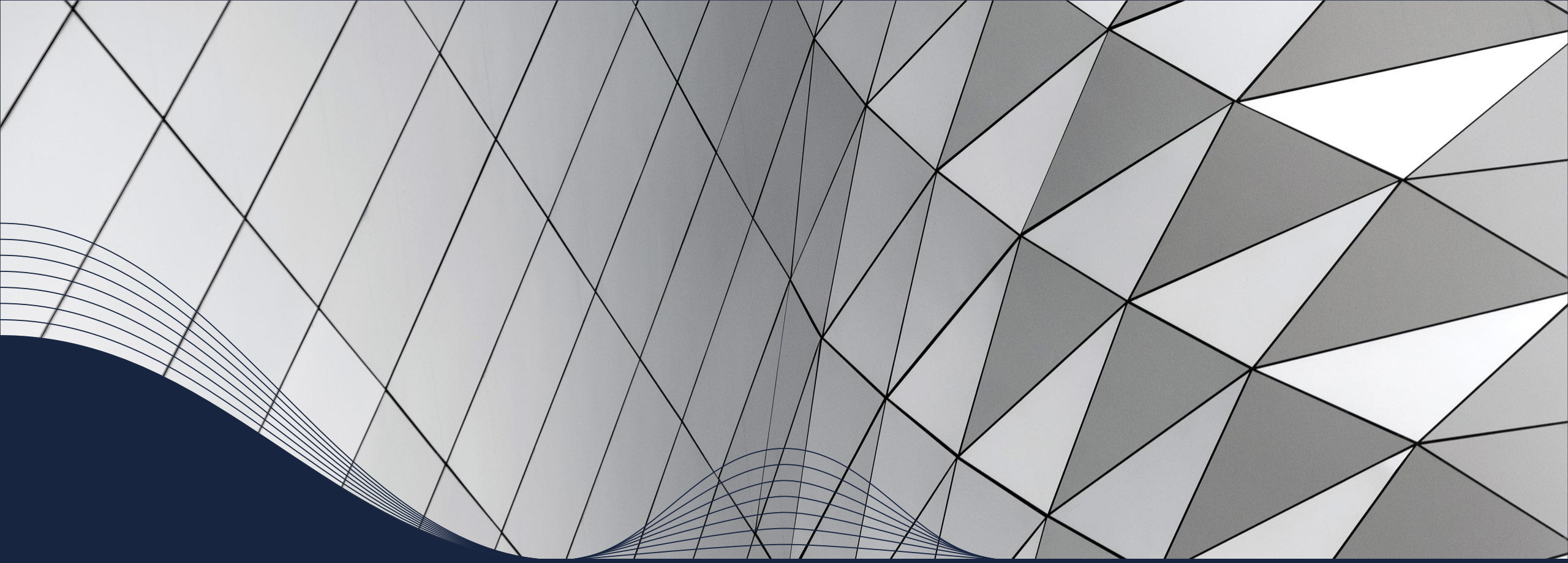


European User Office Meeting 2022

Challenges of and experience with
GDPR compliance for User Offices

DLA PIPER

Contents

- Applicability of GDPR for User Offices
- The role of the User Office under GDPR
- The data processing principles
  - Spotlight: Lawfulness
  - Spotlight: Storage limitation
- Rights of the data subject
  - Spotlight: Right to be forgotten and its' exemptions
- Processing of data for scientific research purposes

Verena Grentzenberg
Partner | Hamburg
IT & Data Security
T: +494 0 188 88 203
M: +49 172 72 57 288
verena.grentzenberg@dlapiper.com

Recognitions

JUVE Handbook 2020/2021: Frequently recommended for data protection; "excellent expertise", client

Legal 500 Germany 2022: Next generation partner and recommended for information technology: data protection; "Verena Grentzenberg is very dedicated, always available and ensures that practical advice is provided within a tight time frame."

Handelsblatt in cooperation with *Best Lawyers 2022:* Recommended for data security and privacy law (for the fifth time in a row)

Applicability of GDPR to User Offices

Scope of GDPR

Material scope

- Processing of personal data by automated means or as part of a filing system (or intended to form part of such a system)
  - Personal data means data relating to identified or identifiable data subjects
- **Not applicable to activities outside the scope of EU law**

Territorial scope

- Establishment in the EU or
- Processing activities related to
  - Offering of goods or services to persons in the EU (irrespective of whether a payment is required)
  - Monitoring of behavior of persons in the EU

Derogations

- Derogations relating to processing (inter alia) **for scientific research purposes**, statistical purposes and archiving purposes in the public interest (Art. 89 GDPR in conjunction with national law)
- Processing by User Offices typically only indirectly serves these purposes

International organizations: not in scope of GDPR

Some scientific research institutes are international organizations

Art. 4 no. 26 GDPR:
“International organisation” means an organisation and its bodies governed (…) on the basis of an agreement between two or more countries.

National law and EU law including GDPR do not apply – international organizations in the EU need to develop own privacy rules (“self-regulation”); however, such rules are often guided by the GDPR.

