



Ausgabe 126 – 25. August 2021

Wormser Hochschulanzeiger

Publikationsorgan der Hochschule Worms

Inhaltsübersicht:

Seite 2

**Dienstanweisung zur Sicherstellung des Datenschutzes
an der Hochschule Worms vom 20.08.2021**

Seite 14

Impressum

Dienstanweisung zur Sicherstellung des Datenschutzes an der Hochschule Worms

1.	Grundlagen, Zielsetzung, Geltungsbereich.....	1
2.	Begriffsbestimmungen	2
3.	Organisation des Datenschutzes	2
4.	Verarbeitungsgrundsätze	3
5.	Datenschutzbeauftragte	3
6.	Datenschutz-Folgenabschätzung	3
7.	Verzeichnis der Verarbeitungstätigkeiten	4
8.	Webseiten und Social Media Auftritte der Hochschule Worms	5
9.	Datenübermittlung an Dritte	5
10.	Auftragsverarbeitung, insbesondere Einschaltung externer Dienstleister	5
11.	Datenschutz in Lehre und Forschung	6
12.	Nutzung von IT-Ressourcen.....	7
13.	Passwortvergabe	7
14.	Nutzung des E-Mail-Dienstes der Hochschule Worms.....	7
15.	Webbasierte Lehrveranstaltungen und Videokonferenzen („Online Meetings“)	8
16.	Verwendung dienstlicher Hardware durch Mitarbeiter/innen (Nr. 2.1.)	9
17.	Verpflichtung auf das Datengeheimnis (gem. § 8 LDSG RLP)	10
18.	Verfahren zur Wahrung der Betroffenenrechte.....	10
19.	Inkrafttreten	11

1. Grundlagen, Zielsetzung, Geltungsbereich

- 1.1 Die Hochschule Worms unterliegt als Körperschaft des öffentlichen Rechts des Landes Rheinland-Pfalz den Anforderungen
 - 1.1.1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (**Datenschutz-Grundverordnung, DS-GVO**),
 - 1.1.2 des Landesdatenschutzgesetzes Rheinland-Pfalz vom 08. Mai 2018 (**LDSG RLP**) und – partiell –
 - 1.1.3 des Bundesdatenschutzgesetzes vom 30. Juni 2017 (**BDSG**),
in der jeweils geltenden Fassung.
- 1.2 Als Anbieterin von Telemedien unterliegt die Hochschule Worms zudem den Anforderungen des Telemediengesetzes vom 26.02.2007 (**TMG**), sofern deren Vorschriften nicht durch solche der DS-GVO ersetzt sind.

- 1.3 Daneben bestehen Sonderregelungen für die Verarbeitung personenbezogener Daten in weiteren Rechtsnormen, etwa dem Hochschulgesetz des Landes Rheinland-Pfalz vom 23. September 2020 (**HochSchG RLP**), in der jeweils geltenden Fassung.
- 1.4 Nach Art. 32 Abs. 1 DS-GVO hat die Hochschule Worms innerhalb ihrer behördlichen Organisation unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Datenschutzniveau zu gewährleisten.
- 1.5 Diese Dienstanweisung dient allen Mitarbeiterinnen und Mitarbeitern (Ziff. 2.1) als verbindliche Grundlage für die rechtskonforme Verarbeitung personenbezogener Daten an der Hochschule Worms. Sie leistet in Umsetzung der Anforderungen des Art. 32 Abs. 1 DS-GVO einen Beitrag zum nachhaltigen Schutz der Grundrechte und Grundfreiheiten der Betroffenen.
- 1.6 Die Dienstanweisung in ihrer jeweils geltenden Fassung muss allen Mitarbeiterinnen und Mitarbeitern der Hochschule Worms jederzeit leicht zugänglich sein.
- 1.7 Informationen zu Rechtsvorschriften, auf die in dieser Dienstanweisung Bezug genommen wird, werden im Intranet der Hochschule unter „Dienstanweisung Datenschutz“ zum Abruf bereitgestellt.

2. Begriffsbestimmungen

- 2.1 „**Mitarbeiterinnen und Mitarbeiter**“ sind alle in einem Dienst- oder Anstellungsverhältnis, Arbeits-, Ausbildungs-, Praktikums- oder Volontariatsverhältnis stehenden Beschäftigten, Leiharbeiterinnen und Leiharbeiter sowie alle freien Mitarbeiterinnen und Mitarbeiter der Hochschule Worms. Mitumfasst sind unabhängig vom Status des Lehrauftrags auch alle Lehrkräfte der Hochschule Worms.
- 2.2 Der DS-GVO sind folgende weitere Begriffsbestimmungen zu entnehmen:
 - Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO)
 - Besondere Arten personenbezogener Daten (Art. 9 DS-GVO)
 - Verarbeitung (Art. 4 Nr. 2 DS-GVO)
 - Einschränkung der Verarbeitung (Art. 4 Nr. 3 DS-GVO)
 - Profiling (Art. 4 Nr. 4 DS-GVO)
 - Pseudonymisierung (Art. 4 Nr. 5 DS-GVO)
 - Verantwortlicher (Art. 4 Nr. 7 DS-GVO)
 - Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO)
 - Empfängerin oder Empfänger (Art. 4 Nr. 9 Satz 1 DS-GVO)
 - Dritter (Art. 4 Nr. 10 DS-GVO)
 - Einwilligung (Art. 4 Nr. 11 DS-GVO)

