Hochschule RheinMain

AMTLICHE MITTEILUNG

Nr.: 798
Veröffentlicht am 02.11.2022

Leitlinie Datenschutz an der Hochschule RheinMain

BEKANNTMACHUNG

Nach § 1 der Satzung der Hochschule RheinMain zur Bekanntmachung ihrer Satzungen vom 04. Juni 2013 (StAnz. vom 29.7.2013, S. 929) wird die Leitlinie Datenschutz an der Hochschule RheinMain hiermit bekanntgegeben.

Wiesbaden, 02.11.2022

Prof. Dr. Eva Waller
Präsidentin

Herausgeber:
Präsidentin
Hochschule RheinMain
Postfach 3251
65022 Wiesbaden

Redaktion:
Abteilung VIII
Rainer Scholl
E-Mail: rainer.scholl@hs-rm.de

LEITINIE DATENSCHUTZ AN DER HSRM

Das Präsidium der Hochschule RheinMain hat am 19.09.2022 im Benehmen mit dem Senat die folgende Datenschutzleitlinie für die HSRM beschlossen.

PRÄAMBEL

Die Verarbeitung personenbezogener Daten ist für das Funktionieren einer modernen Hochschule unerlässlich. Die Wahrung des Schutzes personenbezogener Daten ist dabei eine Aufgabe, die sich in allen Bereichen der Hochschule auf je unterschiedliche Art und Weise stellt. Die Hochschule gewährleistet den Datenschutz entsprechend der gesetzlichen Bestimmungen und versetzt ihre Mitglieder und Angehörigen in die Lage, Datenschutzfragen als Querschnittaufgabe identifizieren und effizient und effektiv bearbeiten zu können.

§ 1 BEGRIFFBESTIMMUNGEN UND GELTUNGSBEREICH

(1) BEGRIFFSBESTIMMUNGEN

Hochschulmitglieder im Sinne dieser Leitlinie sind Professorinnen und Professoren sowie das wissenschaftliche, administrative und technische Personal. [1] Hochschulangehörige im Sinne dieser Leitlinie sind gastweise oder nebenberuflich an der Hochschule tätige Personen sowie die zur Promotion Zugelassenen.[2]

(2) GELTUNGSBEREICH

Diese Leitlinie gilt nicht für die Organe der verfassten Studierendenschaft[3], den Personalrat[4], An-Institute der HSRM, Gesellschaften oder Vereine, an der die HSRM oder Mitglieder oder Angehörige der HSRM im Namen oder im Interesse der HSRM beteiligt ist bzw. sind.

---

[1] Vgl. §37 HessHG
[2] Vgl. §37 HessHG
[3] Die Studierendenschaft als Körperschaft des öffentlichen Rechts (Art. 76 Abs.1 S.2 HHG) ist eine juristische Person. Als solche ist sie zwar ‚Glied der Hochschule', entscheidet aber selbständig und eigenverantwortlich über die Verarbeitung personenbezogener Daten. Der/die Präsident:in der Hochschule entscheidet hier nicht mit, sondern übt lediglich die Rechtsaufsicht über die Aktivitäten der verfassten Studierendenschaft und damit auch über die damit einhergehende Verarbeitung personenbezogener Daten aus (§ 80 S.1 HHG). Im Ergebnis ist die verfasste Studierendenschaft selbst Verantwortlicher i.S.d. DS- GVO.
[4] HMWK-ERLASS 1722, 20. November 2020

§2 DATENSCHUTZSTRATEGIE UND DATENSCHUTZZIELE

(1) DATENSCHUTZSTRATEGIE

Zur Gewährleistung des Datenschutzes entsprechend der gesetzlichen Bestimmungen an der Hochschule und zur Unterstützung ihrer Mitglieder und Angehörigen bei der Erfüllung von Datenschutzaufgaben strebt die Hochschule folgende Ziele an:

1. Sicherstellung der Erfüllung der gesetzlichen Bestimmungen und der sich hieraus ergebenden Pflichten durch hochschulinterne Klärung der Verantwortlichkeiten;
2. Aufbau und Betrieb eines systematischen datenbankgestützten Datenschutzmanagementsystems (DSMS);
3. Schaffung von Unterstützungsstrukturen für die Bewältigung datenschutzrechtlicher Fragestellungen;
4. Einrichtung eines datenschutzrechtlichen Schulungsangebots für Mitglieder und Angehörige;
5. Bereitstellung von Vorlagen und Leitfäden

Die Umsetzung dieser strategischen Ziele wird zwei Jahre nach Inkrafttreten dieser Richtlinie geprüft. Den Ergebnissen dieser Prüfung wird ggfls. durch eine Anpassung dieser Richtlinie Rechnung getragen.