GDPR treats international organizations as “third countries” with respect to transfers of personal data from the EU – such transfers need to meet the special transfer requirements of the Art. 44 – 50 GDPR, unless there is an international treaty allowing the transfer.

The role of the User Office under GDPR

Roles under GDPR

Controller

- Determines purposes (“why”) and means (“how”) of processing of personal data
- Natural or legal person, public authority or agency

Joint Controller

- When two or more controllers jointly determine “why” and “how” personal data shall be processed
- Must conclude an arrangement setting out their respective responsibilities for complying with obligations under GDPR
- Essence of arrangement must be made available to data subjects

Processor

- Processes personal data only on behalf of the controller (typically, an external party)
- Duties of the processor must be specified in a contract or another legal act (the data processor agreement or “DPA”)
- Example: provision of IT services, including server hosting or cloud storage

Roles of organizations under GDPR

Typical roles of the organization the User Office works for:

Controller

- Determines purposes (“why”) and means (“how”) of processing of personal data
- Natural or legal person, public authority or agency

The organization the User Office works for typically acts as (separate) controller

Joint Controller

- When two or more controllers jointly determine “why” and “how” personal data shall be processed
- Must conclude an arrangement setting out their respective responsibilities for complying with obligations under GDPR
- Essence of arrangement must be made available to data subjects

Processor

- Processes personal data only on behalf of the controller (typically, an external party)
- Duties of the processor must be specified in a contract or another legal act (the data processor agreement or “DPA”)
- Example: provision of IT services, including server hosting or cloud storage

Roles of organizations under GDPR

Typical roles of the organization the User Office works for:

- Determines purposes ("why") and means ("how") of processing of personal data
- Natural or legal person, public authority or agency

The organization the User Office works for typically acts as (separate) controller

Controller

In certain scenarios, the User Office can be a joint controller – for example in the **context of a conference organized jointly with other parties**, the processing of participant data could qualify as joint processing ("JC") and if that is the case, requires a JC arrangement and transparency towards the data subject

Joint Controller

- Processes personal data only on behalf of the controller (typically, an external party)
- Duties of the processor must be specified in a contract or another legal act (the data processor agreement or "DPA")
- Example: provision of IT services, including server hosting or cloud storage

Processor

Roles of organizations under GDPR

Typical roles of the organization the User Office works for:

- Determines purposes (“why”) and means (“how”) of processing of personal data
- Natural or legal person, public authority or agency

The organization the User Office works for typically acts as (separate) controller

Controller

In certain scenarios, the User Office can be a joint controller – for example in the **context of a conference organized jointly with other parties**, the processing of participant data could qualify as joint processing (“JC”) and if that is the case, requires a JC arrangement and transparency towards the data subject

Joint Controller

- Processes personal data only on behalf of the controller (typically, an external party)

When the User Offices engages other parties with processing data on its behalf (e.g., IT service providers), it must conclude a **data processor agreement** (DPA) with the processor on behalf of its organization

Processor

The data processing principles

User Offices – overview processing activities

Application

- Administration of the applications
- Assessment of technical and scientific feasibility of the research project
- Admission of the projects
- Terms and Conditions for Access

Research project

- Providing travel resources and accommodation
- Safety and access regulations
- Providing devices, material and databases

