bwDigiRecht
Rechtsinformationsstelle für die digitale Lehre

# Rechtsbereichs-spezifische Betrachtung von KI: Datenschutz

Eine Handreichung der Rechtsinformationsstelle für die digitale Lehre bwDigiRecht

23.05.2025

Jana Knecht

Inhaltsverzeichnis

# Rechtsbereichsspezifische Betrachtung von KI: Datenschutz[1]

***Jana Knecht (bwDigiRecht), 23.05.2025***

Die vorliegende Handreichung untersucht die rechtlichen Implikationen des Einsatzes von Systemen der Künstlichen Intelligenz (KI) in der Lehre im Zusammenhang mit datenschutzrechtlichen Anforderungen. Der Schwerpunkt liegt auf der Analyse der datenschutzrechtlichen Rahmenbedingungen gemäß der Datenschutz-Grundverordnung (DSGVO) sowie der KI-Verordnung. Im Fokus stehende zentrale Fragestellungen betreffen die Zulässigkeit der Verarbeitung personenbezogener Daten durch KI-Systeme. Dabei werden die datenschutzrechtlichen Rechtsgrundlagen differenziert betrachtet und hinsichtlich ihrer Anwendbarkeit im Kontext von KI bewertet. Im Hochschulkontext werden die Anforderungen wie das Prinzip der Datenminimierung, die Erfüllung von Transparenzpflichten und der Umgang mit automatisierten Entscheidungen näher betrachtet. Anhand konkreter Anwendungsbeispiele, etwa des Einsatzes von Proctoring-Software bei Prüfungen, werden zentrale rechtliche Herausforderungen, einschließlich der datenschutzrechtlichen Bewertung von Datenübermittlungen in Drittstaaten, herausgearbeitet.[2]

## 1. Rechtmäßigkeit der Verarbeitung personenbezogenen Daten im Kontext von KI-Systemen

Die KI-Verordnung adressiert in vielfältiger Weise datenschutzrechtliche Fragestellungen im Zusammenhang mit dem Einsatz von KI.[3] Ein wesentlicher Punkt für die nachfolgenden Erläuterungen ist das Verhältnis zwischen der KI-Verordnung und der DSGVO. Zwar wird in Art. 2 Abs. 7 Satz 2 KI-VO zunächst festgehalten, dass die KI-Verordnung die DSGVO grundsätzlich nicht berührt. Von diesem Grundsatz macht Art. 10 KI-VO jedoch Ausnahmen.[4] Diese Ausnahmen betreffen zum einen Verarbeitung von besonderen Kategorien personenbezogener Daten i.S.d Art. 9 Abs. 1 DSGVO zur Aufdeckung und Behebung von Bias bei Hochrisiko-KI-Systemen, Art. 10 Abs. 5 KI-VO, zum anderen Nutzung von personenbezogenen Daten in Reallaboren, Art. 59 KI-VO. Die KI-Verordnung ist daher im datenschutzrechtlichen Kontext als eine Ergänzung der DSGVO zu verstehen, welche insbesondere in

[1] Alle hier zitierten Online-Quellen wurden zuletzt am 22.05.2025 abgerufen. Kostenlos abrufbare Medien sind in den Fußnoten und im Literaturverzeichnis verlinkt.

[2] Wir danken der Zentralen Datenschutzstelle der baden-württembergischen Universitäten (ZENDAS) für den konstruktiven Austausch und die inhaltlichen Anregungen.

[3] *Bayrisches Landesamt für Datenschutzaufsicht*, KI & Datenschutz, Künstliche Intelligenz.

[4] Vgl. *Martini/Wendehorst*, KI-VO: Verordnung über Künstliche Intelligenz Art. 10, Rn. 6.

den Bereichen der Datensicherheit, der Transparenz und der Datenverarbeitungspflichten relevant wird.[5]

Im Zentrum der datenschutzrechtlichen Vorgaben steht der Schutz **personenbezogener Daten**. Diese sind gemäß Art. 4 Nr. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Identifizierbarkeit kann etwa durch Namen, Matrikelnummern, Standortdaten oder Online-Kennungen gegeben sein.[6] Der Schutz dieser Daten ist zentral, da sie Rückschlüsse auf die Identität und Privatsphäre der betroffenen Person zulassen.[7]

Gerade beim Einsatz von KI-Systemen ist die rechtmäßige Verarbeitung personenbezogener Daten von zentraler Bedeutung, insbesondere im Hinblick auf die erforderliche Rechtsgrundlage.[8] Eine besondere Schutzwürdigkeit kommt dabei den in Art. 9 Abs. 1 DSGVO definierten **besonderen Kategorien** personenbezogener Daten, den sogenannten sensiblen Daten, zu. Dazu zählen unter anderem Angaben zur ethnischen Herkunft, politischen Meinung, Religion, Gesundheit oder sexuellen Orientierung.

Die Verarbeitung personenbezogener Daten ist gemäß Art. 6 Abs. 1 DSGVO nur rechtmäßig, wenn mindestens eine der dort aufgeführten Rechtsgrundlagen erfüllt ist. Diese Norm bildet den zentralen Maßstab für die datenschutzkonforme Datenverarbeitung und konkretisiert das Verbot mit Erlaubnisvorbehalt des europäischen Datenschutzrechts.[9] Die möglichen Rechtsgrundlagen reichen von der Einwilligung der betroffenen Person über die Erfüllung eines Vertrags oder rechtlicher Verpflichtungen bis hin zur Wahrung lebenswichtiger Interessen, der Wahrnehmung einer Aufgabe im öffentlichen Interesse oder der Wahrung berechtigter Interessen der Verantwortlichen oder von Dritten. Dabei sind die jeweiligen Umstände sorgfältig zu berücksichtigen, insbesondere wenn mehrere Rechtsgrundlagen gleichzeitig relevant sein können. Für die Verarbeitung personenbezogener Daten im

---

[5] Vgl. *Scheuerer*, OdW 2025, (88 f.); *Martini/Wendehorst*, KI-VO: Verordnung über Künstliche Intelligenz, Art. 2, Rn. 141-144.

[6] *Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, Was sind personenbezogene Daten?, ZENDAS Was sind personenbezogene Daten? (Datenschutz in der Hochschule).

[7] *Knecht*, Rechtsbereichsspezifische Betrachtung von KI: Grundrechte, Archiv Handreichungen bwDigiRecht - Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg.

[8] *Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024 - Künstliche Intelligenz und Datenschutz, S. 4 f., DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.

[9] *Ehmann/Selmayr*, Datenschutz-Grundverordnung, Art. 6 DSGVO, Rn. 1; Vgl. *Martini/Wendehorst*, KI-VO: Verordnung über Künstliche Intelligenz Art. 59, Rn.5, Die KI-VO greift das datenschutzrechtliche Verbotsprinzip punktuell auf (vgl. Art. 10 Abs. 5, Art. 59), ohne die DSGVO als solche zu modifizieren (Art. 2 Abs. 7); ergänzende Pflichten, etwa aus Art. 13 und 14 DSGVO, bleiben weiterhin anwendbar (vgl. Erwägungsgrund 140 S. 2).

Kontext digitaler Systeme und insbesondere bei KI-Anwendungen ist eine präzise rechtliche Bewertung unerlässlich.

### *1.1. Einwilligung*

Im datenschutzrechtlichen Kontext stellt Art. 6 Abs. 1 lit. a DSGVO die **Einwilligung** der betroffenen Person als eine mögliche rechtliche Grundlage für die Verarbeitung personenbezogener Daten dar. Damit eine solche Einwilligung wirksam ist, muss sie auf **freiwilliger Basis, informiert sowie eindeutig und spezifisch** für einen oder mehrere bestimmte Verarbeitungszwecke erfolgen.[10] Erwägungsgrund 43 zur DSGVO weist darauf hin, dass bei einem bestehenden Ungleichgewicht zwischen der betroffenen Person und dem Verantwortlichen Zweifel an der Eignung der Einwilligung als Rechtsgrundlage bestehen können. Solche Konstellationen können insbesondere dann vorliegen, wenn eine öffentliche Stelle verantwortlich ist, wie es beispielsweise bei Hochschulen der Fall ist.