3. Organisation des Datenschutzes

- 3.1 Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO ist die Hochschule Worms, die nach § 79 Abs. 1 HochSchG vom Präsidium geleitet wird. Die Wahrnehmung der Aufgaben als Verantwortlicher im Sinne des Datenschutzrechts ergibt sich aus dessen nach § 79 Abs. 4 HochSchG erstellten Geschäftsverteilungsplan.
- 3.2 Die Verwaltung unterstützt den Verantwortlichen nach Absatz 1 bei der Durchführung und Sicherstellung des behördlichen Datenschutzes als Daueraufgabe für alle Bereiche der Hochschule Worms.
- 3.3 Das Präsidium benennt gemäß Art. 37 DS-GVO, § 37 LDSG RLP eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten (siehe Ziffer 5).

4. Verarbeitungsgrundsätze

- 4.1 Die Verarbeitung personenbezogener Daten durch die Hochschule Worms darf nur erfolgen, wenn eine gesetzliche Vorschrift die Verarbeitung erlaubt oder Betroffene in die Verarbeitung eingewilligt haben (sog. Verbot mit Erlaubnisvorbehalt).
- 4.2 Alle Mitarbeiterinnen und Mitarbeiter (Ziffer 2.1) der Hochschule Worms sind für die Einhaltung der Datenschutzbestimmungen verantwortlich. Sie sind diesbezüglich dem Präsidium, den im Datenschutz eingesetzten Personal sowie der Datenschutzbeauftragten oder dem Datenschutzbeauftragten der Hochschule Worms auf Aufforderung auskunftspflichtig.
- 4.3 Für die Verarbeitung von personenbezogenen Daten gelten die in der DS-GVO bestimmten Verarbeitungsgrundsätze:
 - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (Art. 5 Abs. 1 Buchst. a) DS-GVO)
 - Zweckbindung (Art. 5 Abs. 1 Buchst. b) DS-GVO)
 - Datenminimierung (Art. 5 Abs. 1 Buchst. c) DS-GVO)
 - Richtigkeit (Art. 5 Abs. 1 Buchst. d) DS-GVO)
 - Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e) DS-GVO)
 - Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f) DS-GVO)
 - Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO)
- 4.4 Ergänzende Vorschriften, insbesondere des Landesdatenschutzgesetzes und des Hochschulgesetzes, sind zu beachten.

5. Datenschutzbeauftragte

- 5.1 Gemäß Art. 37 DS-GVO, § 37 LDSG benennt das im Präsidium der Hochschule Worms verantwortliche Mitglied unter Mitbestimmung des örtlichen Personalrates gemäß § 80 Abs. 2 Nr. 8 Personalvertretungsgesetz RLP die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten der Hochschule Worms.
- 5.2 Die oder der Datenschutzbeauftragte ist in dieser Funktion weisungsfrei, darf zur Erfüllung der Aufgaben jederzeit Einsicht in sämtliche personenbezogenen Datenverarbeitungsvorgänge nehmen und ist hierüber zur Verschwiegenheit verpflichtet.
- 5.3 Der gesetzliche Aufgabenbereich der oder des Datenschutzbeauftragten ergibt sich aus Art. 39 DS-GVO.

6. Datenschutz-Folgenabschätzung

- 6.1 Vor der Einführung einer neuen Form der Datenverarbeitung, insbesondere eines neuen Datenverarbeitungsverfahrens unter Verwendung neuer Technologien, ist eine Datenschutz-Folgenabschätzung durchzuführen, sofern die geplante Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat.
- 6.2 Ein solches Risiko kann auch bei wissenschaftlichen Umfragen und Befragungen, deren Zweck es ist, Aufschluss über personenbezogene Daten zu erlangen, vorliegen. Die Datenschutz-Folgenabschätzung ist zusätzlich erforderlich bei umfangreicher Verarbeitung besonderer Kategorien personenbezogener Daten, der Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder der systematischen, umfangreichen Überwachung öffentlich zugänglicher Bereiche. Eine Datenschutz-Folgenabschätzung ist unter den Voraussetzungen des Absatzes 1 auch erforderlich bei bestehenden automatisierten Verfahren zur Erhebung von personenbezogenen Daten,

sofern eine solche noch nicht durchgeführt worden und auch keine Vorabkontrolle nach der bis zum 24.05.2018 geltenden Rechtslage erfolgt ist.