(2) DATENSCHUTZZIELE, TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Jede Verarbeitung personenbezogener Daten muss den Zielen der

1. Zweckbindung
2. Nichtverkettung
3. Datenminimierung/Datensparsamkeit
4. Speicherbegrenzung
5. Transparenz
6. Intervenierbarkeit
7. Vertraulichkeit

8. Verfügbarkeit und Integrität

verpflichtet sein.[5]

Im Rahmen der Umsetzung der Datenschutzstrategie der Hochschule sind diese Datenschutzziele in sämtlichen technischen, organisatorischen sowie infrastrukturellen Bereichen zugrunde zu legen. Die Hochschule trifft zudem diejenigen technischen und organisatorischen Maßnahmen, die erforderlich sind, um ein angemessenes Schutzniveau für verarbeitete personenbezogen Daten sicherzustellen.

§3 MASSNAHMEN ZUR UMSETZUNG DER DATENSCHUTZ-STRATEGIE

(1) ORGANISATORISCHE SICHERSTELLUNG DER ERFÜLLUNG DER GESETZLICHEN DATENSCHUTZBESTIMMUNGEN

1. Die Verantwortung für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz und den Regelungen dieser Leitlinie liegt bei der Hochschule, vertreten durch die Präsident:in. Die Präsident:in kann die Aufgabenwahrnehmung auf ein Präsidiumsmitglied delegieren.

2. Die Einhaltung der datenschutzrechtlichen Bestimmungen ist überdies Verpflichtung und Verantwortung aller Mitglieder und Angehörigen der Hochschule. Die Leitungskräfte sind für die Einhaltung der Datenschutzverpflichtungen in ihrem Bereich verantwortlich und motivieren ihre Mitarbeiterinnen und Mitarbeiter für die Erreichung der Zielsetzungen dieser Leitlinie. Die Mitarbeiterinnen und Mitarbeiter unterstützen die Leitungskräfte bei der Erfüllung der datenschutzrechtlichen Vorgaben (bspw. durch Beachtung von Berechtigungs- und Löschkonzepten) und sind zu Hinweisen an Vorgesetzte bei Datenpannen und Sicherheitslücken verpflichtet, sobald sie diese erkennen.

3. Die Leitungskräfte benennen einen Datenschutzkoordinator/eine Datenschutzkoordinatorin auf Abteilungs- bzw. Fachbereichsebene. Die Leitungskraft teilt die Benennung dem/der Datenschutzbeauftragten und dem/der Justiziar:in für das Datenschutzmanagement mit.

[5] Siehe Anlage 1

(2) AUFBAU UND BETRIEB EINES SYSTEMATISCHEN DATENBANKENGESTÜTZTEN DATENSCHUTZMANAGEMENTSYSTEMS

1. Das Datenschutzmanagementsystem ist die zentrale datenbankgestützte Plattform der Hochschule zur Erfüllung ihrer datenschutzrechtlichen Verpflichtungen (insbes. zur Führung des Verzeichnisses der Verarbeitungstätigkeiten, zur Durchführung von Datenschutzaudits, zur Bearbeitung von Betroffenenanfragen und Sicherheitsvorfällen), zur Steuerung der damit verbundenen Prozesse und zum Reporting an das Präsidium und ggfls. an die Aufsichtsbehörde. Seine Nutzung für die Durchführung und Dokumentation datenschutzrechtlich relevanter Prozesse ist für die Hochschulleitung, die Hochschulverwaltung, die zentralen Einrichtungen und die Fachbereiche verbindlich.

