Amtliche Bekanntmachung
der Fachhochschule Südwestfalen

- Verkündungsblatt
der Fachhochschule Südwestfalen -

Baarstraße 6, 58636 Iserlohn

Nr. 861 Ausgabe und Tag der Veröffentlichung: 08.08.2018

Datenschutzrichtlinie
der
Fachhochschule Südwestfalen

Stand: 02.08.2018

Der Wortlaut wird im Folgenden bekannt gegeben:

Datenschutzrichtlinie der Fachhochschule Südwestfalen

1. Grundlage

Die Fachhochschule Südwestfalen verarbeitet eine Vielzahl von personenbezogenen Daten von ihren Mitgliedern, Angehörigen, Bewerberinnen und Bewerbern, externen Dienstleistern und Lieferanten sowie weiteren Personen, um ihre Aufgaben nach dem Hochschulgesetz zu erfüllen.

Personenbezogene Daten sind gemäß Art. 4 Satz 1 Nr. 1 der Datenschutz-Grundverordnung vom 27. April 2016 (DSGVO) alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Unter Verarbeitung versteht man gem. Art. 4 Satz 1 Nr. 2 DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Der Schutz der informationellen Selbstbestimmung von betroffenen Einzelpersonen verwirklicht deren Grundrecht aus Art. 8 der EU-Grundrechte-Charta, das durch die DSGVO, 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 Fachhochschule Südwestfalen 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.

2. 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 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 DSGVO und den weiteren konkretisierenden Vorgaben der DSGVO und des Landesrechts erfolgt.

Zur Erreichung des Ziels ist der Aufbau eines Datenschutz-Management-Systems 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 Information 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 Informationssicherheits-Management 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 DSGVO bei Datenschutzverstößen gegenüber Aufsichtsbehörde und betroffenen Personen. Hierzu gehört insbesondere die Sensibilisierung und Schulung der Beschäftigten, 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. Verantwortlichkeiten

- **Hochschulleitung (Rektorat):** 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:

  http://www4.fh-swf.de/de/home/beschaeftigte/organisation_1/beauftragteundvertretung/datenschutzbeauftragte/index.php

- Diese(r) überwacht die Einhaltung der gesetzlichen Vorgaben zum Datenschutz und berät die Hochschulleitung auf Anfrage zur Umsetzung des Datenschutzes. Sie/Er ist Ansprechpartner/in für betroffene Personen und für die zuständige Datenschutzaufsichtsbehörde.
- **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. Führungskraft im Sinne dieser Datenschutzrichtlinie bezeichnet jede Person, die in der Hochschule Führungsaufgaben, wie zum Beispiel die Planung, Organisation und Kontrolle von Aufgaben und/oder die Führung von Mitarbeitern, wahrnimmt. Dies sind insbesondere die Mitglieder des Rektorats, die Dekaninnen und Dekane, die Leiterinnen und Leiter der Zentralen Einrichtungen, die Hochschullehrerinnen und Hochschullehrer, die Dezernentinnen und Dezernenten sowie die Sachgebietsleiterinnen und -leiter. 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 Information und Schulung. Sie haben Regelverletzungen oder Sicherheitslücken unverzüglich der/dem behördlichen Datenschutzbeauftragten und der/dem IT-/Informationssicherheitsbeauftragten mitzuteilen.
- **Bedienstete:** Bedienstete im Sinne dieser Richtlinie sind die Beamtinnen und Beamten, die Arbeitnehmerinnen und Arbeitnehmer, die Lehrbeauftragten, die Dienstvertragsnehmerinnen und Dienstvertragsnehmer im Verbundstudium, die Auszubildenden sowie sonstige Personen, die im Auftrag oder auf Veranlassung der Hochschule personenbezogene Daten verarbeiten. 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 mitzuteilen.

