Universität Konstanz

Data protection law and research
Nothing but a nuisance?

Peter Brettschneider

2021/6/24

Contents

1. Introduction
2. Applicability
3. Lawfulness of processing
4. Basic principles
5. Bureaucracy – forms and documents
6. An effort worth while?

1. Introduction

1. How important is data protection law in your opinion? Please rate

    - essential guarantee (1)
    - fairly important (2)
    - Indifferent (3)
    - nuisance (4)

1. Introduction

2. What effects has data protection law had on your research projects?

   - I have never experienced any adverse effects. (1)
   - It has complicated / stalled projects on occasion. (2)
   - It has at least on one occasion prevented a planned project. (3)

Data protection a fundamental right

- The protection of personal data is not just a legal obligation, it is a **fundamental right**!
- **Art. 8 EU Charter of Fundamental Rights**: “Everyone has the right to the protection of personal data concerning him or her.”
- Essential prerequisite for democracy and an open society in a digital age.

2. Applicability

- Applicable law
- Personal data
- Anonymous data

Example – Mrs. Merkwürdig’s data

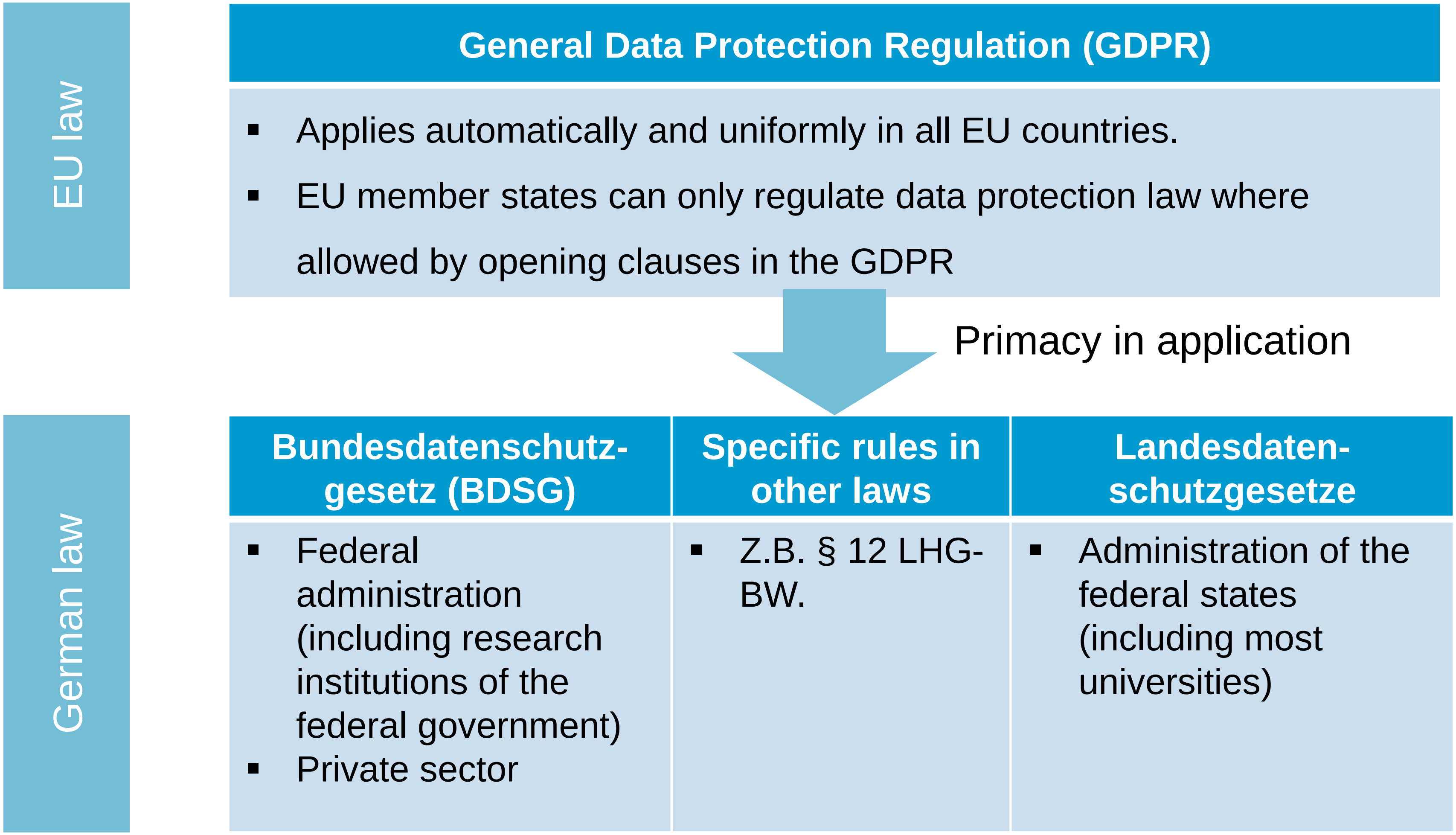
Mrs. Merkwürdig, a scientist at the University of Konstanz, studies the effects of working at home. In a questionnaire she collects inter alia the following background information:

- Gender
- Position (professor / post-doc / PhD-candidate)
- Department
- Years working at the University of Konstanz (> 10 / 5-10 / < 5 years)

Questions:

1. Which laws regulate the issue?
2. Data protection law only concerns personal information. To what extend is this the case concerning the collected background information?