Project completion

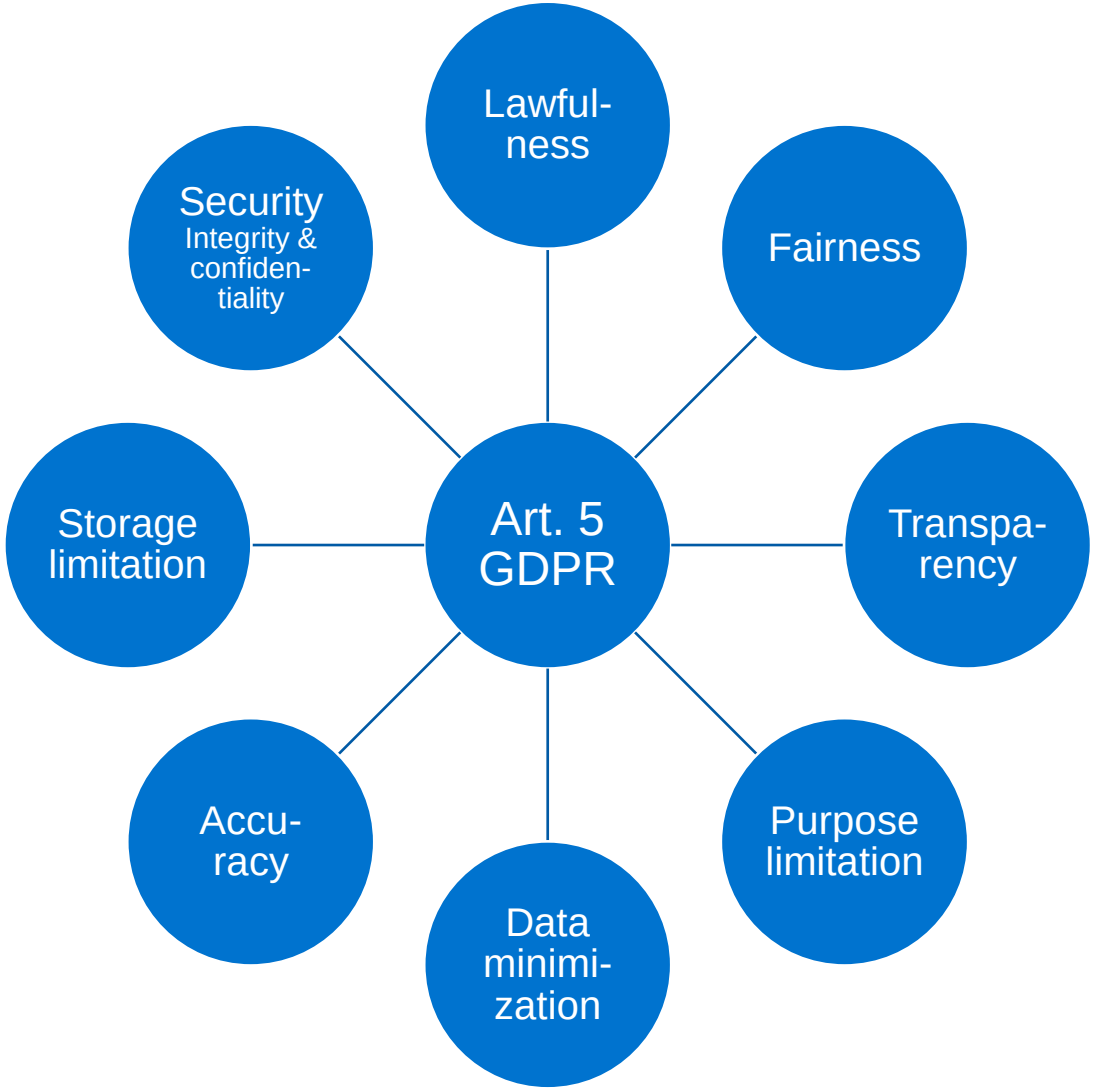
- Analysis
- Experimental reports
- Publication and Open Access
- Surveys

Processing and transfer of data

The data processing principles

Accountability:

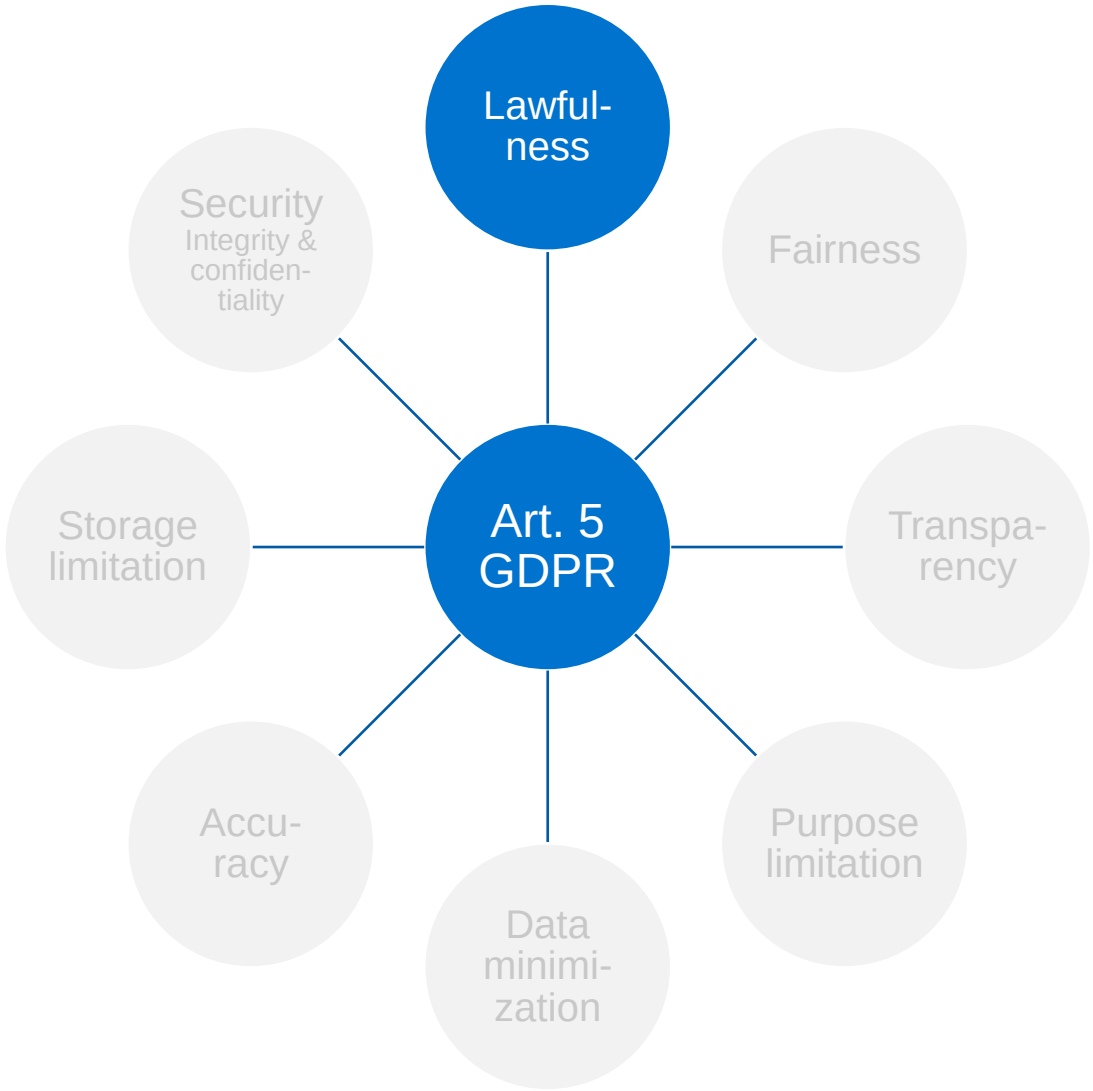
Controllers shall be responsible for and be able to demonstrate compliance with these principles