Das Verhältnis zwischen Studierenden und Hochschulen ist durch eine institutionelle Hierarchie geprägt, die sich während des gesamten Studiums bemerkbar macht. Insbesondere im Prüfungszusammenhang verfügen Hochschulen aufgrund gesetzlicher Regelungen, etwa durch das Landeshochschulgesetz (LHG) oder einschlägige Prüfungsordnungen, über spezifische hoheitliche Befugnisse.[11] Eine ausführlichere Betrachtung dieser Fragestellung findet sich in der Handreichung von bwDigiRecht zum Datenschutz bei elektronischen Fernprüfungen.

Im Zuge der COVID-19-Pandemie implementierte die Hochschule Aalen ein bewertendes KI-System *Digiexam*[12], dessen Einsatz sich auf Art. 6 Abs. 1 S. 1 lit. e Abs. 3 DSGVO i.V.m. § 32a Abs. 1, Abs. 2 S. 3 Landeshochschulgesetz für Baden-Württemberg (LHG BW) stützte. Nach Auffassung der Hochschule Aalen erlaubt diese Norm die Verarbeitung personenbezogener Daten, sofern sie für die Wahrnehmung einer im **öffentlichen Interesse** liegenden Aufgabe erforderlich ist, in diesem Fall die Aufrechterhaltung des Lehrbetriebs unter pandemiebedingten Einschränkungen.[13] Zu Beginn der Nutzung erfolgte eine Verarbeitung biometrischer Gesichtsmerkmale im Sinne des Art. 9 Abs. 1 DSGVO, womit besonders

[10] *Ehmann/Selmayr*, Datenschutz-Grundverordnung, Art. 4 Rn. 50 ff.
[11] Vgl. *Dieterich*, in: Prüfungsrecht, Rn. 806.
[12] *Hochschule Aalen*, Hinweise zum Datenschutz – Einsatz von „DigiExam“ an der Hochschule Aalen, DigiExam_03-Infoschreiben.
[13] Dies geht aus der Korrespondenz zwischen der Hochschule Aalen und des LfDI BW hervor, *Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg*, Kommunikation mit Hochschule Aalen wegen „DigiExamBW“, S. 2, Kommunikation mit Hochschule Aalen wegen "DigiExamBW" - FragDenStaat.

**sensible personenbezogene Daten** betroffen waren.[14] Die entsprechende Rechtsgrundlage bildete die ausdrückliche Einwilligung der Studierenden gemäß Art. 9 Abs. 2 lit. a DSGVO. Eine Verarbeitung dieser besonderen Datenkategorie wird an der Hochschule Aalen inzwischen nicht mehr vorgenommen.[15] Bei der Auswahl der KI-Anbietenden können die Hochschulen als die für die Datenverarbeitung Verantwortlichen Einfluss auf die Modifikation der KI-Systeme nehmen, indem beispielsweise besonders schützenswerte Daten nicht verarbeitet werden und die Verarbeitung generell im Sinne der Datenminimierung begrenzt wird.[16] Es ist sicherzustellen, dass **gleichwertige alternative Lehrformate** ohne KI-Einsatz bereitgestellt werden, damit Studierende aufgrund einer Verweigerung der Einwilligung nicht benachteiligt werden.[17]

Eine Herausforderung bei der Nutzung von KI-Systemen stellt jedoch die **Dynamik** dieser Technologien dar.[18] Insbesondere bei **selbstlernenden** oder sich **entwickelnden KI-Systemen** können sich die Verarbeitungszwecke im Laufe der Nutzung verändern. Diese Problematik wirft rechtliche Fragestellungen auf, da es mitunter herausfordernd ist, sicherzustellen, dass eine einmal erteilte Einwilligung der betroffenen Person auch im Falle sich wandelnder Verarbeitungszwecke weiterhin wirksam bleibt. Die DSGVO fordert jedoch, dass die Einwilligung stets spezifisch und in informierter Weise im Hinblick auf die jeweils beabsichtigte Datenverarbeitung erfolgt und dieser entsprechen muss.[19]

### *1.2. Erfüllung eines Vertrages*

Neben der Einwilligung sieht die DSGVO in Art. 6 Abs. 1 lit. b auch die Möglichkeit vor, die Datenverarbeitung auf die Erfüllung eines Vertrages zu stützen. In Fällen, in denen KI-Technologien einen **vertraglichen Zweck** erfüllen, kann die Datenverarbeitung als vertragsbedingte Notwendigkeit

---

[14] *Hochschule Aalen*, Antwort der HS Aalen auf das Schreiben vom 23.12.2020 des LfDIs, in Anfrage „Kommunikation mit Hochschule Aalen wegen "DigiExamBW"“ - FragDenStaat.

[15] *Hochschule Aalen*, Hinweise zum Datenschutz – Einsatz von „DigiExam“ an der Hochschule Aalen, DigiExam_03-Infoschreiben.

[16] *Der Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg*, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v. 2, S. 8 ff., Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

[17] *Knecht*, Rechtsbereichsspezifische Betrachtung von KI: Grundrechte, Archiv Handreichungen bwDigiRecht - Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg.

[18] *Kopp*, Rechtsgrundlagen zur Datenverarbeitung bei KI, Rechtsgrundlagen zur Datenverarbeitung bei KI.

[19] *Der Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg*, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v. 2, S. 18 ff., Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

gerechtfertigt werden. Dabei ist jedoch zu beachten, dass sich solche Verträge nicht auf die Beziehung zwischen Studierenden und Dienstleistenden beziehen, sondern beispielsweise auf Verträge zwischen einer Hochschule und den externen Anbietenden. In diesem Fall erfolgt keine direkte Verarbeitung **personenbezogener** Daten.

### *1.3. Rechtliche Verpflichtungen*

**Art. 6 Abs. 1 lit. c DSGVO** ermöglicht die Verarbeitung personenbezogener Daten, wenn diese zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der Verantwortliche unterliegen. Dieser Erlaubnistatbestand findet im Hochschulbereich Anwendung, wenn die Datenverarbeitung auf einer spezifischen gesetzlichen Grundlage beruht, die die Hochschule zur Durchführung bestimmter Aufgaben verpflichtet.[20] Im Kontext der KI an Hochschulen kann Art. 6 Abs. 1 lit. c DSGVO etwa dann zur Anwendung kommen, wenn KI-Systeme zur Erfüllung gesetzlicher Verpflichtungen im Rahmen der **Lehre**, der **Prüfungsorganisation** oder der **Studierendenverwaltung** eingesetzt werden.[21]

### *1.4. Öffentliches Interesse*

Der Einsatz von KI in der Hochschullehre kann datenschutzrechtlich auf Art. 6 Abs. 1 lit. e DSGVO gestützt werden, sofern die Verarbeitung personenbezogener Daten zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Gemäß Art. 6 Abs. 3 DSGVO bedarf es hierfür zusätzlich einer spezifischen Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedstaaten. Im Hochschulkontext werden diese Aufgaben regelmäßig durch die jeweiligen Landeshochschulgesetze sowie hochschulinterne Ordnungen konkretisiert. So bestimmt beispielsweise § 12 Abs. 1 Landeshochschulgesetz Baden-Württemberg (LHG BW), dass personenbezogene Daten verarbeitet werden dürfen, wenn und soweit dies zur Erfüllung der gesetzlichen Aufgaben der Hochschule erforderlich ist. Zu diesen Aufgaben zählt insbesondere die Durchführung und Organisation von Lehre und Prüfungen.

Im Kontext der Hochschullehre kann der Einsatz von KI insbesondere in Form von adaptiven Lernsystemen oder intelligenten Lernplattformen erfolgen, die eine personalisierte Bereitstellung von Lerninhalten sowie eine differenzierte Analyse individueller Lernfortschritte ermöglichen. Gleiches gilt

[20] Vgl. *Der Landesbeauftragte für den Datenschutz Niedersachsen*, Hochschulen, so erlaubt § 17 des Niedersächsischen Hochschulgesetzes (NHG) die Verarbeitung personenbezogener Daten für Zwecke wie Einschreibung, Teilnahme an Lehrveranstaltungen und Prüfungen sowie Nutzung von Hochschuleinrichtungen, Hochschulen | Der Landesbeauftragte für den Datenschutz Niedersachsen.