Applicable law (anwendbares Recht)



EU law

General Data Protection Regulation (GDPR)

- Applies automatically and uniformly in all EU countries.
- EU member states can only regulate data protection law where allowed by opening clauses in the GDPR

Primacy in application

German law

Bundesdatenschutzgesetz (BDSG)	Specific rules in other laws	Landesdatenschutzgesetze
▪ Federal administration (including research institutions of the federal government) ▪ Private sector	▪ Z.B. § 12 LHG-BW.	▪ Administration of the federal states (including most universities)

Example – Mrs. Merkwürdig’s data

Mrs. Merkwürdig, a scientist at the University of Konstanz, studies the effects of working at home. In a questionnaire she collects inter alia the following background information:

- Gender
- Position (professor / post-doc / PhD-candidate)
- Department
- Years working at the University of Konstanz (> 10 / 5-10 / < 5 years)

Questions:

1. Which laws regulate the issue?

GDPR + Landesdatenschutzgesetz BW + special rules in other laws

Personal data (personenbezogene Informationen)

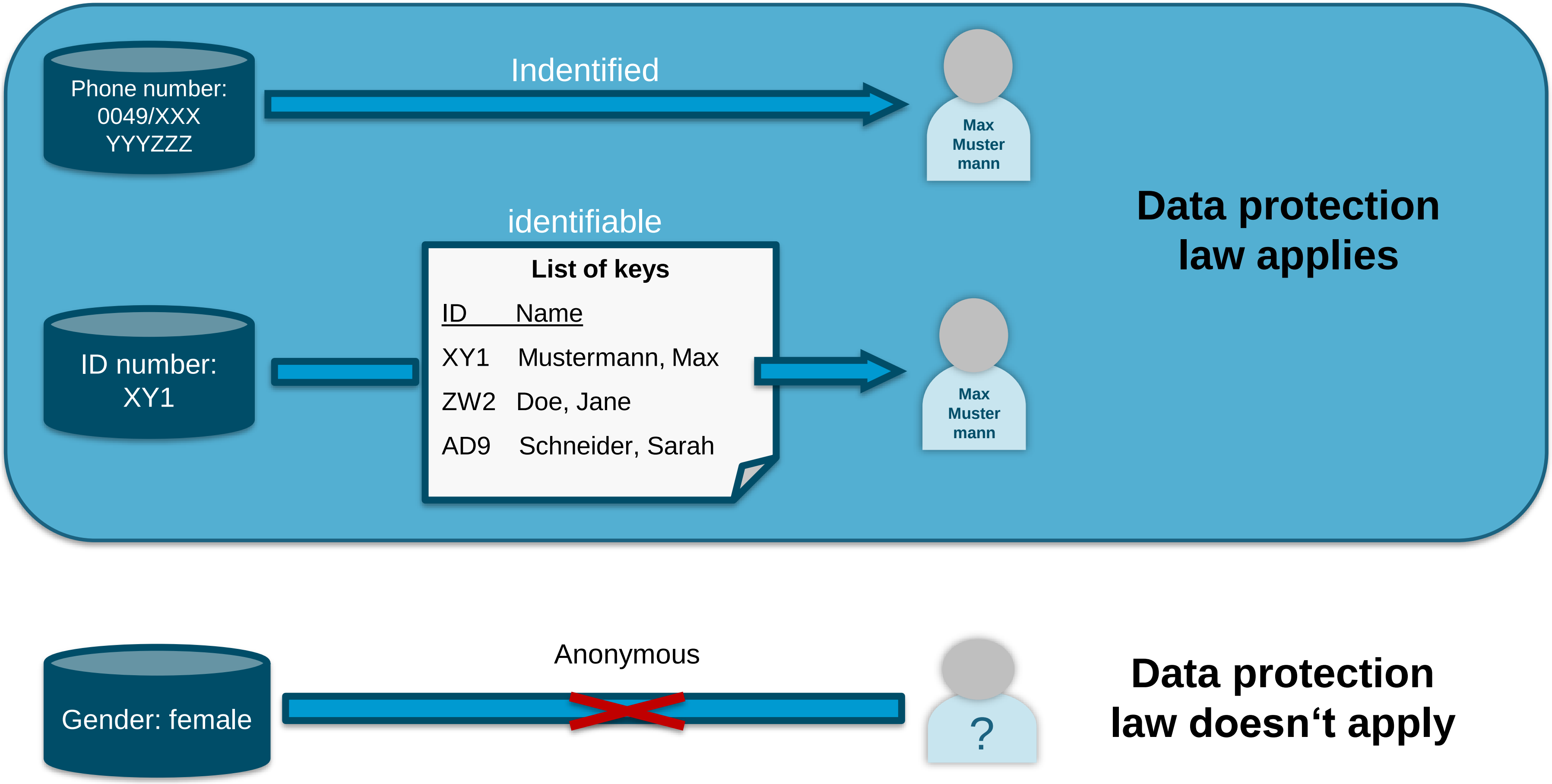
Personal data (Art. 4 No° 1 GDPR)

