

# Datenschutz-Leitlinie FH Bielefeld

vom 01.10.2014 (Amtliche Bekanntmachung/Verkündungsblatt 2014-24, S. 216-218) in der Fassung vom 05.07.2018 (Überarbeitung vor dem Hintergrund der EU-Datenschutzgrundverordnung (EU-DSGVO))

## Gliederung

1. Basis.....	145
2. Zielsetzung.....	145
3. Verantwortlichkeiten.....	146
4. Verstöße .....	148
5. Inkrafttreten.....	148

## 1. Basis

Die FH Bielefeld verarbeitet bei der Erfüllung ihrer Aufgaben eine Vielzahl personenbezogener Daten von ihren Mitgliedern, Angehörigen, Bewerbern, von Forschung betroffenen Personen und von Kooperationspartnern sowie von weiteren Personengruppen. Der Schutz der informationellen Selbstbestimmung dieser Personen verwirklicht deren Grundrecht „auf Schutz der sie betreffenden personenbezogenen Daten“ gemäß Art. 8 der EU-Grundrechte-Charta. Die Einhaltung dieses als Datenschutz bezeichneten Persönlichkeitsrechts wird durch die EU-Datenschutzgrundverordnung, das Landesdatenschutzgesetz und bereichsspezifische Regelungen zum Datenschutz an Hochschulen weiter konkretisiert.

Die FH Bielefeld als öffentliche Stelle und Stätte der freien geistigen Entfaltung, ist sich der Bedeutung des Grundrechts auf informationelle Selbstbestimmung bewusst und setzt sich aktiv für dessen Verwirklichung ein. Zur Einhaltung des Datenschutzes baut die FH Bielefeld ein Datenschutzmanagementsystem auf, mit dem der gesetzeskonforme Schutz personenbezogener Daten gewährleistet wird. Die Hochschulleitung unterstützt diese Anstrengungen auf allen Ebenen und stellt die erforderlichen Ressourcen zur Verfügung.

## 2. Zielsetzung

Die Einhaltung des Datenschutzes muss durch organisatorische, prozessuale und technische Maßnahmen nachweisbar sichergestellt werden.

Art. 5 Abs. 2 und Art. 24 Abs. 1 EU-Datenschutzgrundverordnung (EU DS-GVO) beinhalten eine Rechenschaftspflicht, nach der die datenverarbeitende Stelle nachweisen können muss, dass die Verarbeitung von personenbezogenen Daten unter Einhaltung der Datenschutzbestimmungen aus Art. 5 Abs. 1 der EU DS-GVO und den weiteren konkretisierenden Vorgaben aus der EU DS-GVO und dem Landesrecht erfolgt.

Zur Erreichung des Ziels ist der Aufbau eines Datenschutzmanagements erforderlich, das insbesondere die folgenden materiellen Anforderungen nachweisbar sicherstellen soll:

- a) **Gewährleistung einer rechtmäßigen, fairen und transparenten Verarbeitung:**
  - a. Eine Verarbeitung erfolgt nur mit Rechtsgrundlage (Gesetz, Einwilligung).
  - b. Vorrang der Direkterhebung bei der betroffenen Person.
  - c. Transparente Informationen über Art und Umfang der Verarbeitung, Betroffenen- und Beschwerderechte.
  - d. Führung eines Verzeichnisses von Verarbeitungstätigkeiten zur Ermöglichung von internen und externen Kontrollen durch die Aufsichtsbehörde.
- b) **Einhaltung der Anforderungen zur Zweckbindung**, indem Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
- c) **Einhaltung des Grundsatzes der Datenminimierung**, indem nur die für die Aufgabenerfüllung erforderlichen Daten erhoben und verarbeitet werden.
- d) **Gewährleistung der sachlichen Richtigkeit der Daten**, indem Maßnahmen getroffen werden, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.
- e) **Speicherbegrenzung**, indem Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person mit den gebotenen gesetzlichen Ausnahmen nur so lange ermöglicht wie es für den Zweck der Verarbeitung erforderlich ist.
- f) **Gewährleistung von Verfügbarkeit, Integrität und Vertraulichkeit**, indem die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, insbesondere den Schutz vor:
  - a. Unbefugter oder unrechtmäßiger Verarbeitung
  - b. Unbeabsichtigtem Verlust
  - c. Unbeabsichtigter Zerstörung oder Schädigung