[21] *Seckelmann/Horstmann*, Ordnung der Wissenschaft 2024, 169 (172).

für den Einsatz KI-gestützter Systeme zur Unterstützung bei der Qualitätssicherung in der Lehre, etwa durch die Analyse von Lehrveranstaltungen oder der Wirksamkeit didaktischer Konzepte. Rechtsgrundlagen hierfür ergeben sich aus hochschulrechtlichen Vorschriften zur Evaluation und Qualitätssicherung, wie etwa § 5 LHG BW. Weitere potenzielle Anwendungsbereiche KI liegen im Einsatz KI-gestützter Chatbots oder virtueller Tutoren, die Studierende im Selbststudium begleiten, individuelle Unterstützung bieten und den Zugang zu Lehrinhalten niederschwelliger gestalten. Auch diese Systeme können im Rahmen des gesetzlichen Bildungsauftrags als datenschutzrechtlich zulässig betrieben werden.

Im Bereich der Prüfungen kann KI datenschutzkonform eingesetzt werden, etwa zur automatisierten Plagiatsprüfung, zur Auswertung elektronischer Prüfungsleistungen oder im Rahmen digitaler Aufsichtsmaßnahmen. Hier stellt die Prüfungsdurchführung eine hoheitliche Aufgabe dar, deren rechtlicher Rahmen regelmäßig durch Prüfungsordnungen und hochschulrechtliche Regelungen bestimmt ist. Das öffentliche Interesse wurde exemplarisch am Fall der elektronischen Fernprüfungen in der Handreichung von bwDigiRecht zum Datenschutz bei elektronischen Fernprüfungen näher erläutert.

### *1.5. Berechtigte Interessen*

Art. 6 Abs. 1 lit. f DSGVO erlaubt die Verarbeitung personenbezogener Daten, wenn sie zur Wahrung berechtigter Interessen der Verantwortlichen oder von Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Im Gegensatz zu Art. 6 Abs. 1 lit. e DSGVO, der auf Aufgaben im öffentlichen Interesse oder hoheitliche Tätigkeiten abstellt, findet lit. f grundsätzlich **nur bei nicht-hoheitlichem Handeln** Anwendung.

Im Kernbereich hoheitlicher Tätigkeiten, etwa bei Prüfungsabwicklung, Immatrikulation oder curricularer Lehre, ist Art. 6 Abs. 1 lit. f DSGVO hingegen **nicht anwendbar**, da die Datenverarbeitung in diesem Fall auf gesetzlicher Grundlage im Sinne von Art. 6 Abs. 1 lit. e i.V.m. Art. 6 Abs. 3 DSGVO erfolgen muss. Für öffentlich-rechtlich verfasste Hochschulen scheidet Art. 6 Abs. 1 lit. f als Erlaubnistatbestand also regelmäßig aus, soweit sie im Rahmen ihrer öffentlichen Aufgaben tätig werden. [22]

[22] *Der Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg*, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v. 2, S. 21 f., Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

## 2. Grundsätze der Datenverarbeitung im Kontext der KI-Systeme

Die Integration von KI in den Hochschulbereich erfordert die präzise Beachtung datenschutzrechtlicher Bestimmungen, um die **Grundrechte der Betroffenen**, insbesondere den Schutz der Privatsphäre, zu gewährleisten.[23] Im Einklang mit der DSGVO müssen Hochschulen sicherstellen, dass bei der Nutzung von KI-Systemen auch die datenschutzrechtlichen Grundsätze konsequent eingehalten werden.[24] DSGVO legt in Art. 5 Abs. 1 zentrale Grundsätze für die Verarbeitung personenbezogener Daten fest, die als Leitlinien für jede datenschutzkonforme Datenverarbeitung gelten. Dazu zählen insbesondere die Rechtmäßigkeit, Verarbeitung nach Treu und Glauben und Transparenz (lit. a), die Zweckbindung (lit. b), die Datenminimierung (lit. c), die Richtigkeit der Daten (lit. d), die Speicherbegrenzung (lit. e) sowie die Integrität und Vertraulichkeit (lit. f). Diese Grundsätze stellen sicher, dass personenbezogene Daten nur in einem kontrollierten, nachvollziehbaren und verantwortungsvollen Rahmen genutzt werden dürfen[25] und das Fundament für die rechtmäßige Verarbeitung personenbezogener Daten von Studierenden, Lehrenden und Mitarbeitenden bilden. Verantwortliche Stellen, wie Hochschulen, müssen zudem nach Art. 5 Abs. 2 DSGVO nachweisen können, dass sie diese Prinzipien im Sinne der Rechenschaftspflicht einhalten. Insbesondere im Kontext automatisierter Datenverarbeitung durch KI-Systeme kommt der Einhaltung dieser Grundsätze eine zentrale Bedeutung zu.

### *2.1. Transparenz- und Informationspflichten*

Der datenschutzrechtliche Grundsatz der Transparenz gemäß Art. 5 Abs. 1 lit. a DSGVO ist im Zusammenhang mit dem Einsatz von KI-Systemen besonders relevant. In Verbindung mit den Informationspflichten nach Art. 12 bis 14 DSGVO ergibt sich, dass betroffene Personen, wie Studierende, Lehrende oder Mitarbeitende, grundsätzlich darüber zu informieren sind, wenn ihre personenbezogenen Daten erhoben oder anderweitig verarbeitet werden.[26] Dies gilt unabhängig davon, ob die Verarbeitung mithilfe eines KI-Systems erfolgt.

Kommt im Einzelfall ein KI-System zum Einsatz, hat dies Auswirkungen auf den **Inhalt und Umfang** der zu erteilenden Informationen. Diese Information umfasst auch die Rechtsgrundlage der

[23] *Knecht*, Rechtsbereichsspezifische Betrachtung von KI: Grundrechte, Archiv Handreichungen bwDigiRecht - Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg.
[24] Vgl. *Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, S. 8 ff., 20191106_positionspapier_kuenstliche_intelligenz.pdf.
[25] Vgl. *Ehmann/Selmayr*, Datenschutz-Grundverordnung, Art. 5 DSGVO, Rn. 5-10.
[26] Vgl. *Bayrisches Landesamt für Datenschutzaufsicht*, KI & Datenschutz, Informationspflichten, Künstliche Intelligenz.

Datenverarbeitung, den Zweck der Verarbeitung, sowie, die Logik der automatisierten Entscheidungen, die durch das KI-System getroffen werden.[27]

Die KI-Verordnung verfolgt ein abgestuftes Pflichtenprogramm, das sich nach dem Risiko des jeweiligen KI-Systems richtet.[28] So werden bestimmte KI-Anwendungen vollständig verboten, während Hochrisiko-KI-Systeme und general purpose AI (GPAI) in den Kapiteln 3 und 5 der KI-VO einem umfassenden Regelungsregime unterworfen werden. Darüber hinaus fordert Art. 50 KI-VO Transparenz von den Betreibenden und Anbietern von KI-Systemen, wobei Hochschulen als Anbietende oder Betreibende in diesem Kontext präzise Informationen zu den eingesetzten KI-Technologien zur Verfügung stellen müssen.[29] Die Informationspflichten sind unabhängig vom Risikoniveau des KI-Systems zu erfüllen. Betreibende von Hochrisiko-KI-Systemen sind darüber hinaus verpflichtet, die betroffenen Personen über die Nutzung des Systems zu informieren, was eine Transparenz im Umgang mit personenbezogenen Daten gewährleistet.[30]

Ein weiterer relevanter Aspekt beim Einsatz von Hochrisiko-KI-Systemen ist die in Art. 12 KI-VO normierte Verpflichtung zur technischen **Protokollierungsfähigkeit**. Danach müssen Hochrisiko-KI-Systeme so konzipiert und entwickelt sein, dass sie eine Aufzeichnung relevanter Vorgänge ermöglichen, insbesondere zur Nachvollziehbarkeit und Überprüfbarkeit des Systemverhaltens während der Nutzung. Es handelt sich dabei jedoch **nicht um eine allgemeine Pflicht zur durchgehenden Protokollierung aller Ereignisse**, sondern um eine **technische Voraussetzung**, die je nach Risiko- und Einsatzkontext konkretisiert werden kann.