- 6.3 Zuständig für die Überprüfung der Erforderlichkeit einer Datenschutz-Folgenabschätzung ist das für Datenschutz zuständige Präsidiumsmitglied, das die oder den Datenschutzbeauftragten zur Beratung hinzuziehen kann. Die geplante Einführung einer neuen Form der Datenverarbeitung ist dem für Datenschutz zuständigen Präsidiumsmitglied von der Leitung der verantwortlichen Fachabteilung in Textform anzuzeigen. Hierbei sind die geplanten Verarbeitungsvorgänge, der Zweck der Verarbeitung, die Betroffenen sowie etwaige vorgesehene Maßnahmen zum Datenschutz zu beschreiben. Das für Datenschutz zuständige Präsidiumsmitglied prüft sodann die Erforderlichkeit einer Datenschutz-Folgenabschätzung.
- 6.4 Hält das für Datenschutz zuständige Präsidiumsmitglied nach Beratung durch die Datenschutzbeauftragte der den Datenschutzbeauftragten die Durchführung einer Datenschutz-Folgenabschätzung für angezeigt, erstellt die nach Ziffer 6.3 zuständige Fachabteilung eine Datenschutz-Folgenabschätzung; sie wird hierbei von dem oder der Datenschutzbeauftragten beraten und unterstützt. Die Datenschutz-Folgenabschätzung muss mindestens die in Art. 35 Abs. 7 DS-GVO benannten Inhalte aufweisen.
- 6.5 Ohne Freigabe durch das für Datenschutz zuständige Präsidiumsmitglied darf kein neues, ganz oder teilweise automatisiertes Verfahren zur Verarbeitung personenbezogener Daten in Betrieb genommen werden. Als ganz oder teilweise automatisierte Verfahren gelten sämtliche Verarbeitungsverfahren, die mindestens teilweise unter Verwendung einer Datenverarbeitungsanlage ausgeführt werden. Dies betrifft bereits einen möglichen Testbetrieb, sofern hierbei personenbezogene Daten verarbeitet werden. Entsprechendes gilt für nichtautomatisierte (analoge) Verfahren zur Verarbeitung personenbezogener Daten, die in einem Dateisystem, also einer Datensammlung, die gleichartig aufgebaut ist und nach bestimmten Ordnungsmerkmalen zugänglich ist oder ausgewertet werden kann, gespeichert sind oder gespeichert werden sollen. Unterliegt die Einführung eines neuen Verfahrens der Datenverarbeitung der Mitbestimmung, sind zudem die Rechte des Personalrats zu berücksichtigen.
- 6.6 Die Vorschriften des Artikels 35 DS-GVO und des § 9 LDSG sind zu beachten.

7. Verzeichnis der Verarbeitungstätigkeiten

- 7.1 In einem Verzeichnis von Verarbeitungstätigkeiten sind sämtliche ganz oder teilweise automatisierten Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem elektronischen System gespeichert sind oder gespeichert werden sollen, aufzulisten. Das Verzeichnis von Verarbeitungstätigkeiten muss die in Art. 30 Abs. 1 DS-GVO aufgeführten Angaben enthalten.
- 7.2 Für das Verzeichnis von Verarbeitungstätigkeiten ist das vom Landesdatenschutzbeauftragten bereitgestellte und auf die Belange der Hochschule Worms angepasste Formular zu verwenden. Das Formular wird von der Hochschule in deren Intranet zur Verfügung gestellt. Die Verarbeitungstätigkeiten können auch digital erfasst werden.
- 7.3 Die Verarbeitungstätigkeiten werden durch die jeweiligen Fachabteilungen erfasst und dem – derzeit beim Datenschutzbeauftragten - zentral geführten Verzeichnis zur dortigen Ablage übermittelt. Die für das Einzelverfahren verantwortliche Fachabteilung behält eine Kopie.

8. Webseiten und Social Media Auftritte der Hochschule Worms

- 8.1 Webseiten und Social Media Auftritte der Hochschule Worms (derzeit "Facebook", "YouTube", "LinkedIn", „Instagram“ und „Twitter“) sind nur zu dienstlichen Zwecken erlaubt. Sie unterliegen dem jederzeitigen Zugriffs- und Entscheidungsrecht des Präsidiums.
- 8.2 Inhalte werden grundsätzlich nicht zensiert. Hiervon ausgenommen sind die rechtliche Kontrolle des Datenschutzes sowie die inhaltliche Kontrolle im Sinne der freiheitlichen demokratischen Grundordnung der Bundesrepublik Deutschland und zur Verhinderung von Straftaten und Ordnungswidrigkeiten.
- 8.3 Webseiten und Social Media Auftritte sind mit einem Impressum nach § 5 Telemediengesetz auszustatten.
- 8.4 Webseiten und Social Media Auftritte sind mit einer Datenschutzerklärung zu versehen, die konkret auf die etwaige Datenverarbeitung der Seite und des Social Media Unternehmens hinweist. Die Nutzerin oder der Nutzer der Seite muss im Rahmen der Datenschutzerklärung umfassend Aufklärung über die Verfahren der Seite, sowie über ihre oder seine individuellen Rechte bis hin zum Widerspruchsrecht erhalten. Verantwortlich hierfür ist die entsprechend für den Auftritt zuständige Leitung der verantwortlichen Fachabteilung der Hochschule Worms nach Beteiligung der oder des Datenschutzbeauftragten und des für Datenschutz zuständigen Präsidiumsmitgliedes.