Spotlight: Lawfulness

Accountability:

Controllers shall be responsible for and be able to demonstrate compliance with these principles



Spotlight: Lawfulness

Overview of legal bases for non-sensitive personal data (Art. 6 (1) GDPR)

- Consent (note: can be withdrawn at any time and only valid if voluntarily given)
- Performance of contract to which person is subject or pre-contractual processing at the request of the person – **most User Office processing activities are justified by this legal basis**
- Compliance with a legal obligation (e.g., under national tax laws, **health and safety regulations**, radiation protection laws and similar)
- Protection of vital interests of a natural person (e.g., in case of an **accident at the facility causing the user to become unconscious**)
- Performance of a task carried out in the public interest (only if the controller was entrusted with a public task by law)
- Legitimate interests of controller or third party (e.g., **non-EU sanction list screenings, surveys**)

Practice example: Sanction list screening by User Offices

Data processing principles: Lawfulness and accountability

What is sanction list screening?

- Obligation to check whether a person or organization is included on a sanctions list due to criminal and terrorist activities
- In this case, this person or organization must not receive any economic resources or financial benefits

Which sanction lists need to be checked?

- User Offices established in the EU are required by law to screen against EU sanction lists – there are no exceptions for scientific research facilities
- Sponsoring organizations/countries outside the EU may additionally require the User Office to screen against their country lists or international lists (e.g., US sanction lists, the UN Sanctions List)
- User Offices outside the EU maybe subject to own country lists (e.g., US or UK sanction lists)

Lawfulness (legal basis)

- Screening of natural persons requires **a legal basis (lawfulness)**
- For EU list screening a legal basis exists for User Offices in the EU, but there is debate as to whether it is „compliance with a legal obligation“ or „legitimate interests“
- For non-EU lists or User Offices not subject to EU law in general, the only available legal bases are legitimate interests or consent