Diese Protokollierungsfähigkeit dient der Transparenz, der Überprüfbarkeit sowie der Qualitätssicherung und kann im Einzelfall auch datenschutzrechtlich relevant sein. [31] Soweit dabei personenbezogene Daten verarbeitet werden, ist für die Zulässigkeit der Verarbeitung regelmäßig auf Art. 6 Abs. 1 lit. c DSGVO abzustellen, wenn eine rechtliche Verpflichtung zur Dokumentation besteht.[32]

---

[27] *Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024 - Künstliche Intelligenz und Datenschutz, S. 6 f., DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.
[28] *Europäische Kommission*, AI Act.
[29] *Merkle*, RDi 2024, 414 (416).
[30] Vgl. *Martini/Wendehorst*, KI-VO: Verordnung über Künstliche Intelligenz, Art. 50, Rn. 89 f.
[31] *Golland*, EuZW 2024, 846 (853).
[32] Vgl. *Ansgar/Matthias*, Formularhandbuch Datenschutzrecht, Normen der KI-VO mit Einfluss auf datenschutzrechtliche Normen.

### *2.2. Zweckbindung*

Ein weiterer zentraler datenschutzrechtlicher Grundsatz, der bei der Verarbeitung von Daten durch KI-Systeme beachtet werden muss, ist der **Grundsatz der Zweckbindung** gemäß Art. 5 Abs. 1 lit. b DSGVO. Dieser besagt, dass personenbezogene Daten nur für **klar definierte und rechtmäßige Zwecke** erhoben und verarbeitet werden dürfen.[33] Eine nachträgliche Änderung des Verarbeitungszwecks ist gemäß Art. 6 Abs. 4 DSGVO nur dann zulässig, wenn der neue Zweck mit dem ursprünglichen Zweck der Datenerhebung kompatibel ist. Dies stellt eine zusätzliche rechtliche Hürde dar, insbesondere bei der **Erweiterung von Verarbeitungszwecken** in KI-Systemen. Eine solche Erweiterung könnte die Notwendigkeit einer neuen rechtlichen Bewertung und möglicherweise einer erneuten Einwilligung der betroffenen Person zur Folge haben, um sicherzustellen, dass die ursprüngliche Zustimmung weiterhin gültig und wirksam ist.[34]

### *2.3. Datenminimierung und Speicherbegrenzung*

Besondere Aufmerksamkeit ist auch dem Grundsatz der **Datenminimierung** zu schenken. KI-Systeme müssen **datensparsam** gestaltet werden, was gemäß Art. 5 Abs. 1 lit. c DSGVO bedeutet, dass nur die **minimal erforderlichen** Daten verarbeitet werden dürfen.[35] Zudem muss die **Datensicherheit** gewährleistet sein, um unberechtigte Zugriffe auf personenbezogene Informationen zu verhindern. Hier kommt der **Pseudonymisierung** gemäß Art. 4 Nr. 5 DSGVO eine Schlüsselrolle zu: Durch die Ersetzung direkter Identifikatoren wie Namen oder Matrikelnummern durch künstliche Codes (z. B. „LE82J7“) wird der Personenbezug temporär unterbrochen, während eine spätere Re-Identifizierung mittels separater Schlüssel möglich bleibt.[36] Dies bietet eine Möglichkeit, die Risiken im Zusammenhang mit der Nutzung von KI-Systemen zu verringern.

Die **Anonymisierung** hingegen bezeichnet die Verarbeitung von Daten in einer Weise, dass der Personenbezug entfernt wird und die Daten damit dem Anwendungsbereich der DSGVO gemäß Erwägungsgrund 26 DSGVO entzieht. Eine vollständige, absolute Anonymisierung, bei der eine Re-Identifizierung für niemanden möglich ist, ist in der Praxis oft nicht umsetzbar und datenschutzrechtlich nicht zwingend erforderlich. Es ist ausreichend, wenn eine Re-Identifizierung nur mit

[33] *Ehmann/Selmayr*, Datenschutz-Grundverordnung DSGVO Art. 5, Rn. 20 ff.
[34] *Mühlhoff/Ruschemeier*, ZfDR 2024, 337 (351 f.).
[35] *Ehmann/Selmayr*, Datenschutz-Grundverordnung, DSGVO Art. 5, Rn. 29.
[36] *Der Europäische Datenschutzausschuss*, Leitlinien zur Pseudonymisierung, S. 9 f., Guidelines 01/2025 on Pseudonymisation | European Data Protection Board.

unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft möglich wäre.[37] Im Hochschulkontext ist dies insbesondere in der Forschung relevant, wo sensible Daten aggregiert oder durch Generalisierung (z. B. Ersetzung von Ortsangaben durch Regionskennungen) anonymisiert werden können.[38] Allerdings wird vor der Illusion der Anonymisierung gewarnt, da moderne KI-Methoden durch Cross-Referenzen scheinbar neutraler Datensätze häufig Re-Identifizierungen ermöglichen.[39]

Die KI-Verordnung verschärft diese Anforderungen für als hochriskant eingestufte Systeme, wie KI-gestützte Zulassungs- oder Prüfungstools: Auch bei anonymisierten Daten bleiben Transparenzpflichten gemäß Art. 50 KI-VO i.V.m. Art. 13 KI-VO bestehen. Konkret bedeutet dies, dass Hochschulen selbst bei anonymisierter Datennutzung dokumentieren müssen, wie sie Risiken wie algorithmische Verzerrungen minimieren und Betroffenenrechte gewährleisten. Für pseudonymisierte Daten gelten zudem die Grundsätze der Datenminimierung und Speicherbegrenzung, beispielsweise durch automatisierten Löschprozess für Schlüsseldateien nach Abschluss des Verarbeitungszwecks.[40] Ein praktisches Beispiel liefern chatbotbasierte Studienberatungssysteme: Werden diese mit pseudonymisierten Nutzungsdaten trainiert, muss die Hochschule sicherstellen, dass Logs mit Interaktionsverläufen standardmäßig ohne personenbezogene Metadaten (z. B. IP-Adressen) gespeichert und Zugriffe auf Schlüsseldateien streng kontrolliert werden.[41] Gleichzeitig sind Betroffene über die Verarbeitungsschritte zu informieren, einschließlich des Hinweises auf das Widerspruchsrecht nach Art. 21 DSGVO.

### *2.4. Datenrichtigkeit*

Im Kontext der KI-Nutzung gewinnt auch das Gebot der **Datenrichtigkeit** nach Art. 5 Abs. 1 lit. d DSGVO an Bedeutung, wonach unrichtige Daten unverzüglich berichtigt oder gelöscht werden müssen. Der **Berichtigungsanspruch** der betroffenen Person nach Art. 16 DSGVO steht hier in direkter Wechselwirkung mit der Funktionsweise von KI-Systemen, insbesondere im Bereich von Large Language Models.[42] Diese Systeme neigen dazu, aufgrund der probabilistischen Natur ihrer Datenverarbeitung

[37] *Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit*, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, S. 3 f., Positionspapier-Anonymisierung.pdf.
[38] *Radboud Universiteit*, Anonymising and pseudonymising, Anonymising and pseudonymising | Radboud University.
[39] *International Association of Privacy Professionals*, The myth of anonymization: Why AI needs a new privacy paradigm, The myth of anonymization: Why AI needs a new privacy paradigm | IAPP.
[40] Vgl. *bitkom*, Umsetzungsleitfaden zur KI-Verordnung, S. 93 ff., bitkom-umsetzungsleitfaden-ki.pdf.
[41] *Bundesamt für Sicherheit in der Informationstechnik*, Whitepaper Transparenz von KI-Systemen, S. 12 ff., BSI - Presse - BSI veröffentlicht Whitepaper zur Transparenz von KI-Systemen.
[42] *Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit*, Checkliste zum Einsatz LLM-basierter Chatbots, S. 4, Dokumentvorlage zur einheitlichen Gestaltung.

auch fehlerhafte oder unzutreffende Informationen zu generieren, was das Risiko von **Halluzinationen** verstärken kann – einem statistischen Nebenprodukt bei generativen Modellen.[43] Unter Halluzinationen versteht man in diesem Zusammenhang die Erzeugung von scheinbar plausiblen, inhaltlich aber objektiv falschen Aussagen durch KI-Systeme, ohne dass ein Bezug zu realen Daten oder Fakten besteht.[44] Derartige systemische Fehler stellen eine Herausforderung für die Umsetzung des Datenrichtigkeitsgebots dar, da die generierten Daten inhaltlich oftmals als korrekt wahrgenommen werden, obwohl sie auf fehlerhaften Annahmen basieren.[45]