9. Datenübermittlung an Dritte

- 9.1 Die Übermittlung personenbezogener Daten an außerhalb der Hochschule Worms stehende Dritte ist nur mit Einwilligung der betroffenen Person oder auf Grundlage einer gesetzlichen Erlaubnis zulässig. Jedwede Weiterleitung personenbezogener Daten bedarf dementsprechend einer vorherigen datenschutzrechtlichen Überprüfung. Für Standardprozesse erfolgt diese Überprüfung im Zusammenhang mit der Erstellung und Revision des Verarbeitungsverzeichnisses (vgl. Ziff. 7).
- 9.2 Befindet sich die Empfängerin oder der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen von Betroffenen. Diese sind mit der oder dem Datenschutzbeauftragten abzustimmen. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann. Begründete Ausnahmen bedürfen der Zustimmung durch für Datenschutz zuständige Präsidiumsmitglied in Abstimmung mit dem Rechenzentrum.

10. Auftragsverarbeitung, insbesondere Einschaltung externer Dienstleister

- 10.1 Sofern Dritte personenbezogene Daten im Auftrag der Hochschule Worms verarbeiten sollen bzw. im Rahmen der Auftragsleistungen, etwa als externe Dienstleister, möglicherweise Zugriff auf personenbezogene Daten erhalten, ist die oder der Datenschutzbeauftragte von der verantwortlichen Fachabteilung frühzeitig vorab in Textform zu informieren, um das weitere Prozedere zu klären.
- 10.2 Als Auftragsverarbeitung im Sinne des Absatzes 1 werden auch die Pflege automatisierter Verfahren und die Wartung von Datenverarbeitungsanlagen durch externe Dienstleistungen betrachtet, sofern der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Entsprechendes gilt für die Aktenvernichtung und andere Leistungen durch externe Dienstleistungen, bei denen

Zugriffsmöglichkeiten auf personenbezogene Daten bestehen. Keine Auftragsverarbeitung liegt vor bei der mandatsbezogenen Übermittlung personenbezogener Daten an Berufsgeheimnisträger (z.B. Rechtsanwaltschaft und Steuerberatung zum Zwecke der Mandatsbearbeitung).

- 10.3 Auftragnehmer mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Bei der Auswahl ist sicherzustellen, dass der Auftragnehmer hinreichende Garantien für den Schutz personenbezogener Daten bietet. Die Auswahl ist von der Fachabteilung zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:
- die fachliche Eignung des Auftragnehmers,
 - technische und organisatorische Sicherheitsmaßnahmen des Auftragnehmers,
 - Erfahrung des Auftragnehmers im Markt,
 - sonstige Aspekte, die auf die Zuverlässigkeit des Auftragnehmers schließen lassen (bspw. Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.).
- 10.4 Soll ein Auftragnehmer personenbezogene Daten im Auftrag verarbeiten, bedarf es außerdem zwingend des Abschlusses einer Auftragsverarbeitungsvereinbarung, die inhaltlich den Anforderungen des Art. 28 DS-GVO entspricht. Zum Abschluss einer Auftragsverarbeitungsvereinbarung ist der vom Landesdatenschutzbeauftragten bereitgestellte Mustervertrag, der in der für die Hochschule angepassten Form im Intranet zur Verfügung gestellt wird, als Formulierungshilfe heranzuziehen, sofern keine mit dem Musterformular konforme Vereinbarung des Auftragnehmers vorliegt. In jedem Fall ist sicherzustellen, dass die Belange des Datenschutzes vollumfassend berücksichtigt werden. Jede Auftragsverarbeitungsvereinbarung bedarf der vorherigen Zustimmung der oder des Datenschutzbeauftragten.
- 10.5 Der Auftragsverarbeiter und gegebenenfalls sein Vertreter hat das von ihm geführte Verzeichnis von Verarbeitungstätigkeiten, das die von der Hochschule beauftragten Tätigkeiten enthält, der Hochschule in Kopie vorzulegen. Dieses Verzeichnis soll nach dem vom Landesdatenschutzbeauftragten bereitgestellten Muster entsprechen. Zudem hat der Auftragsverarbeiter der Hochschule nachzuweisen, welche geeigneten technischen und organisatorischen Maßnahmen er im Sinne des Artikels 32 DS-GVO, um ein dem Risiko angemessenes Schutzniveau der Sicherheit der Verarbeitung zu gewährleisten.
- 10.6 Die Hochschule führt ein Verzeichnis, in dem die nach den Ziffern 10.1 bis 10.5 bereit gestellten Unterlagen zusammengefasst werden.