- Any **information relating to an identified or identifiable natural person**.
- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data

- **Persons**:
  - Only living persons.
  - No legal entities
- **Citizenship**: irrelevant; non EU-citizens are protected as well.

Identified / identifiable / anonymous



Phone number: 0049/XXX YYYZZZ

Indentified

Max Muster mann

identifiable

ID number: XY1

List of keys

ID	Name
XY1	Mustermann, Max
ZW2	Doe, Jane
AD9	Schneider, Sarah

Max Muster mann

Data protection law applies

Gender: female

Anonymous

?

Data protection law doesn‘t apply

Illustration: derivation of Ziedorn, Datenschutz 2021, S. 15.

Example – Mrs. Merkwürdig’s data

Mrs. Merkwürdig, a scientist at the University of Konstanz, studies the effects of working at home. In a questionnaire she collects inter alia the following background information:

- Gender
- Position (professor / post-doc / PhD-candidate)
- Department
- Years working at the University of Konstanz (> 10 / 5-10 / < 5 years)

Questions:

2. Data protection law only concerns personal information. To what extend is this the case concerning the collected background information?

Example A

Information	Legal assessment
Gender	Roughly half the human population
Position	University of Konstanz: > 200 professors ; > 1.000 PhD candidates
Department	No identification
Years working at the university	No identification
Combination of this data	Example: Gender + position + department can identify a person. E.g. low number of female professors in certain departments (computer sciences, law, mathematics)

Context and combination of information

- **Job / job title**:
  - In the general population usually not unique ; however it can be in a more limited context (e.g. within a single organization / enterprise).
  - Combining the job title with the information that someone is working at the University of Konstanz can identify some persons (e.g. there is only one dean of section 3, only one CIO). On the contrary a PhD candidate remains unidentifiable!
- **Name**:
  - Even a name isn’t necessarily personal information. E.g. Thomas Müller.

Perspective

- **Controller**: natural or legal person which determines the purposes and means of the processing of personal data (Art. 4 No° 7 GDPR).
- Different controllers have different means to identify a person.
- Example: **dynamic IP addresses**
  - An internet provider can identify which user dialed into its WLAN.
  - A scientist usually won’t.
- Example: **publishing research data**
  - Whose perspective is decisive? That of other scientists? That of particularly well-informed third parties (e.g. internet giants, secret services)?

Means

- To determine whether a natural person is identifiable, **all the means reasonably likely to be used** should be taken into account.
- Considerations:
    - cost
    - amount of time required for identification
    - available technology at the time of the processing
    - technological developments

Conclusion

1. **Any trait** that distinguishes a person from the rest of the population. The less persons share a trait , the more likely will it result in identification.
2. **Context is key**: Often only the combination of information makes a person identifiable.
3. **Perspective is key**: Whether information constitutes personal data depends on the **data controller** and the **means** at his disposal: Data may be anonymous in the hand of one controller but identify a person in that of another one.

More examples

Type of information	Examples
Personal identifiers	▪ **Student number** ▪ **IP address** (problematic: dynamic IP addresses) ▪ **Tax number** ▪ **Phone number** ▪ **Email address**
Biographical information	▪ Date of birth ▪ **CV**
Biological information	▪ Eye color ▪ Weight ▪ Appearance
Health information	▪ **Medical history** ▪ **Genetic data**
Religion, politics	▪ Religious and political opinions
Professional and private life	▪ Hobbies ▪ Memberships ▪ Occupation
Recordings / photos	▪ **Video recording** ▪ **Audio recording** ▪ **Photos**
Location data	▪ **Geotracking** ▪ **Address**

Anonymous data

Anonymization:

- Data protection law doesn’t apply to data rendered anonymous!
- Render research data anonymous as early as your research purpose allows it (§ 13 LDSG BW).

Pseudonymization: replacing personal information with keys / pseudonyms

- Data protection law remains applicable.
- Reduces risks for data subjects – easier to justify.