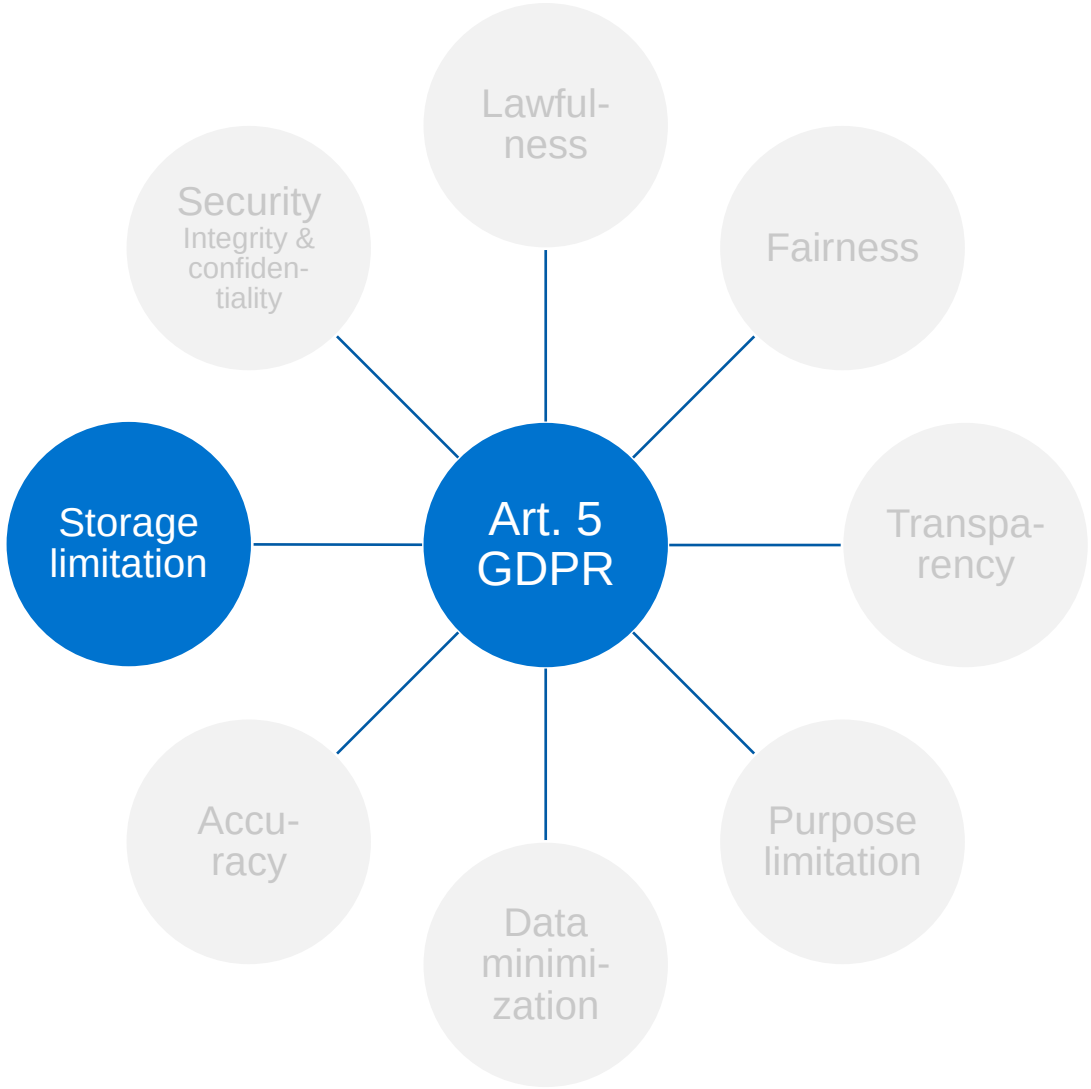
Additional requirements depending on legal basis

- If User Office relies on legitimate interests, a balancing test (“LIA”) is required, which must be **documented (accountability)**
- Balancing test will be influenced by aspects like (i) frequency and (ii) how positive hits are dealt with – note: supervisory authorities have different expectations, which should be known
- For consent to be valid, strict requirements need to be complied with (active, specific, **informed**, voluntary)

Spotlight: Storage limitation

Accountability:

Controllers shall be responsible for and be able to demonstrate compliance with these principles



Spotlight: Storage limitation

