UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

AMTLICHE MITTEILUNGEN

VERKÜNDUNGSBLATT DER UNIVERSITÄT PADERBORN AM.UNI.PB

AUSGABE 07.19 VOM 12. MÄRZ 2019

DATENSCHUTZLEITLINIE DER UNIVERSITÄT PADERBORN

VOM 12. MÄRZ 2019

HERAUSGEBER: PRÄSIDIUM DER UNIVERSITÄT PADERBORN

Datenschutzleitlinie der Universität Paderborn

vom 12. März 2019

Aufgrund des § 2 Absatz 4 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG) vom 16. September 2014 (GV. NRW. S. 547), zuletzt geändert durch Art. 3 des Gesetzes vom 17. Oktober 2017 (GV. NRW. S. 806), hat die Universität Paderborn folgende Leitlinie erlassen:

Präambel

Zweck und Ziel des Datenschutzes ist die Sicherung des Grundrechts auf informationelle Selbstbestimmung durch den Schutz personenbezogener Daten. Mit dieser Leitlinie legt das Präsidium für alle Hochschulangehörigen und im Auftrag der Hochschule agierenden Personen den Rahmen für den Umgang mit personenbezogenen Daten, die Einhaltung des Datenschutzes und den sicheren Betrieb der informationstechnischen Infrastrukturen an der Universität Paderborn fest.

Was bedeutet Datenschutz für uns als Universität?

Wir dürfen grundsätzlich keine personenbezogenen Daten verarbeiten. Es sei denn: es gibt einen ausdrücklichen Erlaubnistatbestand, beispielsweise eine Rechtsgrundlage, die erforderlichenfalls mit einer Ordnung, Richtlinie oder Dienstvereinbarung der Universität konkretisiert wird oder es liegt eine informierte Einwilligung jedes und jeder Betroffenen vor.

Datenschutz ist im Verständnis der Universität eine wesentliche Voraussetzung für ein Gelingen der Digitalisierung. Die Entwicklung datenschutzkonformer IT-Lösungen und Verarbeitungen wird in der Universität aktiv gefördert und unterstützt.

Verantwortung zu übernehmen bedeutet für uns: Wir wissen, was wir tun! Wir durchdenken Prozesse und gestalten diese. Wenn etwas nicht verantwortbar ist, ist genau dies zu erkennen, zu kommunizieren und zu beheben.

Wir arbeiten vorausschauend. Ungewollte Offenlegung personenbezogener Daten, Fehler beim Transfer von Daten und ähnliches sowie daraus resultierende Verletzungen des Grundrechts auf informationelle Selbstbestimmung der Betroffenen sowie mögliche Schadensersatzansprüche, Zivilrechtsklageverfahren und arbeitsrechtliche Sanktionen gilt es immer und jederzeit von vornherein zu vermeiden.

Jeder Datenschutzverstoß ist einer zu viel! Sollte trotz aller proaktiven Maßnahmen eine Verletzung des Datenschutzes auftreten, haben wir geregelte Prozesse für deren Feststellung und Bearbeitung, um den Schaden für die Betroffenen und die Universität zu minimieren. Wir lernen aus unseren Fehlern und verbessern uns.

1. Grundlage

Die Universität Paderborn verarbeitet bei der Erfüllung ihrer Aufgaben eine Vielzahl personenbezogener Daten von ihren Mitgliedern, Angehörigen, Bewerberinnen und Bewerber, Kooperationspartnerinnen und 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 die Europäische Datenschutzgrundverordnung (DSGVO) in Verbindung mit dem Datenschutzgesetz Nordrhein-Westfalen (DSG NRW), bereichsspezifischen gesetzlichen Regelungen im Hochschulgesetz Nordrhein-Westfalen (HG NRW) sowie durch hochschulinterne Ordnungen weiter konkretisiert.

Auch in der Forschung werden personenbezogene Daten verarbeitet. Teilweise werden dabei sensible Daten einzelner Personen erhoben, deren Verarbeitung einen beträchtlichen Grundrechtseingriff darstellt. Die Wissenschafts- und Forschungsfreiheit ist gemäß Art. 5, Abs. 3 des Grundgesetzes ebenfalls als ein Grundrecht gewährleistet. Weil Grundrechte miteinander in Konflikt geraten können, haben die gesetzgebenden Parlamente Regelungen geschaffen, die sowohl das Grundrecht auf „Forschungsfreiheit“ als auch das Grundrecht auf „Datenschutz/Informationelle Selbstbestimmung“ gewährleisten. Dabei wird die Forschung bei der Verarbeitung personenbezogener Daten durchaus privilegiert, sie ist aber nicht grundsätzlich von datenschutzrechtlichen Pflichten befreit.