Methods of anonymization

Method	Example	
Deleting identifying attributes	Date of birth: 1988/6/20	Date of birth: XXXXXX
Aggregating data	Age Person A: 37 Age Person B: 23 Age Person C: 55 Age Person D: 29	Average Age: 36
Replacing attributes with more general information	Profession Person A: plummer	Profession Person A: craftsman
Differential privacy	Algorithms using aggregation methods and adding a statistical blur.	

Degrees of anonymization

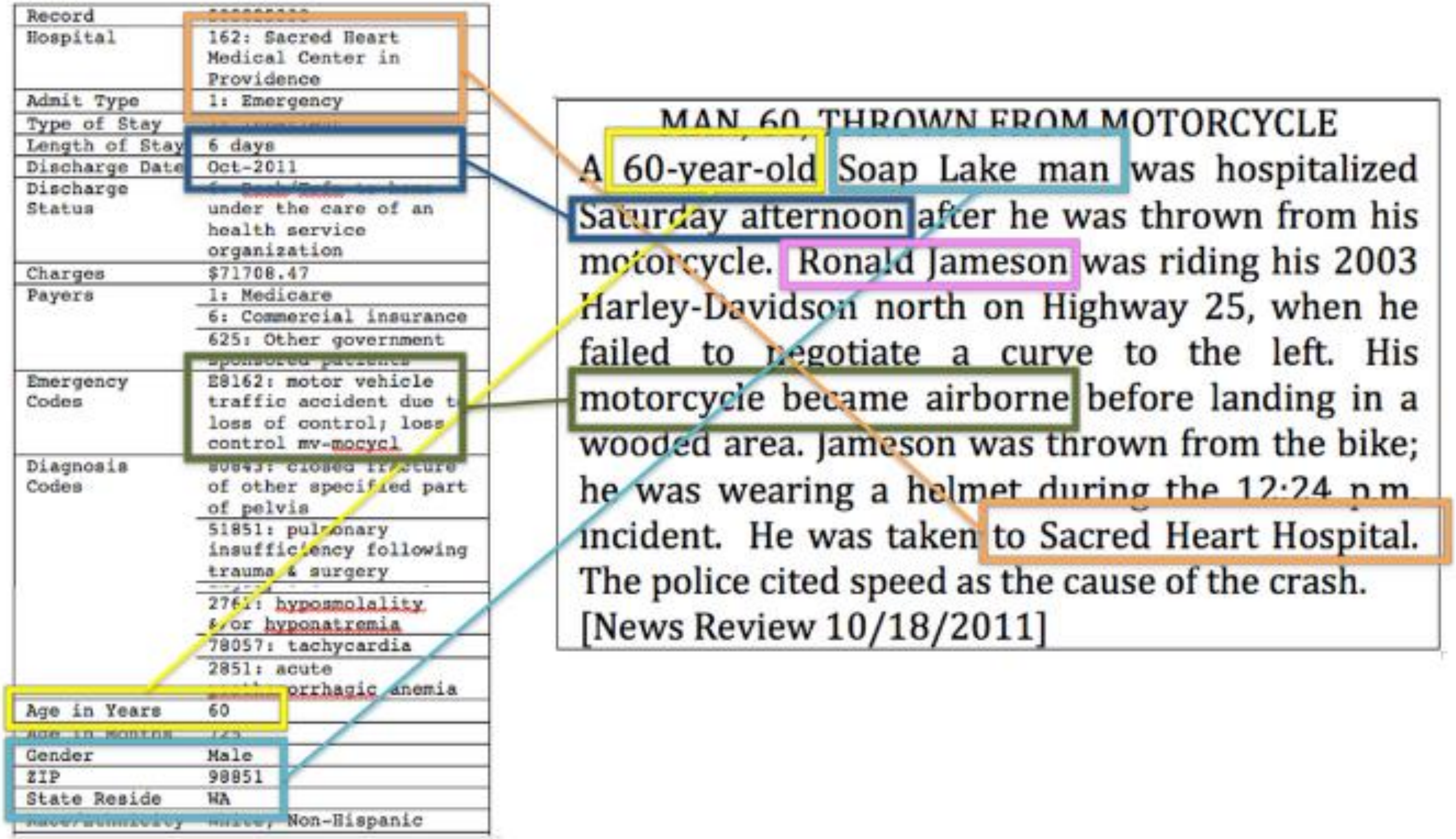
- **Absolute anonymity**: Nobody is able to identify the data subjects(s).
  - Highest standard but usually not legally required – exception official statistics.
- **Factual anonymity**: Deanonymization is not possible with an amount of effort that has to be reasonably expected.
  - Sufficient.
- **Formal anonymity**: All attributes that can directly identify a person are deleted.
  - Usually insufficient! Ignores the possibility of combining information.