11. Datenschutz in Lehre und Forschung

- 11.1 Sämtliche Lehrkräfte sollen, soweit dies möglich ist, auch bei den wissenschaftlichen Arbeiten ihrer Studierenden die Einhaltung der datenschutzrechtlichen Bestimmungen überwachen. Das betrifft insbesondere internetgestützte Projekte, wie beispielsweise Umfragen.
- 11.2 Im Rahmen ihrer Immatrikulation werden die Studierenden auf datenschutzrechtliche Aspekte ihres Studiums in geeigneter Weise hingewiesen; der Empfang entsprechender Informationsunterlagen und die Verpflichtung, den Datenschutz während des Studiums zu beachten, ist zu bestätigen. Bereits immatrikulierte Studierende werden in geeigneter Weise auf die datenschutzrechtlichen Aspekte informiert.
- 11.3 Alle IT-gestützten Umfragen, welche zu wissenschaftlichen oder sonstigen Zwecken in der Forschung und der Lehre durchgeführt werden, sind aufgrund eines

mit der oder dem Datenschutzbeauftragten abgestimmten Leitfadens durchzuführen, der auf der Webseite der Hochschule zum Abruf bereitgestellt wird..

- 11.4 Sämtliche die Studierenden betreffenden Daten, z.B. in schriftlichen Arbeiten, sind personenbezogene Daten und sind daher gemäß Ziff. 4 zu behandeln.

12. Nutzung von IT-Ressourcen

- 12.1 Für alle dienstlichen Datenübertragungen oder -verarbeitungen (Dateitransfer, E-Mail, sog. „Cloud-Dienste“ etc.) personenbezogener Daten sind – zurzeit - Dienste der Hochschule Worms, des ZIT RLP, der Rechenzentrumsallianz, des Bibliothekenverbundes, des DFN-Vereins oder entsprechende Ressourcen der Wissenschaftsinstitutionen der Bundesrepublik Deutschland zu nutzen. Dies gilt auch für die Nutzung von Videokonferenzsystemen für Lehrveranstaltungen und Online-Besprechungen, die seitens der Hochschule bzw. von Mitarbeiterinnen und Mitarbeitern (Ziffer 2.1) organisiert werden.
- 12.2 Wenn das in begründeten Einzelfällen nicht möglich ist, so ist streng darauf zu achten, dass die Datenverarbeitung oder -speicherung ausschließlich auf Servern von Betreibern stattfindet, die der Datenschutz-Grundverordnung unterliegen und eine Datenverarbeitung innerhalb der Europäischen Union gewährleisten. Auf Servern außerhalb der Europäischen Union dürfen personenbezogene Daten nur mit Zustimmung des für Datenschutz zuständigen Präsidiumsmitgliedes und – erforderlichenfalls – des Personalrats verarbeitet werden, sofern die Voraussetzungen der Art. 44 ff. DS-GVO (Übermittlung personenbezogener Daten an Drittländer oder deren internationale Organisationen) vorliegen. Begründete Ausnahmefälle bedürfen der Zustimmung des für Datenschutz zuständigen Präsidiumsmitgliedes in Abstimmung mit dem Rechenzentrum.
- 12.3 Zweifelhafte Dienste, die erkennbar nicht den datensicherheitstechnischen und datenschutzrechtlichen Erfordernissen entsprechen, sind für die dienstliche Nutzung verboten.
- 12.4 Personenbezogene Daten sind grundsätzlich nicht auf beweglichen Datenträgern wie SD Karten, USB-Sticks oder CD-ROM zu speichern.
- 12.5 Erfolgt im begründeten Einzelfall doch eine Speicherung personenbezogener Daten auf beweglichen Datenträgern, sind diese zu verschlüsseln.
- 12.6 Jede Mitarbeiterin und jeder Mitarbeiter hat dafür zu sorgen, dass beim Verlassen des Arbeitsplatzes der Bildschirm gesperrt ist und keine Unterlagen mit personenbezogenen Daten offen einzusehen sind.

13. Passwortvergabe

- 13.1 Für autorisierte Personen ist eine Benutzerkennung einzurichten und ein Anfangspasswort zuzuweisen. Dieses muss bei der ersten Anmeldung geändert werden. Des Weiteren muss es geändert werden nach einem Verdacht der Ausspähung.
- 13.2 Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten und Dritten nicht weitergegeben werden.
- 13.3 Für alle Passwörter gelten im Übrigen verpflichtend die Regeln hinsichtlich der Passwortgestaltung, die im Intranet der Hochschule unter „Dienstanweisung Datenschutz“ zu finden sind.

14. Nutzung des E-Mail-Dienstes der Hochschule Worms

- 14.1 Die Hochschule Worms stellt Mitarbeiterinnen und Mitarbeitern (Ziffer 2.1) ihren E-Mail-Dienst ausschließlich für dienstliche Zwecke zur Verfügung. Die Privatanutzung der dienstlichen E-Mail-Dienste ist untersagt. Sollten E-Mails privaten

Inhalts eingehen, sind diese aus dem dienstlichen E-Mail-Konto zu löschen. Ein vorheriges Weiterleiten privater Nachrichten auf ein privates Konto ist Mitarbeiterinnen und Mitarbeitern in diesem Fall freigestellt.