2. Die Leitungskraft und der/die benannte Datenschutzkoordinator:in werden im Datenschutzmanagementsystem als Verfahrensverantwortliche hinterlegt und sind für die Bearbeitung der mit dem Betrieb des Managementsystems anfallenden Aufgaben verantwortlich.

(3) UNTERSTÜTZUNGSSTRUKTUREN

1. Zur Unterstützung des Präsidiums und der Bereiche der Hochschule wird eine Arbeitsgruppe, Datenschutz und Informationssicherheit‘ gebildet, welcher der/die Datenschutzbeauftragte der Hochschule, der/die Chief Information Security Officer (CISO) und ein:e vom Präsidium benannte:r Justiziar:in für das Datenschutzmanagement angehören. Anfragen in Datenschutzangelegenheiten werden in der Arbeitsgruppe gesammelt, ausgewertet und von deren Mitgliedern ihren Funktionen entsprechend beantwortet.[6]

2. Die Mitglieder der Arbeitsgruppe tauschen sich regelmäßig untereinander und mit dem für den Datenschutz zuständigen Präsidiumsmitglied aus.

3. Der/die Datenschutzbeauftragte unterrichtet und berät das Präsidium, die Angehörigen und Mitglieder der Hochschule, die Verarbeitungen durchführen, hinsichtlich ihrer datenschutzrechtlichen Pflichten und berät – auf Anfrage – bei der Erstellung der Datenschutz-Folgenabschätzungen.

4. Der / die Justiziar:in für das Datenschutzmanagement berät das Präsidium und die Mitglieder sowie die Angehörigen der Hochschule in allen rechtlichen und organisatorischen Fragen des Datenschutzes, führt das Verzeichnis der Verarbeitungstätigkeiten, nimmt

[6] Siehe Anlage 2

ggfls. notwendige Datenschutz-Folgeabschätzungen (DSFA) vor und übernimmt die Betreuung der datenschutzrechtlich relevanten Dokumente der Hoch- schule einschließlich der Verträge zur Auftragsdatenverarbeitung. Er / Sie ist Ansprechpartner:in des Verantwortlichen bei Anfragen zu Betroffenenrechten und nimmt in Abstimmung mit dem Präsidium die Pflichten des Verantwortlichen zur Kommunikation mit den Aufsichtsbehörden (insbesondere Meldung von datenschutz- rechtlichen Verstößen) und bei einschlägigen Gerichtsverfahren wahr.

5. Der / die CISO ist zuständig für grundsätzliche Fragen der Informationssicherheit und informiert über und berät zu Schnittstellenproblemen, die zwischen Informationssicherheit und Datenschutz entstehen können.

(4) SCHULUNGS- UND SONSTIGE UNTERSTÜTZUNGSANGEBOTE

1. Den Mitgliedern und Angehörigen der Hochschule werden regelmäßig adressatengerechte Datenschutzschulungen und -weiterbildungen angeboten. Die Schulungen werden von dem/der Justiziar:in für das Datenschutzmanagement im Zusammenwirken mit der/dem Datenschutzbeauftragten konzipiert und als e-Learning durchgeführt.

2. Der / die Justiziar:in für das Datenschutzmanagement erstellt thematisch strukturierte Leitfäden (bspw. für die Erstellung von Löschkonzepten) und Vorlagen (bspw. für Einwilligungserklärungen), die bei der Erfüllung datenschutzrechtlicher Verpflichtungen heranzuziehen sind.

§ INKRAFTTRETEN

Diese Leitlinie tritt am Tage nach der Veröffentlichung in den Amtlichen Mitteilungen der Hochschule RheinMain in Kraft.

ANLAGE 1:
DATENSCHUTZZIELE

Die Datenschutzziele werden nachstehend wie folgt definiert:

(1) ZWECKBINDUNG

1. Das Datenschutzziel Zweckbindung bezeichnet die Anforderung, personenbezogene Daten grundsätzlich nur für festgelegte, eindeutige und rechtmäßige Zwecke zu erheben und nur in einer mit diesen Zwecken vereinbarenden Weise weiterzuverarbeiten.