Besondere datenschutzrechtliche Pflichten treffen die Anbietende von Hochrisiko-KI-Systemen. Systeme, die häufig biometrische Daten verarbeiten oder in besonders sensiblen Kontexten wie der Auswahl von Studierenden und Lehrpersonen zum Einsatz kommen, unterliegen besonderen datenschutzrechtlichen Anforderungen. .[46] Die **Data Governance**-Vorschriften nach Art. 10 KI-VO haben insbesondere die Qualität der Datenverwaltung und der Daten zu gewährleisten, die für das Training und die Validierung von Hochrisiko-KI-Systemen verwendet werden. Die Nutzung sensibler Daten zur Erkennung und Korrektur von Verzerrungen in den Trainingsdatensätzen wird unter bestimmten Bedingungen zugelassen, wobei Art. 9 Abs. 2 lit. g DSGVO i.V.m. mit nationalem Recht als Grundlage für die Verarbeitung dient, wenn ein erhebliches öffentliches Interesse an der Wahrung der Grundrechte besteht.[47]

Die Vorschriften zur **menschlichen Aufsicht** über den Einsatz von Hochrisiko-KI gemäß Art. 14 KI-VO fordern, dass natürliche Personen in der Lage sein müssen, das System zu überwachen und bei Bedarf stillzulegen oder fehlerhafte Ausgaben zu korrigieren.[48] Diese Regelung zielt darauf ab, die Entscheidungsmacht des Menschen zu wahren und ermöglicht eine Überprüfung von KI-basierten Ergebnissen. Dies steht im Einklang mit den Vorgaben der DSGVO, die insbesondere bei automatisierten Entscheidungen eine menschliche Aufsicht verlangen kann, um eine datenschutzkonforme Verarbeitung gemäß Art. 22 DSGVO sicherzustellen.[49]

---

[43] *Bayrisches Landesamt für Datenschutzaufsicht*, KI & Datenschutz, Künstliche Intelligenz.
[44] *Özer*, Is Artifical Intelligence Hallucinating?, S. 333, Is Artifical Intelligence Hallucinating? - PMC.
[45] *Scheuerer*, OdW 2025, (88).
[46] Vgl. *Simitis u. a.*, Datenschutzrecht DS-GVO/BDSG, Art. 9 DSGVO.
[47] *Martini/Wendehorst*, KI-VO: Verordnung über Künstliche Intelligenz, Art. 2, Rn. 143; *Kühling/Buchner*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Art. 9, Rn. 88-91a.
[48] *Borges*, Potenziale von künstlicher Intelligenz mit Blick auf das Datenschutzrecht, S. 29.
[49] *Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024 - Künstliche Intelligenz und Datenschutz, S. 5, Rn. 12., DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.

### 3. Automatisierte Entscheidungen

Eine besonders komplexe Herausforderung stellen **automatisierte Entscheidungsprozesse** dar, die beispielsweise bei der **Bewertung von Studienleistungen** oder der **Bewerbungsauswahl** zum Einsatz kommen. Artikel 22 DSGVO verbietet grundsätzlich automatisierte Entscheidungen, die rechtliche oder ähnlich schwerwiegende Auswirkungen auf betroffene Personen haben, es sei denn, diese basieren auf einer ausdrücklichen Einwilligung, sind für die Erfüllung eines Vertrags erforderlich oder gesetzlich zulässig (Art. 22 Abs. 2 DSGVO).[50]

Im Hochschulkontext betrifft dies beispielsweise automatisierte Zulassungsverfahren zu einem Studiengang, die auf algorithmischen Auswahlkriterien beruhen, oder KI-gestützte Bewertungssysteme für Prüfungsleistungen. Entscheidend ist, ob die automatisierte Verarbeitung zu einer **abschließenden Entscheidung** führt, die ohne menschliches Ermessen getroffen wird.[51] Beispielsweise würde ein System, das Bewerbende allein anhand eines Scores aussortiert, unter Art. 22 DSGVO fallen, sofern kein ausreichender Entscheidungsspielraum einer natürlichen Person besteht.[52] Der Europäische Gerichtshof (EuGH) hat in seiner Schufa-Entscheidung[53] klargestellt, dass bereits die Erstellung eines algorithmischen Scores als automatisierte Entscheidung gilt, wenn Dritte diesen maßgeblich nutzen, ohne eigene Prüfung vorzunehmen.[54] Übertragen auf Hochschulen bedeutet dies: Wird ein Bewertungstool eingesetzt, das Studierenden automatisch Noten zuweist und diese ohne kritische Überprüfung durch Lehrende übernommen werden, liegt eine verbotene automatisierte Entscheidung vor.[55]

Hochschulen müssen sicherstellen, dass automatisierte Prozesse stets eine echte menschliche Intervention beinhalten.[56] Dies erfordert, dass verantwortliche Personen (z.B. Prüfungsausschüsse) die algorithmischen Ergebnisse aktiv bewerten und gegebenenfalls korrigieren sollen. Zudem sind Betroffene umfassend über die verwendeten Kriterien, die involvierte Logik und die Tragweite der Entscheidung zu informieren (Art. 13 Abs. 2 lit. f DSGVO).[57] Im Falle von Profiling, etwa bei der Analyse

---

[50] Vgl. *Ehmann/Selmayr*, Datenschutz-Grundverordnung DSGVO, Art. 22, Rn. 6, Rn. 17, 18, Rn. 19.
[51] *Härting*, Rechtliche Rahmenbedingungen des Profilings gemäß der DSGVO, Rechtliche Rahmenbedingungen des Profilings gemäß der DSGVO.
[52] *TÜV Süd*, Automatisierte Einzelentscheidungen, Automatisierte Entscheidung im Einzelfall einschließlich Profiling.
[53] EuGH, v. 07.12.2023 - C-634/21.
[54] *Foitzick*, KI bei (automatisierten) Entscheidungen, KI bei (automatisierten) Entscheidungen.
[55] *Schütt*, Wie die Notengebung durch die Künstliche Intelligenz gerechter werden kann, Campus Schulmanagement - Gerechtere Notengebung durch KI.
[56] *Stingl*, EuGH stuft Schufa-Score als automatische Entscheidungsfindung ein – Auswirkungen auch auf KI-Anwendugen, Aktuelles - Universität Regensburg.
[57] *Stingl*, EuGH stuft Schufa-Score als automatische Entscheidungsfindung ein – Auswirkungen auch auf KI-Anwendugen, Aktuelles - Universität Regensburg.

von Lernverhalten zur individuellen Studiengestaltung, ist zusätzlich eine Datenschutz-Folgeabschätzung nach Art. 35 Abs. 3 lit. a DSGVO durchzuführen.

Die DSGVO verpflichtet Hochschulen, Verfahren zu etablieren, die Betroffenen ein effektives Widerspruchsrecht (Art. 21 DSGVO) und die Möglichkeit zur Anfechtung automatisierter Entscheidungen bieten.[58] Dies umfasst nicht nur die Überprüfung durch eine natürliche Person, sondern auch die Darlegung des eigenen Standpunktes (Art. 22 Abs. 3 DSGVO).[59] Beispielhaft könnten Studierende fordern, dass eine KI-generierte Prüfungsbewertung durch Lehrende neu bewertet wird, wobei die zugrundeliegenden Daten und Algorithmen offengelegt werden müssen.[60]

### 4. Drittlandtransfer

Der Einsatz von KI in der Hochschullehre nimmt rasant zu; sei es zur automatisierten Leistungsdiagnostik, in adaptiven Lernplattformen oder bei der Unterstützung administrativer Abläufe.[61] Damit gehen jedoch erhebliche datenschutzrechtliche Anforderungen einher, insbesondere wenn personenbezogene Daten, einschließlich besonders sensibler Informationen nach Art. 9 DSGVO, in sogenannte Drittländer übermittelt werden, also in Staaten außerhalb des Europäischen Wirtschaftsraums (EWR), die keinen Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO aufweisen.