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 DSGVO beinhalten eine Rechenschaftspflicht, nach der die Universität Paderborn als datenverarbeitende Stelle nachweisen können muss, dass die Verarbeitung von personenbezogenen Daten unter Einhaltung der Datenschutzbestimmungen aus Art. 5 Abs. 1 der DSGVO und den weiteren konkretisierenden Vorgaben aus der DSGVO sowie dem Landes- und dem Bundesrecht erfolgt.

Zur Erreichung des Ziels wird ein Datenschutzmanagement etabliert, das insbesondere die folgenden materiellen Anforderungen nachweisbar sicherstellen soll:

a) Gewährleistung einer rechtmäßigen, fairen und transparenten Verarbeitung:
   a. Eine Verarbeitung personenbezogener Daten erfolgt nur mit Rechtsgrundlage (Gesetz, hochschulinterne Ordnungen, 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 Universität 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 (Auftragsverarbeitung).
i) Prüfung der Rechtmäßigkeit vor Datentransfers an Stellen außerhalb der EU.
j) Strukturelle und organisatorische Sicherstellung der Meldepflichten aus Art. 33 und 34 DSGVO 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 bei Vorliegen der Voraussetzungen aus Art. 35 DSGVO.

3. Umsetzung

Die Universität Paderborn als öffentliche Stelle und eine 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 Universität Paderborn ein Datenschutzmanagementsystem auf, mit dem der gesetzeskonforme Schutz personenbezogener Daten gewährleistet wird (siehe Abbildung). Grundlage des Datenschutzmanagementsystems ist diese Leitlinie. Darauf aufbauend wird ein Datenschutzkonzept entwickelt. Dieses beinhaltet eine Organisationsstruktur mit Verantwortlichkeiten, Prozessen und Aufgaben. Außerdem werden Handreichungen für die Mitarbeitenden (Vorlagen, Anleitungen, Musterverträge, Formulare, Muster für Schulungen, Checklisten etc.) entwickelt. Ein weiterer Bestandteil des Datenschutzkonzeptes ist die technische Unterstützung der Prozesse und der Dokumentation (Dokumentationssystem).

4. Verantwortlichkeiten

- **Präsidium:** Das Präsidium trägt die Gesamtverantwortung für die Einhaltung des Datenschutzes. Es ist verantwortlich für die Einführung und Weiterentwicklung eines Datenschutzmanagementsystems (DSMS). Es trägt durch seine Entscheidungen dem Organisationsziel Rechnung und stellt die erforderlichen finanziellen, personellen und zeitlichen Ressourcen für die Umsetzung des Datenschutzes zur Verfügung. Das Präsidium trägt dafür Sorge, dass Mitglieder und Angehörige der Universität durch Informationsangebote oder Schulungen für den Datenschutz und die Sicherheit personenbezogener Daten sensibilisiert werden.
- **Behördliche Datenschutzbeauftragte oder Datenschutzbeauftragter:** Die oder der bestellte Datenschutzbeauftragte überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz sowie die Mitarbeitersensibilisierung durch Schulungen und berät das Präsidium und auf Anfrage Mitarbeitende, die Verarbeitungen durchführen, zur Umsetzung des Datenschutzes. Die oder der behördliche Datenschutzbeauftragte berät die Datenschutzkoordinatorinnen und Datenschutzkoordinatoren bei deren Aufgabe zur Umsetzung der Datenschutzanforderungen. Sie oder er ist Ansprechpartnerin oder Ansprechpartner für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde.
- **Informationssicherheitsbeauftragte oder Informationssicherheitsbeauftragter:** Die oder der Informationssicherheitsbeauftragte berät das Präsidium bei allen Fragen zur IT-/Informationssicherheit. Sie oder er tauscht sich regelmäßig und darüber hinaus anlassbezogen mit der oder dem behördlichen Datenschutzbeauftragten zur Ordnungsmäßigkeit der Verarbeitungstätigkeiten, Maßnahmen der Informationssicherheit und zu datenschutzrelevanten

Sicherheitsvorfällen aus. Im Falle eines Konflikts einer Sicherheitsmaßnahme mit dem Datenschutz verpflichtet sich die oder der Informationssicherheitsbeauftragte an einer Lösung mitzuwirken, die beiden Aspekten angemessen Rechnung trägt.