4. Verarbeitung personenbezogener Daten im Kontext der Hochschule

Die Verarbeitung personenbezogener Daten erfolgt im Kontext der Hochschule insbesondere

- bezüglich Studieninteressierter und Studierender in den Systemen zur Studierenden- und Prüfungsverwaltung,
- bezüglich Bewerberinnen und Bewerbern sowie Beschäftigter in den Systemen zum Bewerbermanagement und zur Personalverwaltung,
- bezüglich Lehrender im Rahmen der Evaluation,
- bezüglich Lehrender und Lernender im Rahmen der Veranstaltungsplanung,
- bezüglich Lehrender und Lernender im Rahmen der Angebote des Blended Learning (E-Learning-Plattform, Kommunikationsplattform),
- bezüglich Beschäftigter im Rahmen der Tätigkeit der Personalräte,
- bezüglich Vertragspartnern und allen Personen, zu denen es Zahlungsflüsse gibt, in den Systemen zur Finanzverwaltung,
- bezüglich aller Hochschulmitglieder im Rahmen des Identity Management und der damit verbundenen Systeme, z.B. E-Mail-Verwaltung, Groupware, elektronische Chipkarte, Bibliotheksbenutzung,
- bezüglich Dritter im Rahmen von Befragungen und/oder in Forschungsprojekten,

- bezüglich Alumni, ehemaliger Beschäftigter sowie der interessierten Öffentlichkeit in Adressdatenbanken,
- bezüglich der Raumverantwortlichen in der Liegenschaftsverwaltung,
- bezüglich der Hochschulmitglieder und Gäste im Rahmen von Fotoaufnahmen sowie Videoüberwachung

sowie in allen weiteren Fällen, in denen personenbezogene Daten zu einem in der Erfüllung der Aufgaben der Hochschule liegenden Zweck auf der Grundlage einer gesetzlichen Ermächtigung oder einer Einwilligung in einem durch die jeweilige Aufgabe geforderten Umfang verarbeitet werden.

5. Verzeichnis von Verarbeitungstätigkeiten

Vor Einführung eines Datenverarbeitungsprozesses hat die oder der Verantwortliche gemäß Art. 30 DSGVO ein Verzeichnis der Verarbeitungstätigkeiten zu erstellen. Formulare hierzu sind hier hinterlegt:

http://www4.fh-swf.de/de/home/beschaeftigte/organisation_1/beauftragteundvertretung/datenschutzbeauftragte/index.php

Darin müssen Angaben zur/zum Verantwortlichen, zum Verarbeitungszweck, zu den Kategorien betroffener Personen und personenbezogener Daten, Empfängern, vorgesehenen Übermittlungen und eventueller Löschfristen gemacht werden sowie eine Beschreibung der technischen und organisatorischen Maßnahmen erfolgen.

6. Datenschutzfolgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt die oder der Verantwortliche gemäß Art. 35 DSGVO vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden. Die oder der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat der/s Datenschutzbeauftragten ein.

(2) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(3) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

7. Interne Meldewege / Erfüllung von Informationspflichten und Auskunftsverlangen

Fälle einer Verletzung des Schutzes personenbezogener Daten melden die Führungskräfte unverzüglich der/dem behördlichen Datenschutzbeauftragten. Diese/dieser sorgt dafür, dass die Verletzung möglichst innerhalb von 72 Stunden seit Bekanntwerden an die zuständige Aufsichtsbehörde gemeldet wird, es sei denn, diese Verletzung führte voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.

Die Erfüllung von Informationspflichten erfolgt über die jeweilige Führungskraft, ggf. nach Abstimmung mit der/dem behördlichen Datenschutzbeauftragten. Bei Auskunftsverlangen zur Verarbeitung personenbezogener Daten wenden sich die Führungskräfte an die Administrator(inn)en der DV-Anwendungen in ihrem Zuständigkeitsbereich und leiten die zusammengestellten Daten über die/den jeweiligen Fachvorgesetzten an die/den behördlichen Datenschutzbeauftragte/n weiter, die/der für die Erfüllung der Auskunftspflicht sorgt.

8. Verstöße

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

9. Inkrafttreten

Diese Richtlinie tritt am Tag nach ihrer Veröffentlichung in Kraft. Sie wird in der Amtlichen Bekanntmachung der Fachhochschule Südwestfalen – Verkündungsblatt der Fachhochschule Südwestfalen – veröffentlicht.

Iserlohn, den 2. August 2018

Der Rektor der Fachhochschule Südwestfalen in Iserlohn

Professor Dr. Claus Schuster