Organizations should not keep personal data for longer than needed for the original purpose

Organizations should perform periodic reviews to identify, and address, data stored beyond intended use

Storing personal data beyond initially stated purpose might be allowed if it is for archiving in the public interest, **scientific** or historical **research**, or statistical purposes

Legal retention periods may require longer storage; e.g., deriving from tax laws, commercial law, employment- and social-insurance laws, health and safety regulations, radiation protection laws

Spotlight: Storage limitation

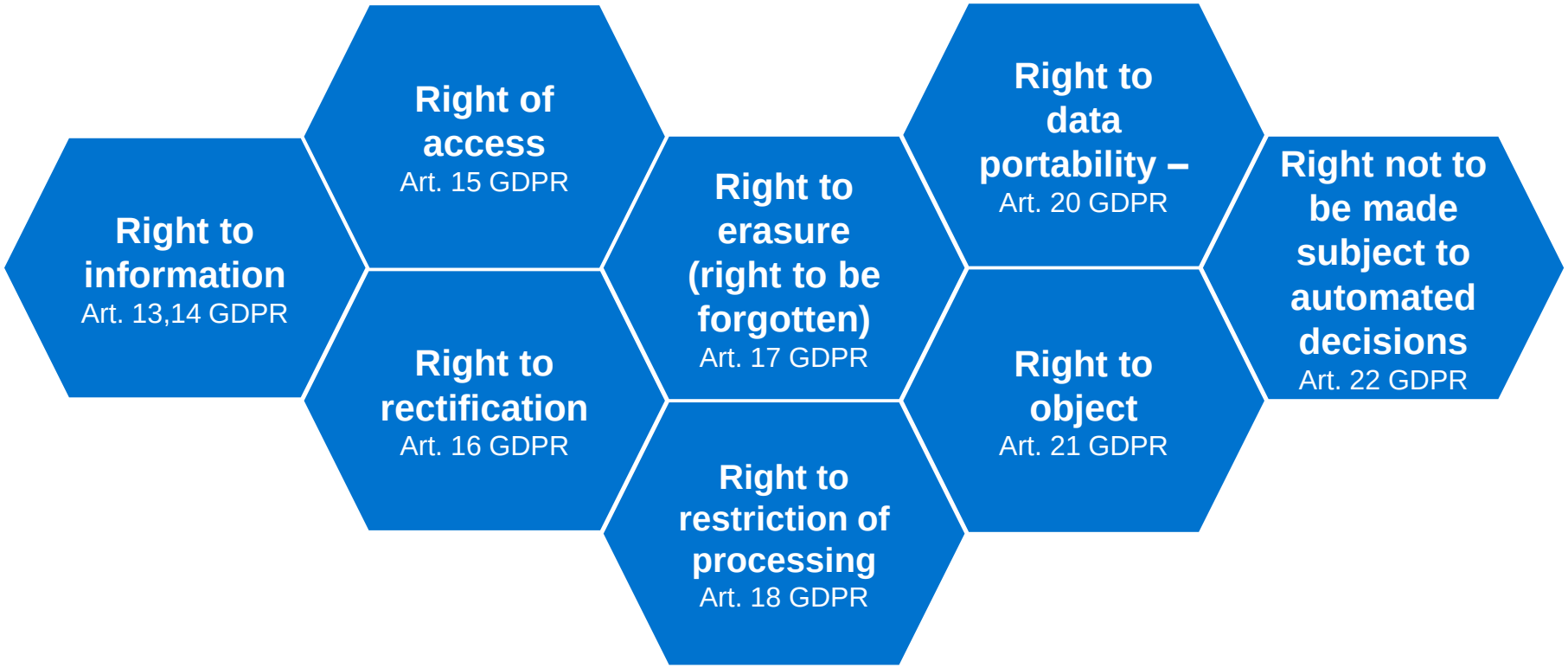
Recommendations for compliance with the principle:

- Determination of maximum storage period per data set, considering legal retention periods and – where no such exist – applicable limitation periods (note: not all data can automatically be stored until the end of the limitation period, in particular if the limitation period is longer than five or even ten years)
- Implementation of (ideally automated) deletion routines with exceptions for specific cases, e.g., legal dispute, scientific relevance (if the requirements for further storage are met)
- No or **strictly limited storage of unstructured personal data** (e.g., in emails, in excel files, on local devices) because such data typically is not captured by deletion routines

Rights of the data subject

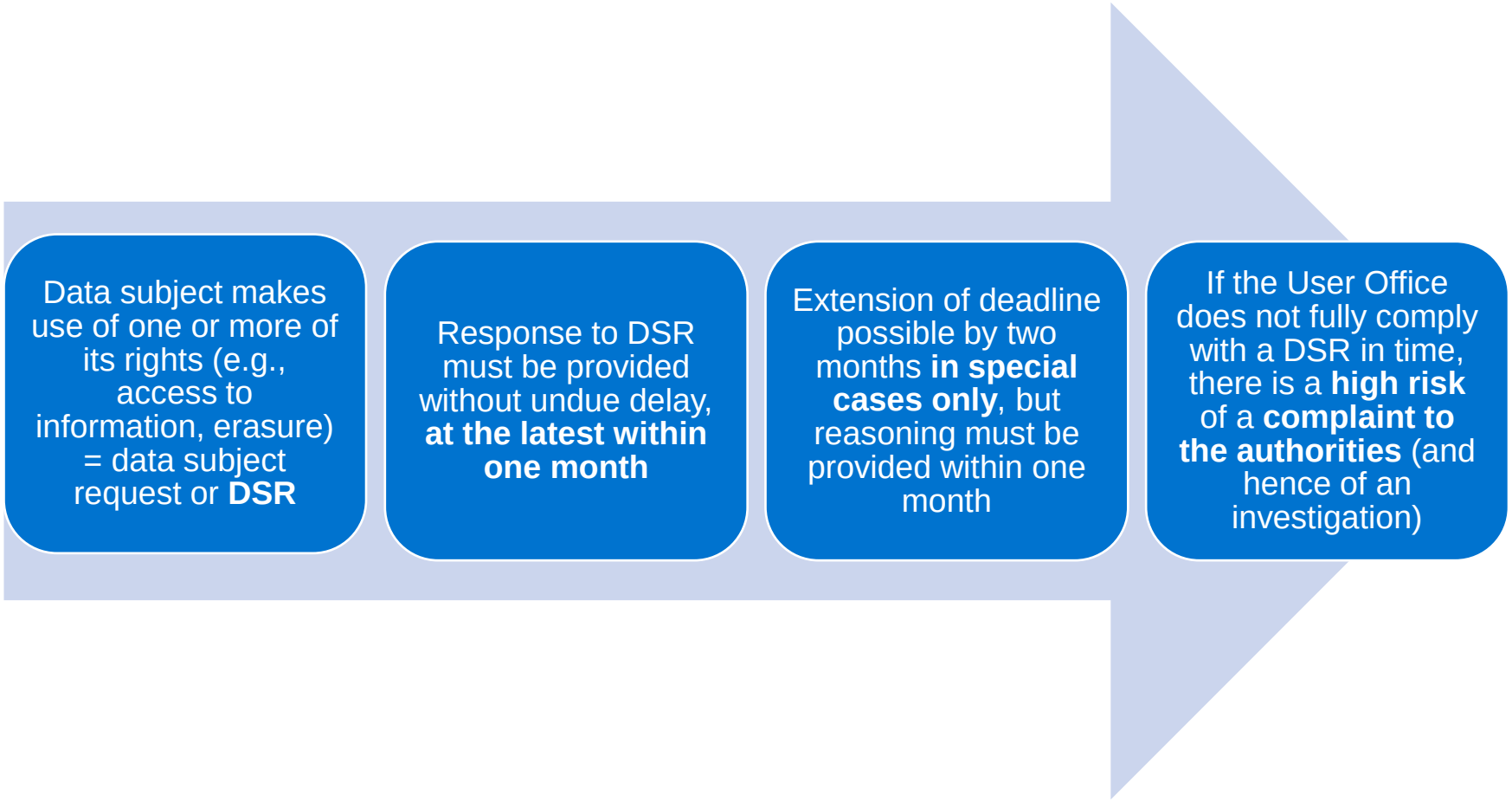
Art. 12-22 GDPR

Rights of the data subject: Overview



Rights of the data subject: Modalities

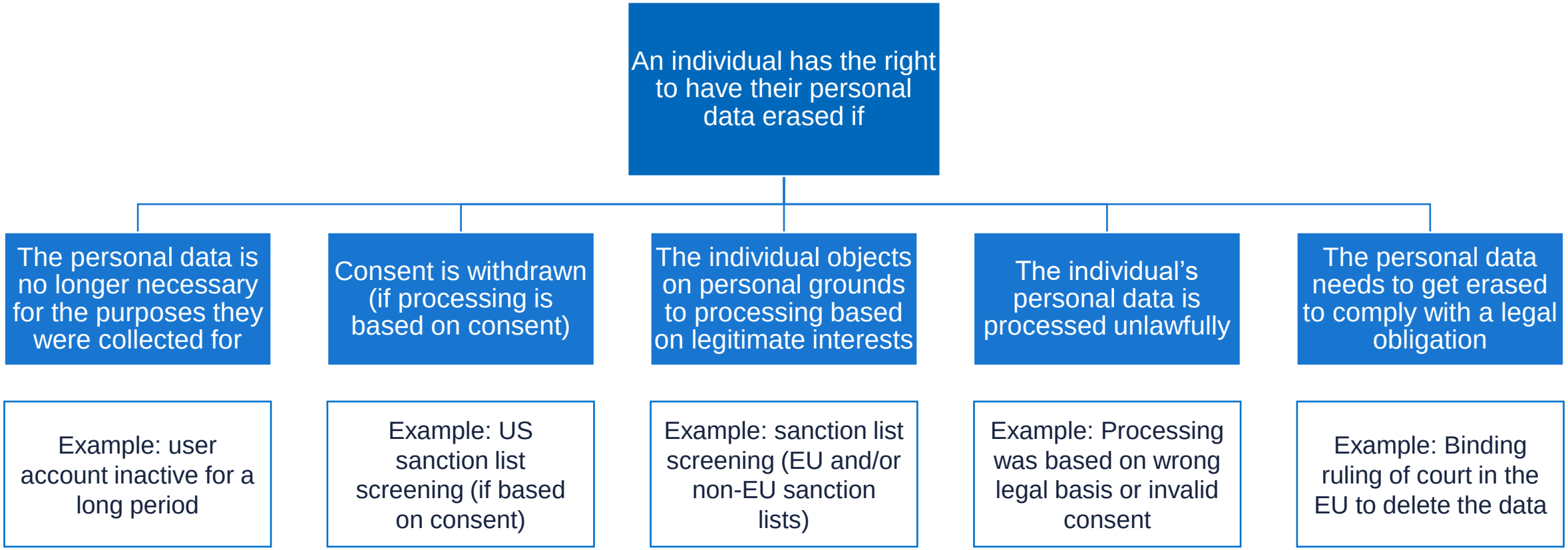
Modalities for compliance with data subject requests (DSRs):



- Establishment of an internal process for the dealing with DSRs is crucial - every User Office should have a **DSR policy** in place!
- **IT systems** used for the processing of the user data must be designed in a way that allow for personal data to be easily localized **and** deleted, if necessary
- **Unstructured data** are a serious challenge and should be avoided from the outset (emails with annexes or even excel files, local storage of user data)

