# “What do they actually want from me?”

## On the dialogue with Data Protection Officers...

... for employees in administration and on the academic side in year 7+ after the entry into force of the GDPR.

Presentation slides with a table of contents and a glossary for reference for all who were overwhelmed or absent during the talk.

Feb 2025

# Contents

# What is data protection?

- **Data protection does not protect data, but individuals** from infringements of their constitutionally guaranteed personality rights by the erroneous or unlawful handling of their data.
- Consequently, among other things:
  1. The highest level of data protection is achieved by avoiding the processing of personal data wherever possible.
  2. Where the data to be processed have no link to an identifiable person (perhaps because the link has been deliberately avoided), no data-protection measures are required.
- **Scope of the presentation:** In the following we will
  - briefly outline the fundamentals of data protection,
  - discuss a subjectively selected set of details derived from those fundamentals, and finally
  - internalise a few practical tips.

But first...

# ... why do Data Protection Officers even exist?

- The role and duties are set out in Article 37–39 GDPR and the respective (German Federal) State Data Protection Act (e.g. §§ 5–7 HDSIG); in particular DPOs are to promote compliance with the GDPR.
- All individuals whose data are processed by a university may contact the DPO at any time (or directly the supervisory authority, i.e. the State Data Protection Authority). DPOs are also regularly the point of contact for exercising data subject rights.
- DPOs are bound by confidentiality in data-protection matters.
- University management (the "controller" within the meaning of Article 4 GDPR for processing carried out by the university) are informed and advised directly by the DPOs.

# DP basics: What is personal data?

When the term "data" is used below, it always refers to **personal data** (herein after referred to as "**PD**").

- "PD are any information relating to an identified or identifiable natural person. **Different pieces of information that together can identify a particular person are also PD**."
- "PD that have been encrypted or pseudonymised but can be used to re-identify a person remain PD and fall within the scope of the GDPR."
- "PD that have been anonymised in such a way that the data subject can not be identified anymore are no longer PD. For the data to be truly anonymised, the anonymisation must be irreversible."

(https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en)

# DP basics: Principles for processing

- A **processing** of PD covers virtually everything that can be done with those data (store, alter, transmit, etc.).
- Article 5 GDPR sets out the principles:
  - **Lawfulness**,
  - **Fairness and transparency**,
  - **Purpose limitation**,
  - **Data minimisation**,
  - **Accuracy**,
  - **Storage limitation**,
  - **Integrity and confidentiality**.
- Compliance with these principles is subject to a **accountability** obligation of the controller (Article 5(2) GDPR).

# DP basics: Lawfulness of processing 1/2

- Prohibition with the reservation of permission: Processing of PD is prohibited unless it is permitted.
- Permission may stem **either** from opening clauses in the GDPR together with other legal provisions (example: data processing for the performance of a task, Art. 6(1)(e) GDPR, Art. 6(3) GDPR in conjunction with federal state legislation governing universities)
- **or** from the data subject's consent (Art. 6(1)(a) GDPR).
- The processing of **special categories** of PD (such as racial or ethnic origin, health data, etc.) is subject to stricter rules in Art. 9 GDPR.

# DP basics: Lawfulness of processing 2/2

Small digression: "**Consent** as a legal basis" (often used in universities, especially in research):

- Regulated in Articles 7 and 8 GDPR; consent
  - must be given in a demonstrable and informed manner; the information about the processing must be written in clear language, and
  - must be given voluntarily (for example this is already questionable in an employment relationship), and
  - can be withdrawn at any time without giving a reason, with effect for the future.
- From the controller's point of view, consent can become a "poisoned" legal basis for processing. Example: a printed brochure has to be destroyed because a depicted person has withdrawn their consent.
- Even for special-category data (Article 9) processing is possible on the basis of **explicit consent** (Article 9(2)(a) GDPR).

# DP basics: Purpose limitation and data minimisation

- Article 5(1)(b) GDPR: "Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes [...] ("**purpose limitation**")."
  The definition of the purposes is made **by the controller** and must be established **before** the processing takes place.
  There are exceptions to purpose limitation, for example for research, but these are themselves subject to conditions.
- Article 5(1)(c) GDPR: "Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("**data minimisation**")."

# DP basics: Storage limitation

- From the principle of **storage limitation** (Article 5(1)(e) GDPR) and its concrete realisation in the right of erasure ("**right to be forgotten**", Article 17 GDPR) it follows that a **erasure** or (effective) **anonymisation** must take place when the PD are no longer necessary for the purpose for which they were collected **and** certain other circumstances **do not** apply (for example a statutory retention obligation).
- The storage-limitation principle is complemented by the purpose-limitation principle:
  Without a clearly defined purpose the moment at which data shall be erased after the purpose has been fulfilled could not be determined unambiguously.
  Purpose limitation also prevents the purpose from being changed retroactively (there are exceptions), which would otherwise weaken or even circumvent obligation to erase.

