 

  

Muster Datenschutzleitlinie

Version 1.0, 22 September 2017

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz CC BY-SA 3.0
<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>
Autor: NRW Projektgruppe „Umsetzung der EU-Datenschutz-Grundverordnung (EU-DSGVO) −
Datenschutzmanagementsysteme“ 2018

gefördert vom 

Muster: Datenschutzleitlinie

# Grundlage

Die Hochschule verarbeitet eine Vielzahl von personenbezogenen Daten von ihren Mitgliedern, Angehörigen, Bewerbern, von Forschung betroffenen Personen und externen Dienstleistern und Lieferanten, um ihre Aufgaben nach dem Hochschulgesetz zu erfüllen. Der Schutz der informationellen Selbstbestimmung von betroffenen Einzelpersonen verwirklicht deren Grundrecht aus Art. 8 der EU-Grundrechte-Charta, das durch die EU-Datenschutzgrundverordnung, das Landesdatenschutzgesetz und die bereichsspezifischen Regelungen zum Datenschutz an Hochschulen weiter konkretisiert wird. Die Hochschule als öffentliche Stelle und Stätte der freien geistigen Entfaltung, ist sich der Bedeutung des Grundrechts auf informationelle Selbstbestimmung bewusst und setzt sich aktiv für die Verwirklichung des Grundrechtsschutzes nach Maßgabe der geltenden Gesetze ein. Zur Erfüllung dieser Anforderungen baut die Hochschule ein Datenschutz-Management-System 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.

# Zielsetzung

Die Verwirklichung des Grundrechts auf informationelle Selbstbestimmung und die Erfüllung der hierfür erlassenen Rechtsnormen muss durch organisatorische, prozessuale und technische Maßnahmen nachweisbar sichergestellt werden.

Art. 5 Abs. 2 und Art. 24 Abs. 1 EU-DSGVO 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-Datenschutzgrundverordnung (EU-DSGVO) und den weiteren konkretisierenden Vorgaben aus der EU-DSGVO und dem Landesrecht erfolgt.

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

1. Gewährleistung einer rechtmäßigen, fairen und transparenten Verarbeitung:
	1. Eine Verarbeitung erfolgt nur mit Rechtsgrundlage (Gesetz, Einwilligung).
	2. Vorrang der Direkterhebung bei der betroffenen Person.
	3. Transparente Informationen über Art und Umfang der Verarbeitung, Betroffenen- und Beschwerderechte.
	4. Führung eines Verzeichnisses von Verarbeitungstätigkeiten zur Ermöglichung von internen und externen Kontrollen durch die Aufsichtsbehörde.
2. 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.
3. Einhaltung des Grundsatzes der Datenminimierung, indem nur die für die Aufgabenerfüllung erforderlichen Daten erhoben und verarbeitet werden.
4. 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.
5. 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.
6. Gewährleistung von Verfügbarkeit, Integrität und Vertraulichkeit, indem die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, insbesondere den Schutz vor:
	1. Unbefugter oder unrechtmäßiger Verarbeitung
	2. Unbeabsichtigtem Verlust
	3. Unbeabsichtigter Zerstörung oder Schädigung

Hier soll die Verzahnung mit dem bestehenden Informationssicherheits-Management an der Hochschule zu größtmöglichen Synergien führen, soweit kein Konflikt zwischen Sicherheitsmaßnahmen und Datenschutz besteht.

1. Verwirklichung der Betroffenenrechte, durch Strukturen und Meldewege, die Auskünfte und daran anknüpfende weitere Betroffenenrechte ermöglichen.
2. Einhaltung der gesetzlichen Anforderungen bei der Einbindung von Dritten in die eigene oder gemeinsame Datenverarbeitung.
3. Prüfung der Rechtmäßigkeit vor Datentransfers an Stellen außerhalb der EU.
4. Strukturelle und organisatorische Sicherstellung der Meldepflichten aus Art. 33 und 34 EU-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.
5. Durchführung von Datenschutz-Folgeabschätzungen bei Vorliegen der Voraussetzungen aus Art. 35 EU-DSGVO

# Verantwortlichkeiten

* **Hochschulleitung (Präsidium, Rektorat, Kanzler):** 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.
* **Behördliche(r) Datenschutzbeauftragte(r):** Die Hochschule hat eine(n) behördliche(n) Datenschutzbeauftragte(n) bestellt. Diese(r) überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz und berät die Hochschulleitung auf Anfrage zur Umsetzung des Datenschutzes. Er/Sie ist Ansprechpartner für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde.
* **IT-/Informationssicherheitsbeauftragte(r):** Der/Die Informationssicherheitsbeauftragte berät die Hochschulleitung bei allen Fragen zur IT-/Informationssicherheit. Er/Sie tauscht sich regelmäßig und darüber hinaus anlassbezogen mit dem/der behördlichen Datenschutzbeauftragten zu Maßnahmen der Informationssicherheit und zu datenschutzrelevanten Sicherheitsvorfällen aus. Im Falle eines Konflikts einer Sicherheitsmaßnahme mit dem Datenschutz verpflichtet sich der/die Informationssicherheitsbeauftragte an einer Lösung mitzuwirken, die beiden Aspekten angemessen Rechnung trägt.
* **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. 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.
* **Bedienstete:** Die Bediensteten nehmen die angebotenen Informations- und Schulungsangebote wahr und nutzen 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 haben Regelverletzungen oder Sicherheitslücken unverzüglich dem/der Vorgesetzten und/oder dem/der behördlichen Datenschutzbeauftragten und/oder dem/der IT-/Informationssicherheitsbeauftragten mitzuteilen.

# 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.

# Inkrafttreten

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