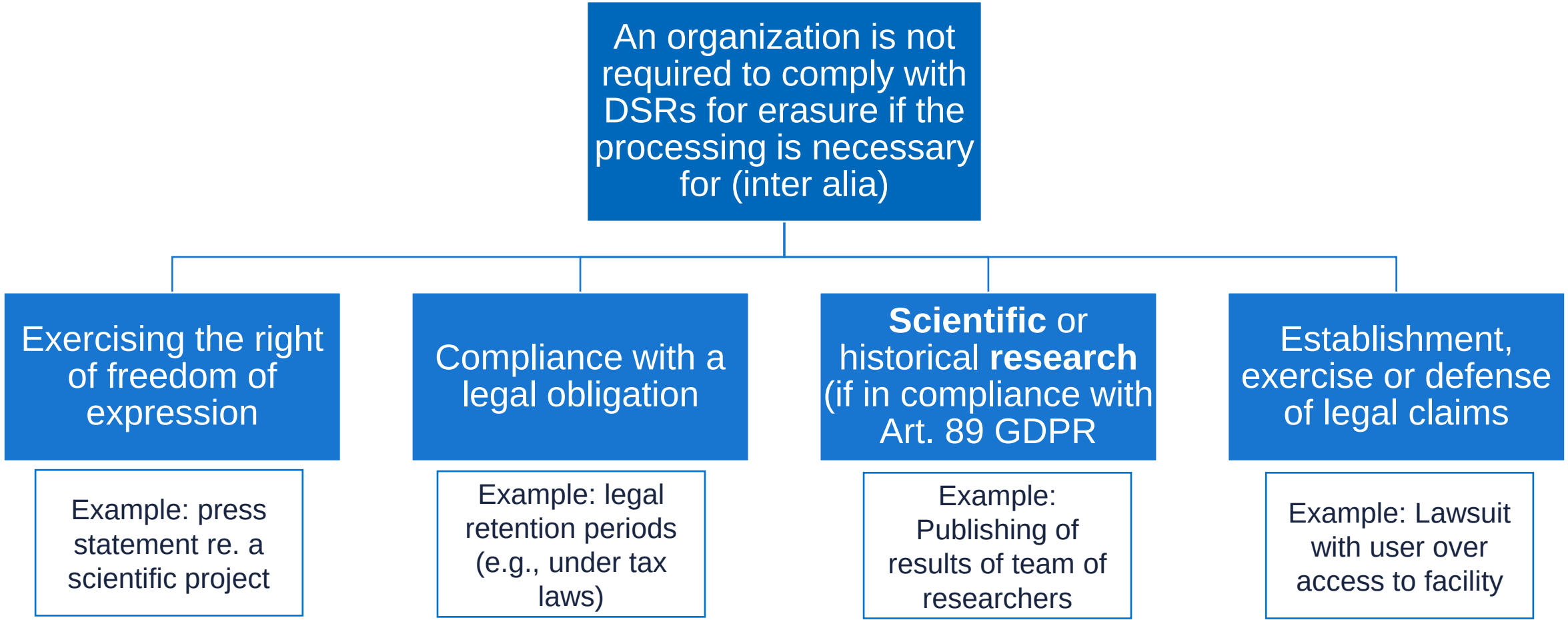
Spotlight: Right of erasure ("right to be forgotten") (1)

The GDPR gives individuals the right to request deletion of their personal data:



Spotlight: Right of erasure ("right to be forgotten") (2)

There are legal exemptions from the right of erasure:



Spotlight: Right of erasure (“right to be forgotten”) (3)

Legal exemption: scientific or historical research purposes or statistical purposes

Despite a request for erasure from an individual, its personal data doesn’t need to be deleted from scientific publications, research papers and databases insofar as this would seriously impair the purpose of the processing, e.g., because the

- Absence of data significantly reduces the statistical validity of results
- Processing relies on completeness of data

Pre-requisite: Compliance with Art. 89 GDPR, which means that certain **safeguards** need to be met

Processing of data for scientific research purposes

Processing for scientific research purposes: Privileges

Processing (inter alia) **for scientific research purposes**, statistical purposes and archiving purposes in the public interest can be subject to certain privileges

- **Principle of purpose limitation**: GDPR assumes that the "*further processing for archiving purposes in the public interest, **scientific** or historical **research purposes** or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*"
  - This means that a User Office could potentially further process user data initially (only) collected for the purpose of granting access to the facility also for scientific purposes
- **Data subject's rights**: GDPR provides for an exemption from the right of erasure and Member State law may provide for derogations from the rights of access and the right of rectification
- Pre-requisite for any privilege: certain safeguards need to be met (see next slide)

Processing for scientific research purposes: Safeguards

General recommendations for safeguards for personal data use for scientific research under Art. 89 GDPR

Pseudonymization and Anonymization

- Specify where there is a need for pseudonymous data and anonymous data and the specific order to follow

Sensitive and non-sensitive data should be treated differently

- Sensitive and non-sensitive data pose different risks
- Distinguish and provide detailed requirements for safeguards for sensitive data

Research and data management plan

- In several EU countries a detailed research / data management plan is required, either by law or by national guidelines

Technical and organizational measures

- Confidentiality, access control procedures and access logging, restricted areas, encryption, personnel training, monitoring of measures
- Roles and responsibilities to be defined

Guidelines for scientific research

- Many EU countries have established practices and/or rules of conduct for (funded) research by national scientific research centers

Guidelines for publication and dissemination

- Personal data for publications and/or disseminations must undergo a technical process to prevent or hinder identification of the data subject (e.g., proper pseudonymization or anonymization)

Source: Study on the appropriate safeguards under Article 89(1)GDPR for the processing of personal data for scientific research, Final Report, EDPS/2019/02-08

Thank you

Verena Grentzenberg
Partner | Hamburg
T: +49 40 188 88 203
M: +49 172 72 57 288
verena.grentzenberg@dlapiper.com