Ein aktuelles Beispiel stellt das chinesische KI-Unternehmen *DeepSeek* dar. Die Datenschutzbehörden mehrerer Bundesländer haben inzwischen koordinierte Prüfverfahren gegen DeepSeek eingeleitet.[62] Kritisiert werden unter anderem die fehlende EU-Vertretung (Art. 27 DSGVO), die Datenspeicherung in China sowie das Fehlen einer Opt-out-Möglichkeit für Nutzende der ein Verstoß gegen Transparenz- und Rechenschaftspflichten darstellt. Besonders gravierend ist die Problematik, wenn durch technische

[58] *Schwartmann/Hermann*, Was Hochschulen beim Datenschutz beachten müssen, EU-Gesetzgebung: Was Hochschulen beim Datenschutz beachten müssen.
[59] *Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit*, Automatisierte Entscheidungen dürfen keine maßgebliche Rolle spielen, Auswirkungen des Schufa-Urteils auf KI-Anwendungen | HmbBfDI.
[60] Vgl. *Heckmann/Rahut*, OdW 2024, 85 (98).
[61] *Muscanell/Gay*, 2025 Students and Technology Report: Shaping the Future of Higher Education Through Technology, Flexibility, and Well-Being, https://www.educause.edu/content/2025/students-and-technology-report#GenerativeAIintheClassroom.
[62] *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, Prüfverfahren gegen DeepSeek eingeleitet, Prüfverfahren gegen DeepSeek eingeleitet | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

Mängel (z. B. Jailbreaks, Tastatureingabeaufzeichnung)[63] die Integrität und Vertraulichkeit der Verarbeitung nach Art. 5 Abs. 1 lit. f DSGVO verletzt wird.[64]

Hochschulen in Sachsen wurden vor dem Einsatz dieser Systeme gewarnt, insbesondere wenn Studierende oder Lehrende ohne ausreichende Aufklärung personenbezogene Daten übermitteln.[65] Auch in Italien hat die Datenschutzbehörde (*Garante per la protezione dei dati personali*) bereits Beschränkungen gegen DeepSeek erlassen, ein möglicher Präzedenzfall für weitere Maßnahmen in der EU.[66]

Etwas anders gestaltet sich die Lage bei Transfers in die USA. Mit dem im Jahr 2023 in Kraft getretenen *EU–US Data Privacy Framework* liegt derzeit ein Angemessenheitsbeschluss gemäß Art. 45 DSGVO vor, auf dessen Grundlage Datenübermittlungen an zertifizierte US-Unternehmen rechtmäßig erfolgen können. [67] Dies wurde jüngst auch durch das Oberlandesgericht (OLG) Köln bestätigt, dass die Wirksamkeit des Abkommens,im Gegensatz zum früheren Privacy Shield nicht in Zweifel zog. [68] Gleichwohl bestehen Vorbehalte: Der Kläger des wegweisenden *Schrems II*-Urteils, Maximilian Schrems, kündigte bereits rechtliche Schritte gegen das neue Abkommen an.[69]

Ein Drittlandtransfer liegt nicht nur bei physischer Datenspeicherung im Ausland vor, sondern bereits dann, wenn etwa Wartung, Fernzugriff oder Support durch Anbietende aus einem Drittland erfolgen. Hochschulen, die entsprechende KI-Systeme in Lehre oder Forschung einsetzen, müssen daher sorgfältig prüfen, ob geeignete Garantien gemäß Art. 46 DSGVO vorliegen und ob der Einsatz überhaupt zulässig ist. Dies bedeutet für die Hochschullehre, dass KI-gestützte Sprachmodelle, Übersetzungstools oder

[63] *datenschutzticker.de*, KI aus Nicht-EU-Staaten: DSGVO-Prüfverfahren und Sicherheitsrisiken bei DeepSeek, DSGVO-Prüfverfahren und Sicherheitsrisiken bei DeepSeek datenschutzticker.de.
[64] *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, Prüfverfahren gegen DeepSeek eingeleitet, Prüfverfahren gegen DeepSeek eingeleitet | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.
[65] Vgl. *Sächsische Datenschutz- und Transparenzbeauftragte*, Empfehlungen der SDTB zu DeepSeek und anderen KI-Anwendungen ohne gesetzlichen Vertreter in der EU, Empfehlungen der SDTB zu DeepSeek und anderen KI-Anwendungen ohne gesetzlichen Vertreter in der EU.
[66] *Garante per la protezione dei dati personali*, Artificial Intelligence: The Italian Data Protection Authority blocks DeepSeek, COMUNICATO STAMPA - Intelligenza artificiale: il Garante privacy blocca... - Garante Privacy.
[67] Vgl. *Zeitschrift für Datenschutz*, ZD 2024, 222 (222), Rn. 81.
[68] *Zeitschrift für Datenschutz*, ZD 2024, 222 (222), Rn. 81.
[69] Vgl. *Open Source Business Alliance – Bundesverband für digitale Souveränität e.V.*, Der transatlantische Datenschutz bleibt ein Problem – Kommt jetzt Schrems III?, Der transatlantische Datenschutz bleibt ein Problem - Kommt jetzt Schrems III? | OSBA – Open Source Business Alliance.

Analyseplattformen nur dann eingesetzt werden dürfen, wenn alle datenschutz- und KI-rechtlichen Voraussetzungen erfüllt sind – eine rein technische Betrachtung greift hier zu kurz.[70]

Um den datenschutzrechtlichen Anforderungen beim Einsatz von KI-Systemen in der Hochschullehre gerecht zu werden, insbesondere bei Drittlandtransfers und der Verarbeitung sensibler Daten, müssen Hochschulen eine Reihe organisatorischer und technischer Maßnahmen ergreifen. Zunächst ist bei Anwendungen mit einem erhöhten Risiko – etwa aufgrund von Drittlandbezug oder dem Umgang mit besonderen Kategorien personenbezogener Daten, regelmäßig eine Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO durchzuführen. Diese dient der frühzeitigen Risikoerkennung und der Definition geeigneter Schutzmaßnahmen.[71]

Soweit möglich, sollten vorrangig Anbietende mit Sitz oder Datenverarbeitung innerhalb des EWR ausgewählt werden. Sofern dies nicht umsetzbar ist und kein Angemessenheitsbeschluss vorliegt, müssen vertragliche Garantien, wie Standardvertragsklauseln, sowie zusätzliche technische Sicherungsmaßnahmen, darunter starke Verschlüsselung und Zugriffsbeschränkungen, implementiert werden, um ein angemessenes Datenschutzniveau zu gewährleisten.[72]

Zugleich sind Hochschulen verpflichtet, Transparenz herzustellen: Lehrende und Studierende müssen klar und verständlich über die Art der Datenverarbeitung, mögliche Übermittlungen in Drittländer sowie ihre Rechte als Betroffene informiert werden.[73] Schließlich sollte die Auswahl der eingesetzten Softwarelösungen datensouverän erfolgen; das heißt, sie sollten so gestaltet sein, dass Datenschutzaspekte bereits in der Konzeption (Privacy by Design) und als Voreinstellung (Privacy by Default) umfassend berücksichtigt werden.[74]

Die Seite des LfDI Baden-Württemberg gibt konkrete Empfehlungen zum Umgang mit KI-Anwendungen von Anbietenden außerhalb der EU ohne benannten Vertretenden. Sie betont Risiken für den

---

[70] Vgl. *Universität Osnabrück*, Handlungsempfehlungen zum Umgang mit KI-basierten Anwendungen, Handlungsempfehlungen zum Umgang mit KI-basierten Anwendungen: virtUOS | Zentrum für Digitale Lehre, Campus-Management und Hochschuldidaktik.

[71] Vgl. *Bayrisches Landesamt für Datenschutzaufsicht*, Datenschutzkonforme Künstliche Intelligenz Checkliste mit Prüfkriterien nach DS-GVO, S. 7, Checkliste KI.

[72] *Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz*, Geeignete Garantien bei der Datenübermittlung in Drittländer, Geeignete Garantien bei der Datenübermittlung in Drittländer | datenschutz.rlp.de.

[73] *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, Empfehlungen zum Einsatz von KI-Anwendungen von Anbietern außerhalb der Europäischen Union, die keinen gesetzlichen Vertreter in der EU benannt haben, Empfehlungen zum Einsatz von KI-Anwendungen von Anbietern außerhalb der Europäischen Union, die keinen gesetzlichen Vertreter in der EU benannt haben | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

[74] *Wilmer*, BvD 2024.