Hier soll die Verzahnung mit dem bestehenden Informationssicherheitsmanagement an der Hochschule zu größtmöglichen Synergien führen, soweit kein Konflikt zwischen Sicherheitsmaßnahmen und Datenschutz besteht.
- g) **Verwirklichung der Betroffenenrechte**, durch Strukturen und Meldewege, die Auskünfte und daran anknüpfende weitere Betroffenenrechte ermöglichen.
- h) **Einhaltung der gesetzlichen Anforderungen bei der Einbindung von Dritten** in die eigene oder gemeinsame Datenverarbeitung.
- i) **Prüfung der Rechtmäßigkeit vor Datentransfers an Stellen außerhalb der EU.**
- j) **Strukturelle und organisatorische Sicherstellung der Meldepflichten aus Art. 33 und 34 EU DS-GVO bei Datenschutzverstößen gegenüber Aufsichtsbehörde und betroffenen Personen.** Hierzu gehört insbesondere die Sensibilisierung und Schulung der Mitarbeiter damit Vorfälle vermieden, richtig erkannt, richtig eingeordnet und richtig gemeldet werden.
- k) **Durchführung von Datenschutz-Folgeabschätzungen (DSFA)** bei Vorliegen der Voraussetzungen aus Art. 35 EU-DSGVO

### 3. Verantwortlichkeiten

- **Hochschulleitung (Präsidium):** Die Hochschulleitung trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Sie trägt durch ihre Entscheidungen dem Organisationsziel Rechnung und stellt die erforderlichen finanziellen, personellen und zeitlichen Ressourcen für die Umsetzung des Datenschutzes zur Verfügung. Die Hochschulleitung trägt dafür Sorge, dass Mitglieder und Angehörige der Hochschule durch Informationsangebote oder

Schulungen für den Datenschutz und die Sicherheit personenbezogener Daten sensibilisiert werden.

Sie ist verantwortlich für die Einführung und Weiterentwicklung des Datenschutzmanagementsystems (DSMS).

- **Behördliche Datenschutzbeauftragte/Datenschutzbeauftragter:** Die Hochschule hat eine behördliche Datenschutzbeauftragte bestellt. Diese überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz sowie die Mitarbeitersensibilisierung durch Schulungen und berät die Hochschulleitung und Beschäftigte, die Verarbeitungen durchführen, auf Anfrage zur Umsetzung des Datenschutzes. Die behördliche Datenschutzbeauftragte berät die von den Verantwortlichen zu benennenden „Datenschutzkoordinatorinnen und -koordinatoren“ bei deren Aufgabe zur Umsetzung der Datenschutzerfordernisse. Sie ist Ansprechpartnerin für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde. Sie gehört dem von der Hochschulleitung zu bildenden Lenkungskreis Datenschutz und IT-/Informationssicherheit an.
- **IT-/Informationssicherheitsbeauftragter:** Der Informationssicherheitsbeauftragte berät die Hochschulleitung bei allen Fragen zur IT-/Informationssicherheit. Der Informationssicherheitsbeauftragte berät die Hochschulleitung bei allen Fragen zur IT-/Informationssicherheit. Datenschutzbeauftragte und IT-/Informationssicherheitsbeauftragter stehen in regelmäßigem Kontakt, tauschen sich bei datenschutzrelevanten Sicherheitsvorfällen aus und erarbeiten gemeinsam Lösungen, die den Anforderungen von IT-/Informationssicherheit und Datenschutz angemessen Rechnung tragen. Er gehört dem von der Hochschulleitung zu bildenden Lenkungskreis Datenschutz und IT-/Informationssicherheit an.
- **Führungskräfte:** Ungeachtet der Gesamtverantwortung der Hochschulleitung ist der Datenschutz ein integraler Bestandteil der jeweiligen Fachaufgabe. Somit trägt jede Führungskraft, ausgehend von der fachlichen Verantwortung, die Verantwortung für den Datenschutz in ihrem Geschäftsbereich. Verantwortung tragen bedeutet, die Prozesse im eigenen Organisationsbereich zu kennen, zu gestalten und zu steuern. Und es bedeutet zu erkennen, wenn Prozesse und Verarbeitungen nicht datenschutzgerecht umgesetzt werden können und dies der Hochschulleitung mitzuteilen.  
Führungskräfte übernehmen eine Vorbildfunktion und sind dafür verantwortlich, Maßnahmen in ihrem Bereich umzusetzen, aufrecht zu erhalten und bei Bedarf an neue rechtliche, technische und organisatorische Gegebenheiten anzupassen. Hierfür sind die technischen, organisatorischen und personellen Voraussetzungen zu realisieren. Hervorzuheben ist hierbei die Sensibilisierung der Bediensteten durch Informationen und Schulungen.
- **„Datenschutz-Koordinatoren“**  
Die Hochschulleitung benennt in Abstimmung mit den Organisationsbereichen sowie der Datenschutzbeauftragten und dem IT-/Informationssicherheitsbeauftragten „Datenschutz-Koordinatorinnen und –Koordinatoren“ zur Unterstützung bei der Bewusstseinsbildung und Sensibilisierung. Sie stehen den Verantwortlichen und Beschäftigten zur Verfügung, geben Hinweise und diskutieren Umsetzungsmöglichkeiten. Sie tauschen sich untereinander aus, bauen eine gemeinsame Wissensbasis auf und entwickeln Ideen für die Bewusstseinsbildung. Sie tragen keine besondere Datenschutzverantwortung, sondern beraten und unterstützen die verantwortlichen Führungskräfte bei deren Aufgaben.