- 14.2 E-Mails sind grundsätzlich mit entsprechender Verfasserin oder Verfasser im Klarnamen zu versenden. Die Nutzung des E-Mail-Dienstes zur Übermittlung personenbezogener Daten oder allgemein dem Amtsgeheimnis unterliegender Daten über das Internet sollte möglichst nur in verschlüsselter Form erfolgen. Über die Erstellung der digitalen Zertifikate berät das Rechenzentrum auf Anfrage. Eine Übermittlung personenbezogener Daten per Mail an Adressaten, die nicht der Hochschule angehören, sollte nur dann erfolgen, wenn eine digitale Verschlüsselung über diese Zertifikate erfolgt.
- 14.3 Ist eine Übermittlung gemäß Ziffer 14.2 nicht möglich, sollen die Daten in eine sichere Cloud (siehe Ziffer 16.7) abgelegt und vom Adressaten dort über einen übermittelten Link abgerufen werden.
- 14.4 Sollte dennoch eine Übermittlung personenbezogener Daten im Rahmen eines Mail-Attachments erfolgen, ist dieses mit einem Passwort zu belegen, das dem Mail-Adressaten auf anderem Wege, beispielsweise telefonisch, mitgeteilt wird.
- 14.5 Dienstliche E-Mails sind grundsätzlich und wo immer möglich über sogenannte Funktionsadressen zu versenden, z.B. helpdesk@hs-worms.de, datenschutz@hs-worms.de, personalrat@hs-worms.de.
- 14.6 Fälschlicherweise erhaltene E-Mails, die personenbezogene Daten enthalten, sind unverzüglich zu löschen. Wurden fälschlicherweise personenbezogene Daten an unbefugte Dritte übermittelt, so ist die Empfängerin oder der Empfänger unverzüglich aufzufordern, diese zu löschen. Eine detaillierte Anleitung, wie bei der Übermittlung von personenbezogenen Daten an Unbefugte zu verfahren ist, findet sich im Intranet unter „Dienstanweisung Datenschutz“.
- 14.7 Die Weiterleitung von dienstlichen E-Mails auf private E-Mail-Konten ist verboten. Ziff. 14.1 Satz 3 bleibt unberührt.

15. Webbasierte Lehrveranstaltungen und Videokonferenzen („Online Meetings“)

- 15.1 Lehrveranstaltungen, die online durchgeführt werden und während der Durchführung einen unmittelbaren Dialog zwischen Lehrenden und Teilnehmenden nicht zwingend erfordern, können von den Lehrenden vorab als sog. Screencast aufgezeichnet werden, um diese Aufzeichnung den Studierenden zum Abruf im Netz bereitzustellen. Bei einem Screencast wird die Lehrveranstaltung somit nicht in Form einer Webkonferenz mit ständigen Rückfragemöglichkeiten übertragen. Ein unmittelbarer Dialog zwischen Lehrenden und Teilnehmenden findet jedenfalls nicht in Echtzeit statt.
- 15.2 Lehrveranstaltungen, die online als Web-Seminare oder Web-Konferenzen unter Einsatz von Videokonferenztechnik durchgeführt werden, sollen als Online Meeting, also live übertragene virtuelle Treffen, durchgeführt werden. Online Meetings ermöglichen den Dialog zwischen Lehrenden und Teilnehmenden während der Durchführung der Lehrveranstaltung. Der Dialog kann bspw. unter Verwendung der Chat-Funktion oder durch Freischaltung der Mikrofone erfolgen. Auf diese Weise haben Teilnehmende ständige Rückfragemöglichkeiten.
- 15.3 Die Aufzeichnung von Online Meetings ohne vorherige freiwillige Einwilligung sämtlicher Teilnehmenden ist verboten und kann unter den Voraussetzungen des § 201 StGB strafrechtlich geahndet werden. Das Verbot gilt für sämtliche Arten von Online Meetings und ist nicht auf Lehrveranstaltungen begrenzt. Soll eine als Online Meeting durchgeführte Veranstaltung aufgezeichnet werden, ist

dies vorab in transparenter Form unter Angabe des Zwecks der Aufzeichnung anzukündigen. Zudem sind vorab Einwilligungen sämtlicher Teilnehmenden einzuholen. Die Einwilligung erfolgt freiwillig und ist jederzeit widerruflich. Haben einzelne Teilnehmende die Einwilligung verweigert, darf die Aufzeichnung nicht erfolgen. Zur Erleichterung der Handhabung wird seitens des Rechenzentrums eine Handreichung erstellt und zur Verfügung gestellt.