Datenschutz, fordert technische Schutzmaßnahmen, Sensibilisierung der Nutzenden und verweist auf zentrale Dokumente wie die KI-Checkliste und die DSGVO. Der Fokus liegt auf Transparenz, Datenminimierung und Einhaltung der Betroffenenrechte.[75]

## 5. Datenschutz-Folgenabschätzung

Die Verwendung von KI in verschiedenen Anwendungsbereichen, insbesondere auch im Hochschulkontext, stellt eine potenzielle Gefahr für die Rechte und Freiheiten betroffener Personen dar. In Anbetracht der potenziellen Risiken, die durch den Einsatz von KI entstehen können, verpflichtet DSGVO den Verantwortlichen gemäß Art. 35 Abs. 1 Satz 1 DSGVO dazu, eine **DSFA** durchzuführen, sofern die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.[76] Diese stellt eine **systematische Prüfung** dar, die durch den Verantwortlichen durchgeführt werden muss, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.[77]

Im Hochschulkontext, in dem KI zur Verarbeitung von personenbezogenen Daten, etwa für Lern- und Bewertungsprozesse, eingesetzt wird, gewinnt die Durchführung einer DSFA besondere Bedeutung.[78] Betreibende von **Hochrisiko-KI-Systemen** sind nach der KI-Verordnung, insbesondere gemäß Art. 26 Abs. 9 KI-VO, verpflichtet, die bereitgestellten Informationen zu verwenden, um eine DSFA vorzunehmen. Diese Informationen müssen gemäß Art. 13 KI-VO als Teil der Betriebsanleitung des KI-Systems zur Verfügung gestellt werden. Es wird erwartet, dass diese Informationen alle relevanten Aspekte der KI-Verarbeitung abdecken, um eine fundierte und gründliche Bewertung der Datenschutzrisiken vor der Inbetriebnahme der Systeme zu ermöglichen.[79]

Zusätzlich zur DSFA sieht die KI-Verordnung vor, dass vor der Inbetriebnahme bestimmter Hochrisiko-KI-Systeme eine **Grundrechte-Folgenabschätzung (GRFA)** durchzuführen ist, wie in Art. 27 KI-VO

---

[75] *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, Empfehlungen zum Einsatz von KI-Anwendungen von Anbietern außerhalb der Europäischen Union, die keinen gesetzlichen Vertreter in der EU benannt haben, Empfehlungen zum Einsatz von KI-Anwendungen von Anbietern außerhalb der Europäischen Union, die keinen gesetzlichen Vertreter in der EU benannt haben | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

[76] *Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024 - Künstliche Intelligenz und Datenschutz, S. 10, Rn. 39, DSK_Orientierungshilfe_KI_und_Datenschutz.pdf.

[77] *Bayrisches Landesamt für Datenschutzaufsicht*, KI & Datenschutz, Datenschutzfolgenabschätzung, Künstliche Intelligenz.

[78] *Rätze*, Datenschutzfolgenabschätzung und künstliche Intelligenz, Datenschutzfolgenabschätzung und künstliche Intelligenz.

[79] *Europäische Kommission*, Künstliche Intelligenz – Fragen und Antworten, S. 6 f., QANDA_21_1683_DE.pdf.

festgelegt. In diesem Verfahren wird evaluiert, welche Auswirkungen die Nutzung des KI-Systems auf die Grundrechte der betroffenen Personen haben könnte.[80] Es ist jedoch zu beachten, dass die Pflichten aus der GRFA in bestimmten Fällen ganz oder teilweise entfallen können, wenn diese gem. Art. 27 Abs.4 KI-VO bereits im Rahmen der DSFA berücksichtigt wurden.[81] Das bedeutet, dass eine gründliche DSFA die Notwendigkeit einer separaten GRFA möglicherweise reduziert, sofern beide Verfahren überlappende Anforderungen abdecken.[82]

## 6. Fazit und Ausblick

Die vorliegende Handreichung verdeutlicht, dass der Einsatz von Künstlicher Intelligenz im Hochschulkontext mit erheblichen datenschutzrechtlichen Anforderungen einhergeht, die sich nicht nur aus der DSGVO, sondern zunehmend auch aus der KI-Verordnung ergeben. Die Verarbeitung personenbezogener Daten durch KI-Systeme ist nur dann zulässig, wenn eine der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen vorliegt. Im Hochschulkontext sind insbesondere die Erfüllung gesetzlicher Verpflichtungen sowie Aufgaben im öffentlichen Interesse relevant.

Die Prinzipien der Datenminimierung, Transparenz und Zweckbindung sind von großer Bedeutung. Hochschulen müssen sicherstellen, dass Studierende, Lehrende und Mitarbeitende umfassend über die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz von KI-Systemen informiert werden, insbesondere über die Zwecke, Rechtsgrundlagen sowie die Logik automatisierter Entscheidungen.

Außerdem wird die Notwendigkeit betont, KI-Systeme datensparsam zu gestalten und, wo möglich, auf Pseudonymisierung oder Anonymisierung zurückzugreifen. Die Protokollierung und Dokumentation der Datenverarbeitung, insbesondere bei Hochrisiko-KI-Systemen, ist verpflichtend und dient sowohl der Transparenz als auch der Qualitätssicherung.

Die rasante Entwicklung von KI-Technologien wird auch in Zukunft neue datenschutzrechtliche Fragen aufwerfen. Es ist davon auszugehen, dass sowohl die Rechtsprechung als auch der Gesetzgeber auch künftig in verstärktem Maße gefordert sein werden, um klare und rechtssichere Rahmenbedingungen für den Einsatz von KI zu entwickeln und fortlaufend an technologische Entwicklungen anzupassen.

[80] *Europäische Kommission*, Künstliche Intelligenz – Fragen und Antworten, S. 6 f., QANDA_21_1683_DE.pdf.
[81] *Punie*, The GDPR and the AI Act: A Harmonized Yet Complex Regulatory Landscape, GDPR and AI Act: A Harmonized Yet Complex Regulatory Landscape.
[82] *Knecht*, Zusammenfassung der KI-Verordnung für den Kontext der Hochschullehre, S. 19, Archiv Handreichungen bwDigiRecht - Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg.

Insbesondere die Fragen nach der Verantwortlichkeit der internationalen Datenübermittlung und der Anpassung bestehender Datenschutzkonzepte an sich ständig weiterentwickelnde KI-Technologien werden zentrale Themen bleiben. Hochschulen und andere Institutionen werden ihre Datenschutzkonzepte kontinuierlich überprüfen und anpassen müssen, um den rechtlichen Anforderungen gerecht zu werden und gleichzeitig die Potenziale von KI-Systemen nutzen zu können. Die Entwicklung von Best Practices und branchenspezifischen Leitlinien wird dabei eine wichtige Rolle spielen, um Rechtssicherheit zu schaffen und den verantwortungsvollen Einsatz von KI zu fördern.[83]

[83] Einen fundierten Überblick über die datenschutzrechtlichen Fragestellungen im Kontext des Einsatzes von KI, einschließlich einer praxisorientierten Check-Liste, liefert das Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ des Landesbeauftragten für Datenschutz und die Informationsfreiheit in Baden-Württemberg vom 17.10.2024.

## 7. Literaturverzeichnis

*Ansgar, Koreng / Matthias, Lachenmann*, Formularhandbuch Datenschutzrecht, 4. Auflage, München 2025

*Bayrisches Landesamt für Datenschutzaufsicht*, Datenschutzkonforme Künstliche Intelligenz Checkliste mit Prüfkriterien nach DS-GVO, 2024, Künstliche Intelligenz

*Bayrisches Landesamt für Datenschutzaufsicht*, KI & Datenschutz, BayLDA, Künstliche Intelligenz

*bitkom*, Umsetzungsleitfaden zur KI-Verordnung, 2024, 1–220, bitkom-umsetzungsleitfaden-ki.pdf

*Borges, Georg*, Potenziale von künstlicher Intelligenz mit Blick auf das Datenschutzrecht, 2021, 1–60, Stiftung-Datenschutz_Gutachten-Georg-Borges-Potenziale-Kuenstliche-Intelligenz-Datenschutzrecht-2021-12.pdf

*Bundesamt für Sicherheit in der Informationstechnik*, Whitepaper Transparenz von KI-Systemen, 2024, BSI - Presse - BSI veröffentlicht Whitepaper zur Transparenz von KI-Systemen