Anonymization in practice

Example: Washington State, USA – public health records	
Hospital	162: Sacred Heart Medical Center in Providence
Length of Stay	6 days
Emergency Code	E8162: motor vehicle traffic accident due to loss of control
Age	60
Gender	Male
ZIP	98851
State of Residence	WA

Question: Is this data anonymous?

Anonymization in practice



Record	[illegible]
Hospital	162: Sacred Heart Medical Center in Providence
Admit Type	1: Emergency
Type of Stay	[illegible]
Length of Stay	6 days
Discharge Date	Oct-2011
Discharge Status	6: Disch/Trnsfr to home under the care of an health service organization
Charges	$71708.47
Payers	1: Medicare 6: Commercial insurance 625: Other government sponsored patients
Emergency Codes	E8162: motor vehicle traffic accident due to loss of control; loss control mv-mocycl
Diagnosis Codes	80843: closed fracture of other specified part of pelvis 51851: pulmonary insufficiency following trauma & surgery 2761: hyposmolality &/or hyponatremia 78057: tachycardia 2851: acute posthemorrhagic anemia
Age in Years	60
Age in Months	725
Gender	Male
ZIP	98851
State Reside	WA
Race/Ethnicity	White, Non-Hispanic

MAN, 60, THROWN FROM MOTORCYCLE

A 60-year-old Soap Lake man was hospitalized Saturday afternoon after he was thrown from his motorcycle. Ronald Jameson was riding his 2003 Harley-Davidson north on Highway 25, when he failed to negotiate a curve to the left. His motorcycle became airborne before landing in a wooded area. Jameson was thrown from the bike; he was wearing a helmet during the 12:24 p.m. incident. He was taken to Sacred Heart Hospital. The police cited speed as the cause of the crash. [News Review 10/18/2011]

Sweeney: Only You, Your Doctor, and Many Others May Know, Technology Science, 2015092903. September 28, 2015. https://techscience.org/a/2015092903/

Tools

- Tools can be highly useful but usually can‘t fully replace manual effort.
- Example: FDZ Qualiservice with **QualiAnon** for sociological data (https://www.qualiservice.org/de/helpdesk/webinar/tools.html)

3. Lawfulness of processing

Any processing personal data is **prohibited unless justified** by one of the six lawful bases in Art. 6 GDPR.

Lawful bases

Art. 6 GDPR	
Consent	Data subject has agreed to the processing of his personal data.
Contract	A contract with the data subject makes processing his data necessary.
Legal obligation	Processing is necessary in order to comply with a legal obligation.
Vital interest	Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
Task in the public interest	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
Legitimate interest	Processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Consent

Conditions

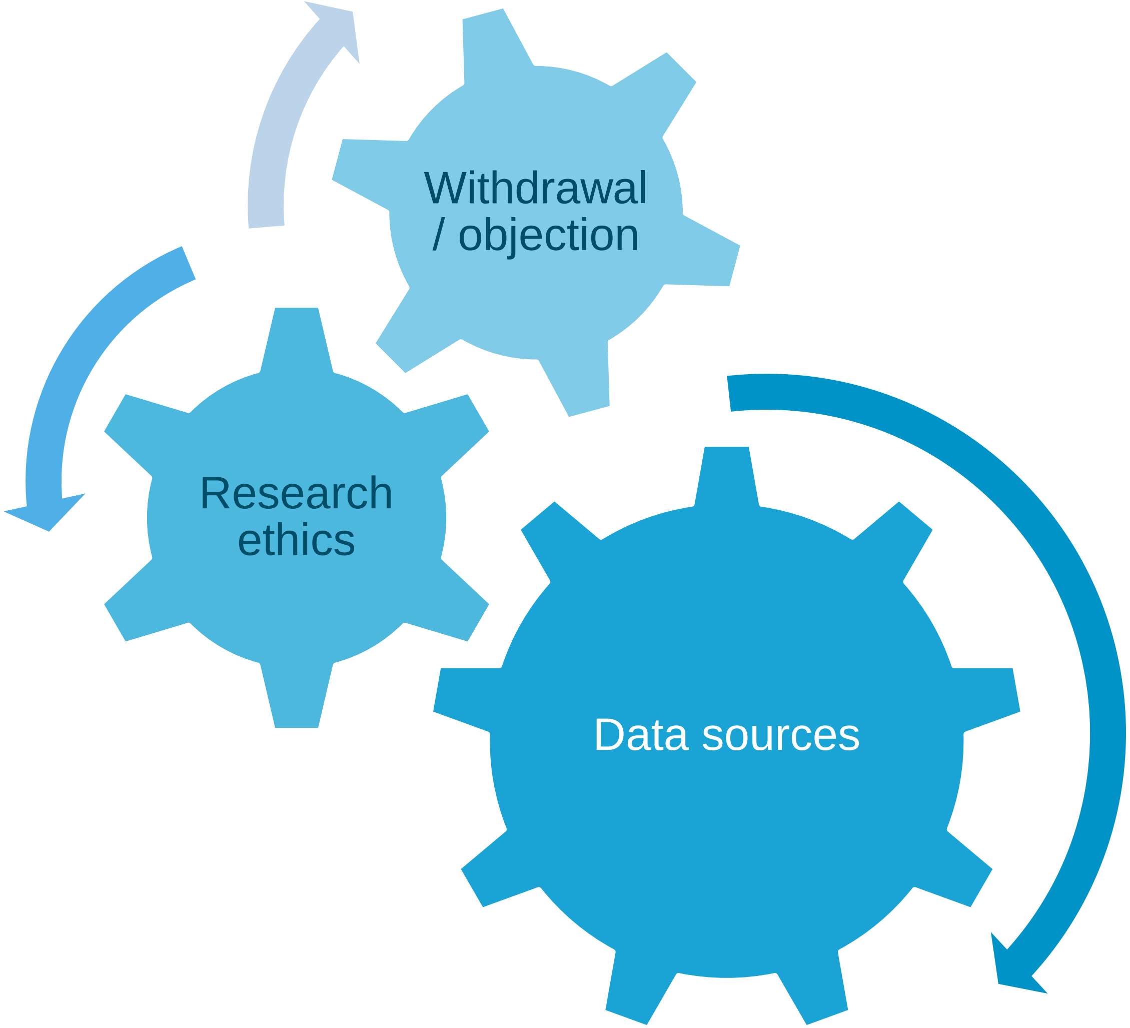
1. **Voluntary:** data subjects must have a genuine choice. There must be no detriment to refusal.
2. **Informed:** data subject must be able to appraise the risks (minimum: identity of the controller, purpose of the data processing). Detailled information duty Art. 13 GDPR!
3. **Specific:** consent must express the specific purpose. Carte blanche / broad consent are usually illegal (exception medical research with pseudonymized data).