16. Verwendung dienstlicher Hardware durch Mitarbeiter/innen (Nr. 2.1.)

- 16.1 Mitarbeiterinnen und Mitarbeiter verwenden für die Wahrnehmung ihrer dienstlichen Tätigkeit grundsätzlich hochschuleigene Endgeräte. Die Nutzung nicht hochschuleigener Endgeräten ist zulässig, wenn von der Hochschule angebotene und zugelassene Clouddienste und/oder hochschuleigene Netzwerke und Terminal-Server über einen VPN-Tunnel genutzt werden und sämtliche Anforderungen des Datenschutzes und der Datensicherheit gewährleistet sind.
- 16.2 Von der Hochschule wird ein Endgerät samt erforderlicher Software und ein Zugang zum Hochschulnetzwerk zur Verfügung gestellt. Die Organisationseinheiten gewährleisten, mit Unterstützung des Rechenzentrums, die technische Betreuung und Wartung der bereitgestellten Hard- und Software.
- 16.3 Den Mitarbeiterinnen und Mitarbeitern ist es untersagt personenbezogene oder sonstige vertrauliche Daten der Hochschule Worms an Dritte weiterzugeben, sie Dritten zur Kenntnis gelangen zu lassen (etwa durch Einsichtnahme am Bildschirm oder auf Ausdrucken), sie auf externen Speichermedien abzuspeichern, zu kopieren oder zu anderen als dienstlichen Zwecken zu verwenden.
- 16.4 Verlässt die Mitarbeiterin oder der Mitarbeiter den (auch mobilen) Arbeitsplatz, muss sichergestellt werden, dass keine Dritten auf die dienstlichen Daten zugreifen können.
- 16.5 Werden Mitarbeiterinnen und Mitarbeiter mit Zustimmung der Hochschule Worms vom mobilen Arbeitsplatz aus dienstlich tätig, bleiben sie Teil der Hochschule Worms. Dies bedeutet, dass alle Weisungsrechte bestehen bleiben und insbesondere alle behördlichen Daten, Informationen und Unterlagen, auf die Mitarbeiterinnen und Mitarbeiter von ihrem mobilen Arbeitsplatz aus Zugriff haben, ausschließlich im Hoheitsbereich der Hochschule Worms bleiben. Einzelheiten zur „Mobilen Arbeit“ werden in einer Dienstvereinbarung geregelt.
- 16.6 Abweichend von Nr. 16.1. ist Mitarbeiterinnen und Mitarbeitern die dienstliche Nutzung browserbasierter Dienste (z.B. Webmailer) des Hochschul-Rechenzentrums über private Endgeräten gestattet, wenn und soweit es sich dabei um reine Webdienste handelt, über die Browsernutzung hinaus keine dienstlichen Informationen auf dem privaten Endgerät gespeichert werden, die Betriebs- und Browsersoftware auf dem jeweiligen Endgerät einen aktuellen Stand hat und das Endgerät über einen aktuellen Virens Scanner verfügt.
- 16.7 Abweichend von Nr. 16.1 ist Lehrbeauftragten die Nutzung nicht-hochschuleigener Endgeräte erlaubt, wenn sichergestellt ist, dass die Speicherung personenbezogener Daten der Hochschule nicht auf diesen Endgeräten gespeichert werden und von der jeweiligen Lehrkraft hinsichtlich des verwendeten Endgerätes sämtliche Anforderungen des Datenschutzes und der Datensicherheit gewährleistet werden. Zur Ablegung personenbezogener Daten sind die von der Hochschule angebotenen Dienste zu nutzen. Dies sind zurzeit die Rheinland-Pfalz-Cloud (seafile), z.B. durch Nutzung des Cloudspeichers als Laufwerk (Seadrive) sowie der Zugriff auf hochschuleigene Netzlaufwerke und Terminalserver über VPN. Ist den Lehrbeauftragten die Nutzung der von der Hochschule angebotenen Dienste nachweisbar nicht möglich, sind sie ver-

pflichtet, mit dem Rechenzentrum eine vergleichbare datenschutzsichere Lösung abzustimmen. In ihrem Lehrauftrag werden Lehrbeauftragte besonders auf diese Dienstanweisung hingewiesen; deren Einhaltung ist zu bestätigen.

17. Verpflichtung auf das Datengeheimnis (gem. § 8 LDSG RLP)

- 17.1 Sämtliche Mitarbeiterinnen und Mitarbeiter (Ziffer 2.1) sind verpflichtet, das Datengeheimnis zu wahren. Sie unterliegen hierbei der Verschwiegenheitspflicht. Die Regelungen des § 37 Beamtenstatusgesetz für verbeamtetes Personal finden analog Anwendung auf den in Ziffer 2.1 genannten im privaten Vertragsverhältnis beschäftigten Personenkreis.
- 17.2 Sämtliche Mitarbeiterinnen und Mitarbeiter sind bei ihrer Einstellung über das Datengeheimnis an der Hochschule Worms schriftlich zu belehren und auf das Datengeheimnis zu verpflichten (Anlage).
- 17.3 Für Studierende gilt Ziffer 11.2.