2. Rechtmäßig ist ein Zweck, wenn die Verarbeitung der betreffenden personenbezogenen Daten auf Rechtsgrundlagen der DSGVO, des HDSIG, des HHG, der (auslaufenden) HImmaV oder hochschulinterner Satzungen bzw. Dienstvereinbarungen beruht.

(2) NICHTVERKETTUNG

Das Datenschutzziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten, die für unterschiedliche Zwecke erhoben wurden, nicht zusammengeführt (verkettet) werden dürfen.

(3) DATENMINIMIERUNG/ DATENSPARSAMKEIT

Das Datenschutzziel Datenminimierung/ Datensparsamkeit konkretisiert und operationalisiert den Grundsatz, nicht mehr personenbezogene Daten zu verarbeiten, als für das Erreichen des Verarbeitungszwecks benötigt werden.

(4) SPEICHERBEGRENZUNG

Das Datenschutzziel Speicherbegrenzung konkretisiert das Datenminimierungsgebot und erstreckt es nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Insbesondere muss sichergestellt werden, dass personenbezogene Daten nur so lange in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, wie es für den Zweck der Verarbeitung erforderlich ist.

(5) TRANSPARENZ

1. Das Datenschutzziel Transparenz bezeichnet die Anforderung, die Datenverarbeitung gegenüber betroffenen Personen und Aufsichtsbehörden transparent zu halten. Dies umfasst Anforderungen an die Rechenschaftspflicht nach Art. 5 DSGVO, Informations- und Auskunftspflichten gemäß Art. 12 ff DSGVO, die Benachrichtigungspflicht nach Art. 33, 34 DS-GVO, die Dokumentation der Verarbeitung nach Art. 30 DS-GVO.

2.Intern bezeichnet es die Anforderung, Datenlebenszyklen (erheben, verwenden, vernichten) zu formulieren und Verantwortlichkeiten für die jeweiligen Teilschritte zu definieren.

(6) INTERVENIERBARKEIT:

1.Das Datenschutzziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Information, Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch und Erwirkung des Eingriffs in automatisierte Einzelentscheidungen bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden und die entsprechenden Maßnahmen durch die verantwortliche Stelle umgesetzt werden.

2. Hierbei sind insbesondere die Vorgaben von Art. 25 DSGVO (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) zu berücksichtigen.

(7) VERTRAULICHKEIT:

1. Das Datenschutzziel Vertraulichkeit bezeichnet die Anforderung, dass keine unbefugte Person personenbezogene Daten zur Kenntnis nehmen oder nutzen kann.

2. Unbefugte sind auch Beschäftigte von technischen Dienstleistern, die zur Erbringung der Dienstleistung keinen Zugriff zu personenbezogenen Daten benötigen, oder Personen in Organisationseinheiten, die keinerlei inhaltlichen Bezug zu einer Verarbeitungstätigkeit oder zu der jeweiligen betroffenen Person haben.

3. Hierbei sind insbesondere die Vorgaben von Art. 25 DSGVO (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen) zu berücksichtigen.

(8) VERFÜGBARKEIT:

1. Das Datenschutzziel Verfügbarkeit gewährleistet die Verfügbarkeit der Daten zu dem jeweiligen Zweck, solange dieser noch besteht.

2. Systeme und Prozesse müssen auf Ereignisse, welche Störungen der regulären Abläufe verursachen, hinreichend vorbereitet sein.

(9) INTEGRITÄT:

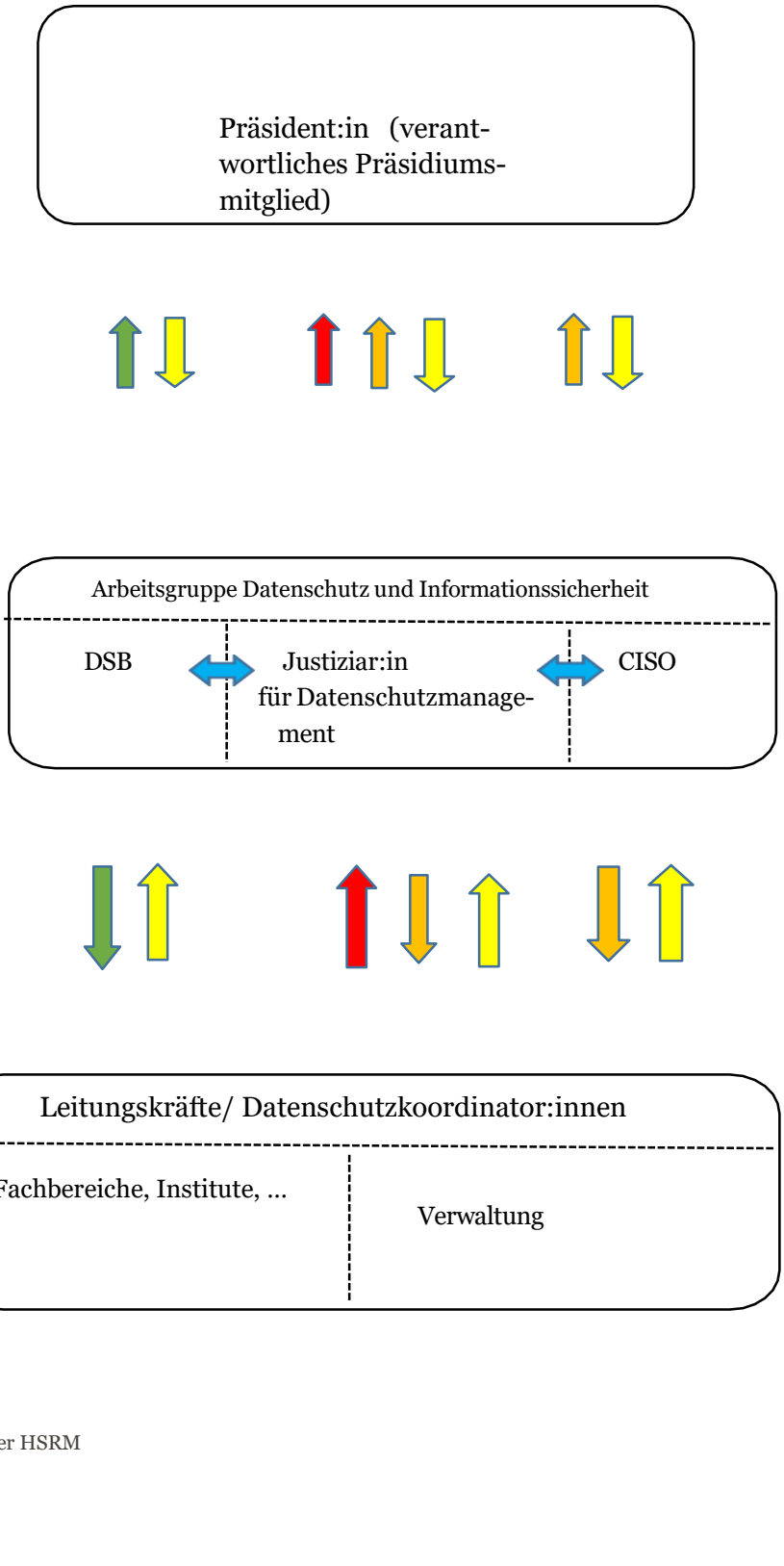
1. Das Datenschutzziel Integrität bezeichnet zum einen die Eigenschaft, dass die zu verarbeitenden Daten unversehrt, vollständig, richtig und aktuell bleiben. Abweichungen von diesen Eigenschaften müssen ausgeschlossen werden oder zumindest feststellbar sein, damit eine Berücksichtigung und Korrektur vollzogen werden kann.

2. Andererseits bezeichnet es die Anforderung, dass informationstechnische Prozesse und Systeme die Spezifikationen kontinuierlich einhalten, die zur Ausübung ihrer zweckbestimmten Funktionen für sie festgelegt wurden.

Quelle: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz) 2019.
https://www.datenschutzkonferenz-online.de/media/ah/20191106_SDM-Methode_V2.0.pdf

ANLAGE 2:

ORGANIGRAMM ZUR VERTEILUNG DER ZUSTÄNDIGKEITEN NACH DIESER LEITLINIE



= Meldung von Datenschutzverstößen
= Unterstützung, Zusammenarbeit
= Anfragen
= Beratung, Überwachung
= Zusammenarbeit