- **No form requirements** (exception Art. 7 Section 2). But controller must be able to demonstrate the consent. Documentation!
- **Prior** to the data processing. No consent ex post.

Countermeasures open to data subjects

Art. 6 GDPR	
Consent	**Right to withdraw consent** at any time (Art. 7 GDPR). ▪ Doesn‘t affect the legality of the data processing to this point. ▪ Triggers a **duty to delete** the personal data. ▪ Removes legal basis for the future.
Task in the public interest	**Right to object** (Art. 21 GDPR): ▪ Data is processed for research purposes ▪ Data subject has, on grounds relating to his particular situation, the right to object to processing. ▪ Exception: processing is necessary for a task in the public interest.
Legitimate interest	

Choosing the adequate legal bases



Special categories of personal data

Personal data revealing:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs,
- trade union membership

Processing of:

- genetic data,
- biometric data
- data concerning health,
- data concerning sex life or sexual orientation

- **Higher requirements** regarding a legal basis (Art. 9 GDPR)
- Balanced by **special rules for scientific research** (§ 13 LDSG BW ; § 27 BDSG)

Excursus: Responsibility / liability

Example – Mrs. Merkwürdig's data: Mrs. Merkwürdig acquired the consent of all participants. However one of them later withdraws his consent. Since this could affect the results of her study, the scientist doesn't want to delete the record.

Questions:

1. Who is responsible (= controller) for processing the data?
2. Mrs. Merkwürdig wants to know what could happen if she ignores the request.

Excursus: Responsibility / liability

Example – Mrs. Merkwürdig's data:

Questions:

1. Who is responsible (= controller) for processing the data?

   Data protection law: Scientist can only be the controller if she acts on her own accord without a directive from the university.

2. The scientist wants to know what could happen if she ignores the request.

   Data protection law: warnings, order to stop violations of data protection law / stop data processing

   Civil law: Any person in an employment relation with the university is only liable for damages personally if she acts with severe negligence or deliberately.