18. Verfahren zur Wahrung der Betroffenenrechte

- 18.1 Betroffene Personen haben nach den Vorschriften der DS-GVO, die im Einzelfall durch das Landesdatenschutzgesetz ergänzt sind, folgende Rechte:
 - Auskunftsrecht (Art. 15 DS-GVO)
 - Recht auf Berichtigung (Art. 16 DS-GVO)
 - Recht auf Löschung / Recht auf Vergessenwerden“ (Art. 17 DS-GVO)
 - Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)
 - Recht auf Datenübertragbarkeit (Art. 19 DS-GVO)
 - Widerspruchsrecht (Art. 21 DS-GVO)
 - Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – unterworfen zu werden ... (Art. 22 DS-GVO)
 - Recht auf Beschwerde bei der Aufsichtsbehörde (Art. 77 DS-GVO)
 - Recht auf wirksamen gerichtlichen Rechtsbehelf... (Art. 79 DS-GVO)
- 18.2 Das für Datenschutz zuständige Präsidiumsmitglied legt in Zusammenarbeit mit der oder dem Datenschutzbeauftragten und dem Personalrat ein Verfahren fest, wie die Rechte der Betroffenen an der Hochschule sichergestellt und wie entsprechende Anträge der Betroffenen bearbeitet werden. Alle Hochschulbediensteten sind zur Unterstützung der Antragsbearbeitung verpflichtet.
- 18.3 Betroffene sind spätestens innerhalb eines Monats über alle ergriffenen Maßnahmen nach den Artikeln 15 bis 22 DS-GVO, die auf ihren Antrag hin erfolgt sind, zu informieren. Diese Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. Die Hochschule unterrichtet die betroffene Person in diesem Fall innerhalb eines Monats nach Eingang des Antrags über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung.
- 18.4 Die oder der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

19. Inkrafttreten

Diese Dienstanweisung tritt mit ihrer Unterzeichnung in Kraft. Sie gilt bis auf Widerruf. Gleichzeitig tritt die Dienstanweisung über den Datenschutz und die Datensicherheit in der Fachhochschule Worms vom 1.12.1999 außer Kraft.

Worms, den 20. August 2021



Prof. Dr. Jens Hermsdorf
Präsident

Anlagen

Anlage: Einheitliche Verpflichtungserklärung



Kerstin Henzel
stellv. Kanzlerin

Anlage zur Dienstanweisung Datenschutz der Hochschule Worms
- Verpflichtungserklärung auf das Datengeheimnis nach § 8 LDSG RLP

Vertraulichkeitsverpflichtung

1. Angaben zum oder zur Verpflichteten

(Name, Titel, Vorname)

Tätigkeit/Tätigkeitsbereich

2. Allgemeine Vertraulichkeit

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Ihnen im Rahmen Ihrer Tätigkeit für die Hochschule Worms auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.

Nach den gesetzlichen Bestimmungen ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder unbefugtem Zugang führt.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen. Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen die Pflichten aus dem Dienst-, Anstellungs- bzw. Auftragsverhältnis dar, der entsprechend geahndet werden kann.

Informationen zu Rechtsvorschriften, auf die in dieser Verpflichtung Bezug genommen wird, werden im Intranet der Hochschule unter „Dienstanweisung Datenschutz“ zum Abruf bereitgestellt (siehe auch Ziffer 1.7. der Dienstanweisung)

3. Geltungsdauer und Geltungsbereich

Die Verpflichtung auf die Vertraulichkeit besteht auch nach der Beendigung des Dienst-, Auftrags- bzw. Beschäftigungsverhältnisses fort. Ihre sich aus einer etwaigen gesonderten Vereinbarung ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Ich erkläre, in Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten. Mit meiner Unterschrift bestätige ich zugleich, dass ich auf die Möglichkeit des Abrufs von Informationen zu Rechtsvorschriften, auf die in dieser Verpflichtung Bezug genommen wird, hingewiesen wurde.

Ort

Datum

Unterschrift Verpflichtete bzw. Verpflichteter

Impressum:

Hochschule Worms | Erenburgerstraße 19 | 67549 Worms
T: +49(0)6241.509-0 | F: +49(0)6241.509-222
E-Mail: kontakt@hs-worms.de | Internet: www.hs-worms.de

Die Hochschule Worms ist eine Körperschaft des Öffentlichen Rechts. Sie wird durch den Präsidenten Prof. Dr. Jens Hermsdorf gesetzlich vertreten. Umsatzsteueridentifikationsnummer: DE813351149

Zuständige Aufsichtsbehörde: Ministerium für Bildung, Wissenschaft, Jugend und Kultur des Landes Rheinland-Pfalz, Mittlere Bleiche 61, D-55116 Mainz. Inhaltlich Verantwortlicher gemäß § 7 TMG: Der Präsident der Hochschule Worms, Prof. Dr. Jens Hermsdorf.