Data Protection Guidelines of Bielefeld UAS

As of 1 October 2014 (Official Notice/Announcement Bulletin 2014-24, pp. 216–218), last revised 5 July 2018 (revision due to the EU General Data Protection Regulation (EU-GDPR))

Outline

Please note: The German version of this document is the legally binding version. The English translation provided here is for information purposes only.

1. Foundations

In fulfilling its duties, Bielefeld UAS processes a large number of personal data of its members, applicants, persons affected by research and cooperation partners as well as other groups of persons. Protecting these persons' informational self-determination realises their basic right "to the protection of personal data concerning him or her" pursuant to Art. 8 of the Charter of Fundamental Rights of the European Union. The EU General Data Protection Regulation, the state data protection act, and specific regulations on data protection at universities further specify compliance with data protection as a personal right.

As a public entity and place of free intellectual development, Bielefeld UAS is aware of the basic right of informational self-determination's importance and actively promotes its implementation. For the compliance with data protection regulations, Bielefeld UAS shall develop a data protection management system, which will ensure the lawful protection of personal data. University Governance supports these efforts on all levels and shall provide the necessary resources.

2. Objective

Compliance with data protection regulations must be ensured through demonstratable organisational, procedural and technological measures.

In accordance with Art. 5 (2) and Art. 24 (1) EU GDPR, the data controller must be able to demonstrate that data are processed in compliance with data protection regulations pursuant to Art. 5 (1) ('accountability') and provisions further specified in the EU GDPR and state legislation.

In order to reach the objective, it will be necessary to develop a data protection management system which, in particular, ensures the following substantive requirements in a detectable way:

a) **Ensuring lawful, fair and transparent data processing:**
    a. Data are only processed on a legal basis (regulations, consent).
    b. Priority lies in direct collection from the data subject.
    c. Transparent information on the nature and scope of processing, rights of the data subject, and right to lodge a complaint.
    d. Maintaining a record of processing activities to enable internal and external monitoring by supervisory authorities.
b) **Compliance with the requirements for purpose limitation** by only collecting data for specified, explicit and legitimate purposes and not processing them in a way that is considered to be incompatible with the initial purposes.
c) **Compliance with the principle of data minimisation** by only collecting and processing data that are necessary for their purposes.
d) **Ensuring accuracy of data** by taking steps to immediately erase or rectify personal data that are inaccurate with regard to the purposes for which they are processed.
e) **Storage limitation** by storing data 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, save for exemptions provided for by applicable law.
f) **Ensuring availability, integrity and confidentiality** by processing data in a manner that ensures appropriate security of the personal data, in particular protection from:
    a. Unauthorised or unlawful processing
    b. Accidental loss
    c. Accidental destruction or damage

    Interlinking with the existing information security management at Bielefeld UAS is to create a maximum of synergies, provided that there is no conflict between security measures and data protection.
g) **Realising the rights of the data subject** through structures and reporting channels that enable disclosures and further rights of the data subjects connected with them.
h) **Compliance with legal requirements in engaging third parties** in individual or joint data processing.
i) **Verifying the lawfulness of data transfers to places outside the EU.**
j) **Structurally and organisationally ensuring the obligations to notify supervisory authorities and data subjects of infringements against data protection in accordance with Art. 33 and 34 EU GDPR.** In particular, this comprises raising awareness and training employees so that incidents can be avoided, correctly recognised, correctly understood, and correctly notified.
k) **Carrying out data protection impact assessments (DPIA)** under the conditions of Art. 35 EU GDPR.

3. Responsibilities

- **University Governance (Executive Board):** University Governance bears overall responsibility for ensuring data protection. Through its decisions, it meets the organisation's needs and provides the necessary financial, personnel and time resources in order to guarantee data protection. University Governance ensures that university members are made aware of data protection and security of personal data by providing information and training.

It is responsible of introducing and developing the data protection management system (DPMS).

- **Data Protection Official:** The university has designated a Data Protection Official who monitors compliance with the legal requirements for data protection and awareness-raising and training of staff, and who provides advice as regards the realisation of data protection for University Governance and employees who process data where requested. The Data Protection Official advises the data protection coordinators, who are to be named by the controllers, in their task of implementing data protection requirements. The DPO is the point of contact for the data subjects and the competent supervisory authority. He or she is part of the steering group on data protection and IT/information security which is to be formed by University Governance.

- **IT/Information Security Official:** The Information Security Official advises University Governance on all questions regarding IT/information security. The Information Security Official advises University Governance on all questions regarding IT/information security. The Data Protection Official and the IT/Information Security Official will be in regular contact with each other, discuss security incidents with relevance to data protection and jointly develop solutions that adequately meet the requirements of IT/information security and data protection.
  He or she is part of the data protection and IT/information security steering group which is to be formed by University Governance.

- **Executives:** Notwithstanding the overall responsibility of University Governance, data protection is an integral part of one's professional task. Thus, all employees with an executive role bear responsibility for data protection in their respective field of activity on the basis of their professional responsibility. Bearing responsibility means knowing, designing and steering the processes within one's own organisational area. And it means recognising where processes and processing cannot be implemented in compliance with data protection regulations and notifying University Governance of this.
  Executives act as role models and are responsible of implementing, maintaining, and adapting measures within their area to new legal, technical and organisational conditions if necessary. For this, they have to realise the technical, organisational, and personnel requirements.
  Particular mention should be made here of raising awareness among employees through information and training.

- **Data Protection Coordinators:**
  In coordination with the areas of organisation and the Data Protection Official and IT/Information Security Official, University Governance names Data Protection Coordinators to support consciousness and awareness-raising. They are at the data controllers' and employees' disposal for advice and discuss implementational measures. They exchange views, build a joint knowledge base and develop ideas for consciousness-raising. The Data Protection Coordinators do not bear special data protection responsibility, but take an advisory and supporting role for executive staff in their tasks.

- **Employees:** Employees participate in the information and training offers that are made available and will process personal data that are accessible to them only within the scope of the tasks entrusted to them.

They will take care that only entitled persons have access to personal data handled by them. They are responsible within the usual scope of employee liability and shall immediately notify their supervisor or the Data Protection Official or IT/Information Security Official of any infringements or security breaches they encounter.

- **Data protection and IT/information security steering group**
  Within the scope of the development of a data protection management system (DPMS), University Governance will install a data protection and IT/information security steering group whose members will hold regular meetings to discuss and develop current issues regarding the university's data protection and IT/information security strategy and, in special cases, to make suggestions or solution proposals to University Governance.

  The IT/Information Security Official and the Data Protection Official will necessarily be part of the group.

4. Infringements

Non-compliance or deliberate infringement of these guidelines or the regulations derived from them is a breach of official duties, which can lead to consequences with regard to the employment, as well as criminal or civil penalties.

5. Effectiveness

These guidelines will become effective the day after their publication in the Announcement Bulletin/Official Notice of Bielefeld UAS (FH Bielefeld Verkündungsblatt/Amtliche Bekanntmachung).

On their effective date, these guidelines will replace the Data Protection Guidelines of Bielefeld UAS of 1 October 2014, Official Notice/Announcement Bulletin (FH Bielefeld Amtliche Bekanntmachung/Verkündungsblatt) 2014-24, pp. 216–218.

Bielefeld, 16 July 2018

signed I. Schramm-Wölk

Prof. Dr. I. Schramm-Wölk

President of Bielefeld University of Applied Sciences