4. Basic principles

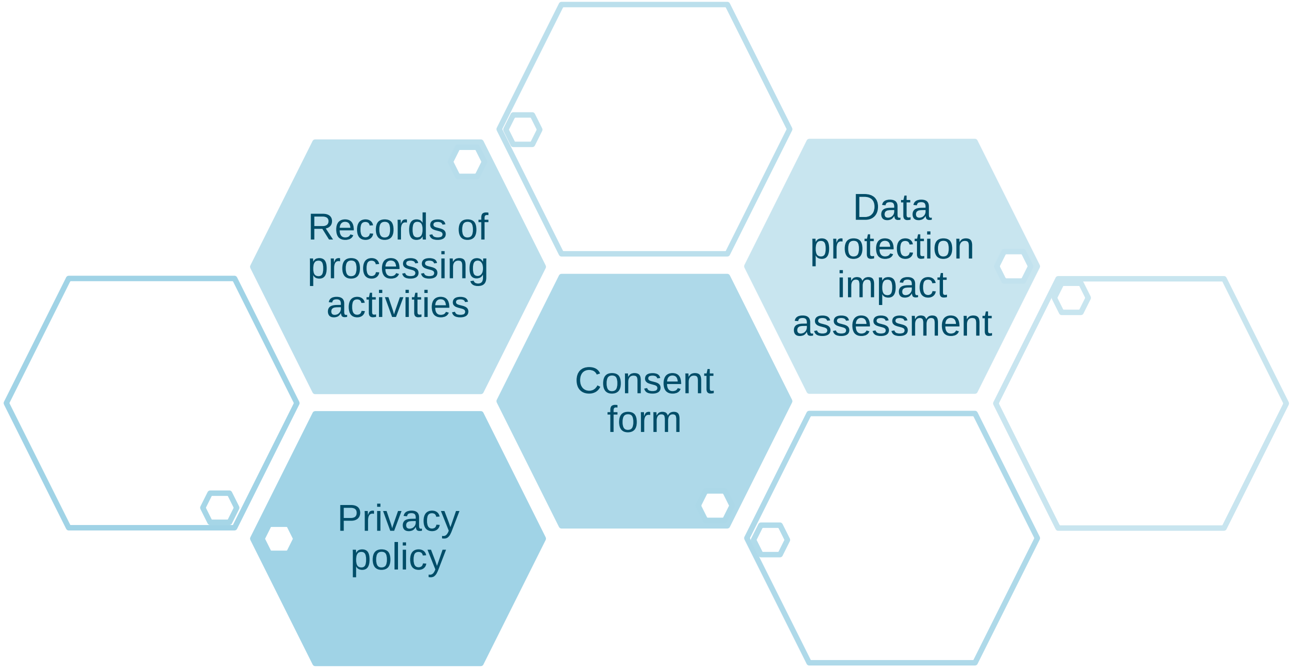
Principles relating to processing of personal data

Art. 5 GDPR	
Lawful, fair, transparent	▪ Lawful: Art. 6 GDPR in more general terms. ▪ Fair: blanket clause for particularly immoral cases. ▪ Transparent: duty to reveal the processing and inform the data subject about it.
Purpose limitation (Zweckbindung)	▪ Any processing of personal data requires a specific and explicitedly stated purpose. Documentation! ▪ Processing data for a different purpose is prohibited if not compatible with the original purpose. Exceptions: consent / research and archiving purposes.
Data minimisation	▪ Personal data has to be kept adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed.

Principles relating to processing of personal data

Art. 5 GDPR	
Accuracy	▪ Duty to erase / rectify data that is inaccurate.
Storage limitation	▪ Duty to erase once they are no longer necessary for their purpose. ▪ Exceptions: archiving in the public interest or research purposes
Integrity and confidentiality	▪ Duty to store personal data with adequate security measures. ▪ E.g.: encryption, pseudonymization, server access control, …
Accountability of the controller	▪ Controller must be able to prove compliance with these data protection duties. Documentation!

5. Bureaucracy – forms and documents


Records of processing activities
Data protection impact assessment
Consent form
Privacy policy

Records of processing activities
Verzeichnis der Verarbeitungstätigkeiten

- Description of a data processing activity (i.a.: controller and contact data; purpose ; type of personal data ; groups of persons with access to that data ; legal basis ; technical data protection)
- One per data processing activity (e.g. one per research project / group of similar projects)
- Continual maintenance

Standard form	University of Konstanz	https://www.uni-konstanz.de/datenschutz/verarbeitungsverzeichnis/formular/

Consent form – Einwilligungserklärung

Standard form Research project	ZENDAS	https://www.zendas.de/themen/datenschutz-grundverordnung/einwilligung_forschungsprojekt.html
Standard form Foto, film, audio	Universität Konstanz	https://www.uni-konstanz.de/universitaet/aktuelles-und-medien/online-und-print-medien-gestalten/foto-und-urheberrecht/

Privacy policy – Datenschutzerklärung

- Duty to inform the data subject if personal data is collected (Art. 13 / 14 GDPR).