- **Bedienstete:** Die Bediensteten nehmen die angebotenen Informations- und Schulungsangebote wahr und verarbeiten die ihnen zugänglichen personenbezogenen Daten nur im Rahmen der ihnen übertragenen Aufgaben. Sie achten darauf, dass nur Berechtigte auf die von ihnen verwalteten personenbezogenen Daten Zugriff haben. Sie sind verantwortlich im Rahmen der üblichen Grenzen der Mitarbeiterhaftung und haben Regelverletzungen oder Sicherheitslücken unverzüglich dem oder der Vorgesetzten oder der behördlichen Datenschutzbeauftragten oder dem IT-/Informationssicherheitsbeauftragten mitzuteilen.
- **Lenkungskreis Datenschutz und IT-/Informationssicherheit**  
Im Rahmen des Aufbaus eines Datenschutzmanagementsystems (DSMS) installiert die Hochschulleitung einen Lenkungskreis Datenschutz und IT-/Informationssicherheit, dessen Mitglieder in regelmäßigen Treffen aktuelle Fragen zur Datenschutz- und IT-/Informationssicherheitsstrategie der Hochschule besprechen, weiterentwickeln und in besonderen Fällen der Hochschulleitung Lösungsvorschläge/Empfehlungen vorlegen. Unbedingt gehören der IT-/Informationssicherheitsbeauftragte und die Datenschutzbeauftragte dem Kreis an.

#### 4. Verstöße

Die Nichteinhaltung oder bewusste Verletzung dieser Leitlinie oder der daraus abgeleiteten ausdrücklichen Regelungen ist eine Verletzung der Dienstpflichten, die dienst- arbeits-, straf- und zivilrechtliche Folgen nach sich ziehen können.

#### 5. Inkrafttreten

Diese Leitlinie tritt am Tag nach ihrer Veröffentlichung im Verkündungsblatt/Amtliche Bekanntmachung der FH Bielefeld in Kraft.

Zum Zeitpunkt ihres Inkrafttretens ersetzt sie die Leitlinie Datenschutz der FH Bielefeld in der Fassung vom 01.10.2014, Amtliche Bekanntmachung/Verkündungsblatt 2014-24, S. 216-218.

Bielefeld, den 16.07.2018

gez. I. Schramm-Wölk

Prof. Dr. I. Schramm-Wölk

Präsidentin der Fachhochschule Bielefeld