# DP basics: Accuracy, integrity and confidentiality

The controller must, by means of technical and organisational measures, ensure that

- the data to be processed are **factually accurate** and, where necessary, kept up to date,
- the data are **available** ("no backup, no mercy"), and
- only those persons who need the data to fulfil the processing purpose have access to them. Access should be governed by the "**need-to-know principle**": as extensive as necessary, but as limited as possible.

The GDPR does not explicitly prescribe a **duty of confidentiality**, but the requirement that processing be carried out only on the basis of instructions (Article 29 GDPR in conjunction with Article 32(4) GDPR) gives rise to a **data secrecy** obligation - i.e. a prohibition on unauthorised processing that implicitly includes a duty of confidentiality. The duty of data secrecy continues to apply after the termination of an employment relationship.

# DP basics: Transparency and data subject rights

The GDPR considerably expands the rights of data subjects (Articles 12–22). In particular it provides:

- a **duty to provide information** on the part of the controller when data are collected, both directly from the data subject and when data are obtained from other sources;
- a **right of access** for data subjects (with prescribed time limits for compliance);
- and rights to **rectification**, **erasure**, **restriction of processing**, **data portability** and **objection to processing**, each exercisable when certain conditions are met.

**Note:** The extension of data subject rights is (together with the provisions on administrative fines) one of the few truly significant changes introduced by the entry into force of the GDPR in 2018 (actually 2016) compared with the previous German legal framework. Most other GDPR provisions were already in place as such, or very similar, under federal and state legislation - they attracted little attention, though, because violations were either lightly punished or not enforced at all.

# DP basics: Criminal liability and administrative fines

- The university management is (externally) responsible for complying with data-protection law. The German legislature has (unfortunately?) excluded administrative fines against public bodies (but not liability; therefore **universities are not immune from compensation claims** - in cases of serious breaches or even where many data subjects are affected, damages can become costly).
- For you personally: if you process PD **negligently or intentionally** in an unlawful manner, this can be pursued as an administrative offence or, in the case of intent, as a criminal offence. Up to two years' imprisonment or a fine may be imposed on anyone who, for example, transmits university address lists to third parties for personal gain (see Section 37(1) HDSIG - other German states have comparable provisions).

# Details: RPA, DPA & Co. - Overview 1/3

- A **record of processing activities** (**RPA**) is required for virtually every processing and must contain a description of that processing in the scope prescribed by the GDPR. An RPA is a "living" document, i.e. it is updated whenever the processing changes.
- The controller's duty to provide information creates the need to produce a **privacy notice** for data subjects (in the case of processing based on consent, the privacy notice must be accompanied by a **consent statement**).

# Details: RPA, DPA & Co. - Overview 2/3

- If a processor (usually an external service provider) is to process data **on behalf of and under the instructions of the controller** (Article 28 GDPR), a **data-processing agreement** (**DPA**) must be concluded. Examples: hosting providers, SaaS vendors, etc.
  - In a data-processing agreement the responsibility for the PD remains with the data controller and does not pass to the data processor. This is the key difference to joint controllership (the next point).
- Where an external organisation **jointly decides with the controller on the means and purposes of the processing**, a contract for **joint controllership** is required (Article 26 GDPR). Example: a collaboration of several universities on a research project.
- DPAs and contracts for joint controllership are normally concluded (signed) by university management.

# Details: RPA, DPA & Co. - Overview 3/3

- The GDPR on **data-protection impact assessments (DPIA)**: *Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*
  - There is a "must-list" of processing activities that inevitably require a DPIA (normally viewable on the website of the relevant supervisory authority).
  - DPIAs can quickly become labour-intensive and complex - consult your DPO.

The "perfect storm": a high-risk processing project that is joint, with an external service provider and relies on consent as the legal basis $\rightarrow$ Bingo! All of the measures and documents mentioned above are required (the situation would be even more demanding if there were an additional transfer of data to a third country).

# Details: Technical and organisational measures ("TOM")

- Article 32 GDPR - "Security of processing".
- The TOM you (and a possible processor) implement to ensure the proper handling of the personal data under your responsibility must be suitable to achieve a **level of protection appropriate to the risk** (*). Among other things, the measures must cover:
  - Pseudonymisation and encryption;
  - Ensuring the ongoing confidentiality, integrity, availability and resilience of the systems and services involved in the processing;
  - The rapid restoration of the availability of the PD in the event of a physical or technical incident;
  - Procedures for the regular testing, assessment and evaluation of the effectiveness of the adopted TOM.

(*) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons whose data are processed.