- **Führungskräfte (Leiterinnen und Leiter der Fakultäten, Zentralen Einrichtungen und Dezernate sowie Professorinnen und Professoren,):** Ungeachtet der Gesamtverantwortung des Präsidiums 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 über die Leitungen der Fakultäten, Zentralen Einrichtungen bzw. Dezernate 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 und die Mitarbeitenden zu sensibilisieren und die Möglichkeit zur Teilnahme an Schulungsangeboten zu eröffnen. Hervorzuheben ist hierbei die Sensibilisierung der Bediensteten durch Informationen und Schulungen.
- **Datenschutz-Koordinatorinnen und Koordinatoren:** Das Präsidium beauftragt in Abstimmung mit den Fakultäten, Zentralen Einrichtungen und der Zentralverwaltung sowie der oder dem Datenschutzbeauftragten und der oder dem Informationssicherheitsbeauftragten „Datenschutz-Koordinatorinnen und -Koordinatoren“ zur Unterstützung bei der Bewusstseinsbildung und Sensibilisierung. Sie werden besonders geschult und stehen mit ihrem Wissen den verantwortlichen Führungskräften und Mitarbeitenden beratend und unterstützend zur Verfügung, tragen jedoch keine besondere Datenschutzverantwortung. Sie tauschen sich untereinander aus, bauen die gemeinsame Wissensbasis aus und entwickeln Ideen für die Bewusstseinsbildung.
- **Mitarbeitende:** Die Mitarbeitenden, insbesondere diejenigen, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben oder Systeme zur Verarbeitung solcher Daten betreuen, 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 Mitarbeitendenhaftung. Sie haben Regelverletzungen oder Sicherheitslücken unverzüglich dem oder der Vorgesetzten und/oder der oder dem behördlichen Datenschutzbeauftragten und/oder der oder dem IT-/Informationssicherheits-beauftragten mitzuteilen.
- **Lenkungskreis Datenschutz und IT-/Informationssicherheit:** Im Rahmen des Aufbaus eines Datenschutzmanagementsystems (DSMS) installiert das Präsidium einen Lenkungskreis Datenschutz und IT-/Informationssicherheit, dessen Mitglieder in regelmäßigen Treffen aktuelle Fragen zur Datenschutz- und IT-/Informationssicherheitsstrategie der Universität besprechen, weiterentwickeln und in besonderen Fällen dem Präsidium Empfehlungen vorlegen. Unbedingt gehören die oder der IT-/Informationssicherheitsbeauftragte und die oder der Datenschutzbeauftragte dem Kreis an.

- **Vorfallteam**: Zur Beurteilung von Informationssicherheitsvorfällen, das sind sämtliche Angriffe auf die IT-Systeme oder Verdachte auf die Offenlegung von und den unerlaubten Umgang mit sensiblen und/oder personenbezogenen Daten wird ein Vorfallteam gebildet. Es besteht aus dem Datenschutzbeauftragten, der/dem Informationssicherheitsbeauftragte/n, der CIO und dem Ständigen Vertreter der Vizepräsidentin für Wirtschafts- und Personalverwaltung. Dort wird der jeder Vorfall – auch bzgl. der Meldung an die Landesbeauftragte oder den Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes NRW – geprüft und bewertet und dem Präsidium werden daraus abgeleitete Empfehlungen gegeben.

5. Verstöße

Die Nichtbeachtung datenschutzrechtlicher Bestimmungen kann für die Universität rechtliche Folgen nach sich ziehen und unter Umständen auch zu Regressansprüchen gegen die Verursacher führen.

6. Inkrafttreten

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

Ausgefertigt aufgrund des Beschlusses des Präsidiums der Universität Paderborn vom 27. Februar 2019.

Paderborn, den 12. März 2019

Die Präsidentin
der Universität Paderborn

Professorin Dr. Birgitt Riegraf

HERAUSGEBER
PRÄSIDIUM DER UNIVERSITÄT PADERBORN
WARBURGER STR. 100
33098 PADERBORN

HTTP://WWW.UNI-PADERBORN.DE

ISSN 2199-2819