Standard form Research project	ZENDAS	https://www.zendas.de/themen/datenschutz-grundverordnung/einwilligung_forschungsprojekt.html
Standard form Foto, film, audio	Universität Konstanz	https://www.uni-konstanz.de/universitaet/aktuelles-und-medien/online-und-print-medien-gestalten/foto-und-urheberrecht/

Data protection impact assessment
Datenschutzfolgenabschätzung

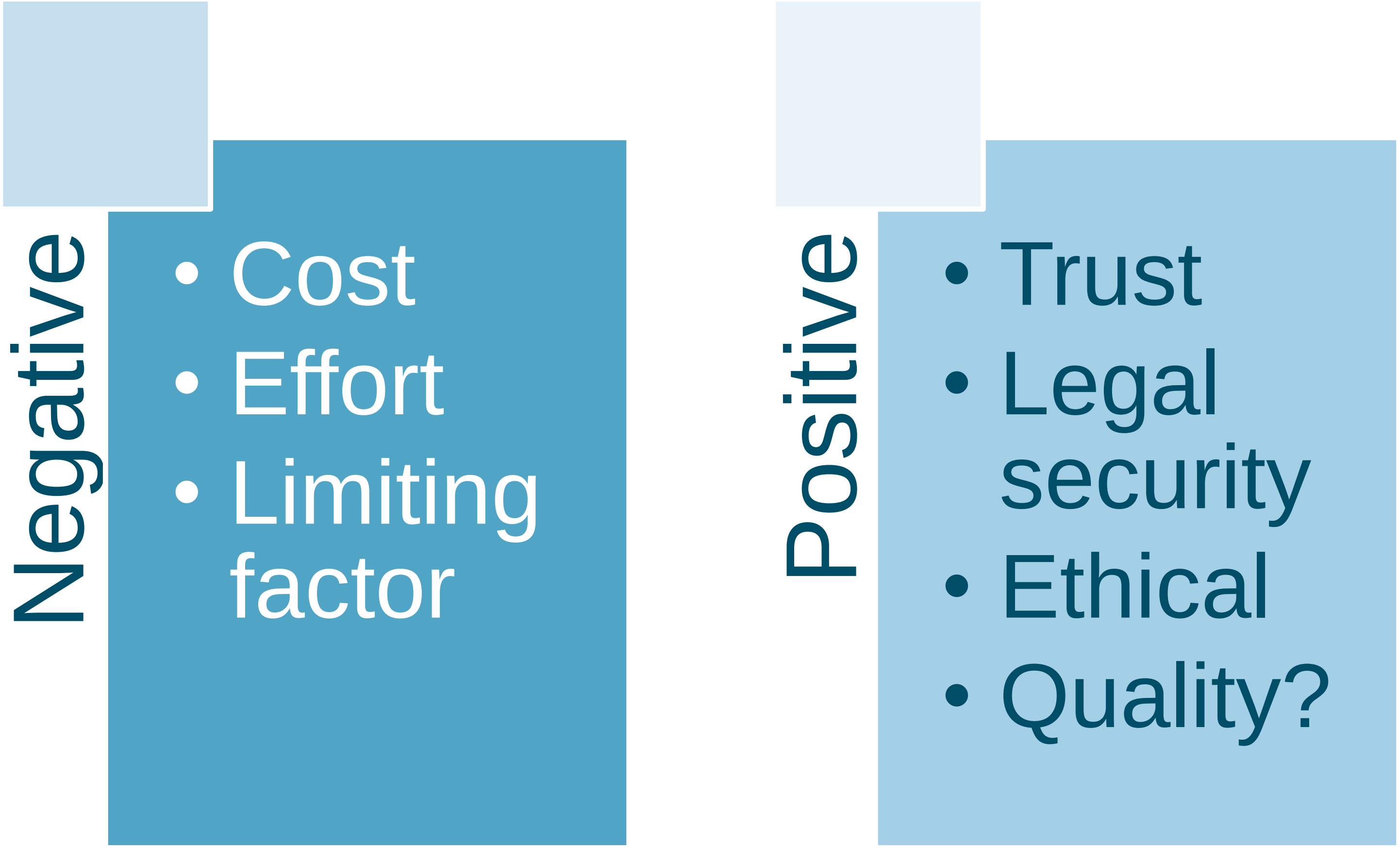
- **Objective**: additional security measure for high risk processing of personal data
- Only **required if** the processing is likely to result in a high risk for the rights ad freedoms of the data subjects**.**
- **Examples:**
  - Profiling
  - Large scale processing special categories of personal data (Art. 9 GDPR)
  - Large scale monitoring of public areas
- DPIA consists of a thorough description and evaluation of the planned data processing in order to reduce the risks by the implementation of additional security measures.

6. An effort worth while?

1. What is your experience? Is data protection just another administrative task that pulls you away from real research?

2. Has this workshop changed your position?

Positive vs. negative effects



Negative

- Cost
- Effort
- Limiting factor

Positive

- Trust
- Legal security
- Ethical
- Quality?

bw2FDM

Thank you!
Herzlichen Dank!

Peter Brettschneider
Fachreferent Rechtswissenschaften · Querschnittsaufgabe
Urheberrecht · bw2FDM

E-Mail: peter.brettschneider[at]uni-konstanz.de