# Details: Processing in third countries/“Cloud” 1/2

- When PD are transferred to a third country (any country outside the scope of the GDPR), a level of protection essentially equivalent to that provided by the GDPR must apply.
- Apart from some obscure exceptions, the controller can guarantee this only if either:
  - a **adequacy decision** exists for the destination country, or
  - a DPA is concluded that incorporates the so-called **Standard Contractual Clauses**.
- When using cloud services, you often have to comply not only with data-protection requirements but also with other contractual obligations (e.g. non-disclosure agreements, NDAs).

# Details: Processing in third countries/“Cloud” 2/2

Because the majority of cloud services involve the transfer of PD to the United States or under U.S. jurisdiction, the current legal situation for the “problem case” United States is as follows:

- For the present “Data Privacy Framework” (“DPF”) there is an adequacy decision by the European Commission.
- If a U.S. provider is “DPF-certified” **and** a DPA has been concluded, the transfer of PD is permissible.
- A DPF certification must be verified (by you!) in advance, e.g. via the participant-search portal: `https://www.dataprivacyframework.gov/s/participant-search`
- The DPF, like its predecessor (the “EU-U.S. Privacy Shield”), may be subject to litigation or termination in the near future. Therefore better avoid building heavy-weight, long-term dependencies on U.S. providers.

# Details: Personal data breaches

- Article 33 GDPR governs "Notifications of personal data breaches".
- A breach must be reported to the supervisory authority when personal data are
  - **leaked** (i.e. you no longer have control over them) **or** there is a reasonable indication that loss of control may have occurred, *or*
  - **data can not be accessed anymore** causing a detriment to the data subjects.
- The **notification deadline** is 72 hours after the breach becomes known to the controller - so don't hesitate, pick up the phone, call your DPO and "confess".
- Typical and frequent breach scenarios:
  - Laptop or USB-stick left on a bus, lost or stolen;
  - E-mail sent with hundreds of addresses in the "CC:" field;
  - Postal letters placed in the wrong envelope;
  - Programming or configuration errors that unintentionally grant access to unauthorised third parties;
  - Restoration after a database or file system crash fails or succeeds only with data loss;

# Practice: A Few Tips in No Particular Order... 1/3

*... based on the university data protection team's experience, drawn from perceived countless e-mails and phone calls:*

- When drafting an RPA, keep in mind that, in most cases, neither your DPO nor the supervisory authority will be familiar with the specific details of your processing. Therefore, (especially in the "purpose" section) write a few sentences that describe the "big picture" of your processing (but no novels!). Explain any abbreviations that are not widely known.
- In particular, when preparing an RPA it can be helpful to visualise your processing activity as a data flow: Where do the data come from (e.g. a survey or the campus-management system)? Where do they go (e.g. a transfer to another institution, or simply erasure or anonymisation)? What happens in between (e.g. processing by a processor)? What measures do you put in place to ensure, for example, the confidentiality and integrity of the data?

# Practice: A Few Tips in No Particular Order... 2/3

- Keep data-protection considerations in mind when you decide on a particular software or platform:
  - Processing on internal systems by your own staff ("on-premises") is preferable to engaging a processor within the scope of the GDPR. That, in turn, is preferable to using a processor located in a third country.
  - Open-source software does not "call home" (and if it does, the feature can be switched off).
  - Article 25 GDPR requires technical and organisational measures for data protection by design and by default. For example, the so-called "Hessian model" for Zoom (a video-conferencing platform) achieved, through default settings, that Zoom transmits only the minimal amount of PD to the provider, making it at least suitable for teaching purposes.
- Processors (at least those covered by the GDPR) will usually have a ready-made GDPR-compliant DPA that you can obtain on request and review (or, better still, have your DPO review).

# Practice: A Few Tips in No Particular Order... 3/3

- In the privacy information you provide to data subjects, do not use the term “anonymous” when you actually mean “pseudonymous” (anonymous data are not PD, whereas pseudonymised data are).
- If you rely on consent as a legal basis, state that the consent is given voluntarily, that no disadvantage will arise from not giving consent, and that consent can be withdrawn at any time without having to give a reason. A contact address for exercising this right must also be supplied.
- Technical and organisational measures (TOMs) are, in practice, the most challenging part of an RPA. Your life will be easier if, at least for central processing activities, you can refer to an existing data security concept or certification.
- Remember data-protection considerations when you write internal documentation or user guides for centrally used software or services. When in doubt, consult your DPO.

# Glossary

- DP/DPA - Data processor/Data Processing Agreement
- DPF - EU-US Data Privacy Framework
- DPIA - Data Protection Impact Assessment
- DPO - Data Protection Officer/Office
- GDPR - (EU) General Data Protection Regulation
- HDSIG - Hessian Data Protection and Freedom of Information Act (successor to the Hessian Data Protection Act, HDSG)
- Hoster - Hosting provider
- LDSG - (German federal) State Data Protection Act(s)
- NDA - Non-Disclosure Agreement
- PD - Personal data
- SaaS - Software-as-a-Service
- TOM - Technical and organisational measures
- RPA - Record of Processing Activities