*Datenschutzkonferenz*, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 2019, 20191106_positionspapier_kuenstliche_intelligenz.pdf

*datenschutzticker.de*, KI aus Nicht-EU-Staaten: DSGVO-Prüfverfahren und Sicherheitsrisiken bei DeepSeek, https://www.datenschutzticker.de/2025/03/ki-aus-nicht-eu-staaten-dsgvo-pruefverfahren-und-sicherheitsrisiken-bei-deepseek/ 2025, DSGVO-Prüfverfahren und Sicherheitsrisiken bei DeepSeek datenschutzticker.de

*Der Bundesbeauftragte für den Datenschutz und die Informationssicherheit*, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2020, Positionspapier-Anonymisierung.pdf

*Der Europäische Datenschutzausschuss*, Leitlinien zur Pseudonymisierung, 2025, Guidelines 01/2025 on Pseudonymisation | European Data Protection Board

*Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit*, Checkliste zum Einsatz LLM-basierter Chatbots, 2023, Dokumentvorlage zur einheitlichen Gestaltung

*Der Hamburgische Beauftragte für Datenschutz und Informationssicherheit*, Automatisierte Entscheidungen dürfen keine maßgebliche Rolle spielen, 2023, Auswirkungen des Schufa-Urteils auf KI-Anwendungen | HmbBfDI

*Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, Prüfverfahren gegen DeepSeek eingeleitet, Pressestelle 2025, Prüfverfahren gegen DeepSeek eingeleitet | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

*Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, Empfehlungen zum Einsatz von KI-Anwendungen von Anbietern außerhalb der Europäischen Union, die keinen gesetzlichen Vertreter in der EU benannt haben, Empfehlungen zum Einsatz von KI-Anwendungen von Anbietern außerhalb der Europäischen Union, die keinen gesetzlichen Vertreter in der EU benannt haben | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

*Der Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg*, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v. 2,

2024, Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz | Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

*Der Landesbeauftragte für den Datenschutz Niedersachsen*, Hochschulen, Hochschulen | Der Landesbeauftragte für den Datenschutz Niedersachsen

*Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg*, Kommunikation mit Hochschule Aalen wegen „DigiExamBW“, FragDenStaat 2021, Kommunikation mit Hochschule Aalen wegen "DigiExamBW" - FragDenStaat

*Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz*, Geeignete Garantien bei der Datenübermittlung in Drittländer, Geeignete Garantien bei der Datenübermittlung in Drittländer | datenschutz.rlp.de

*Dieterich, Peter*, Prozessrechtliche Fragen, in: *Fischer, Edgar / Jeremias, Christoph / Dieterich, Peter (Hrsg.)*, Prüfungsrecht, 8, München 2022

*Ehmann, Eugen / Selmayr, Martin*, Datenschutz-Grundverordnung, 3. Auflage, 2024

*EuGH*, Urteil vom 07.12.2023 - C-634/21, 2023,

*Europäische Kommission*, Künstliche Intelligenz – Fragen und Antworten, 2024, 1–11, QANDA_21_1683_DE.pdf

*Europäische Kommission*, AI Act, 2025,

*Foitzick, Klaus*, KI bei (automatisierten) Entscheidungen, activeMind.legal 2024, KI bei (automatisierten) Entscheidungen

*Garante per la protezione dei dati personali*, Artificial Intelligence: The Italian Data Protection Authority blocks DeepSeek, 2025, COMUNICATO STAMPA - Intelligenza artificiale: il Garante privacy blocca... - Garante Privacy

*Golland, Alexander*, KI und KI-Verordnung aus datenschutzrechtlicher Sicht, EuZW 2024, 846–854

*Härting, Niko*, Rechtliche Rahmenbedingungen des Profilings gemäß der DSGVO, ottoschmidt 2025, Rechtliche Rahmenbedingungen des Profilings gemäß der DSGVO

*Heckmann, Dirk / Rahut, Sarah*, Rechtssichere Hochschulprüfungen mit und trotz generativer KI, OdW 2024, 85–100

*Hochschule Aalen*, Antwort der HS Aalen auf das Schreiben vom 23.12.2020 des LfDIs, 2021, in Anfrage „Kommunikation mit Hochschule Aalen wegen "DigiExamBW"“ - FragDenStaat

*Hochschule Aalen*, Hinweise zum Datenschutz – Einsatz von „DigiExam“ an der Hochschule Aalen, 2021, DigiExam 03-Infoschreiben

*International Association of Privacy Professionals*, The myth of anonymization: Why AI needs a new privacy paradigm, AI News 2025, The myth of anonymization: Why AI needs a new privacy paradigm | IAPP

*Knecht, Jana*, Zusammenfassung der KI-Verordnung für den Kontext der Hochschullehre, 2025, 1–24, Archiv Handreichungen bwDigiRecht - Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg

*Knecht, Jana*, Rechtsbereichsspezifische Betrachtung von KI: Grundrechte, 2025, 1–17, Archiv Handreichungen bwDigiRecht - Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg

*Konferenz der unabhängigen Datenschutzaufsichtsbehörden*, Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024 - Künstliche Intelligenz und Datenschutz, 2024, DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

*Kopp, Nicole*, Rechtsgrundlagen zur Datenverarbeitung bei KI, activeMind.legal 2024, Rechtsgrundlagen zur Datenverarbeitung bei KI

*Kühling, Jürgen / Buchner, Benedikt*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, 4. Auflage

*Martini, Mario / Wendehorst, Christine*, KI-VO: Verordnung über Künstliche Intelligenz, 2024

*Merkle, Marieke Luise*, Transparenz nach der KI-Verordnung – von der Blackbox zum Open-Book?, RDi 2024, 414–421

*Mühlhoff, Rainer / Ruschemeier, Hannah*, KI-Regulierung durch Zweckbindung für Modelle, ZfDR 2024, 337–361

*Muscanell, Nicole / Gay, Kristen*, 2025 Students and Technology Report: Shaping the Future of Higher Education Through Technology, Flexibility, and Well-Being, EDUCAUSE 2025, https://www.educause.edu/content/2025/students-and-technology-report#GenerativeAIintheClassroom

*Open Source Business Alliance – Bundesverband für digitale Souveränität e.V.*, Der transatlantische Datenschutz bleibt ein Problem – Kommt jetzt Schrems III?, 2024, Der transatlantische Datenschutz bleibt ein Problem - Kommt jetzt Schrems III? | OSBA – Open Source Business Alliance

*Özer, Mahmut*, Is Artifical Intelligence Hallucinating?, 2024, Is Artifical Intelligence Hallucinating? - PMC

*Punie, Manon*, The GDPR and the AI Act: A Harmonized Yet Complex Regulatory Landscape, Datenschutznotizen 2025, GDPR and AI Act: A Harmonized Yet Complex Regulatory Landscape

*Radboud Universiteit*, Anonymising and pseudonymising, Anonymising and pseudonymising | Radboud University

*Rätze, Michael*, Datenschutzfolgenabschätzung und künstliche Intelligenz, Mittelstand-Digital Zentrum Chemnitz, Datenschutzfolgenabschätzung und künstliche Intelligenz

*Sächsische Datenschutz- und Transparenzbeauftragte*, Empfehlungen der SDTB zu DeepSeek und anderen KI-Anwendungen ohne gesetzlichen Vertreter in der EU, 2025, Empfehlungen der SDTB zu DeepSeek und anderen KI-Anwendungen ohne gesetzlichen Vertreter in der EU

*Scheuerer, Martin*, Datenschutz, KI und Forschungsprivileg?, OdW 2025

*Schütt, Sven*, Wie die Notengebung durch die Künstliche Intelligenz gerechter werden kann, Campus Schulmanagement 2025, Campus Schulmanagement - Gerechtere Notengebung durch KI

*Schwartmann, Rolf / Hermann, Maximilian*, Was Hochschulen beim Datenschutz beachten müssen, Forschung & Lehre 2018, EU-Gesetzgebung: Was Hochschulen beim Datenschutz beachten müssen

*Seckelmann, Margrit / Horstmann, Jan*, Künstliche Intelligenz im Hochschulbereich und Datenschutz, Ordnung der Wissenschaft 2024, 169–183

*Simitis, Spiros / Hornung, Gerrit / Spiecker, Indra*, Datenschutzrecht DS-GVO/BDSG, 2. Auflage, 2025

*Stingl, Susanne*, EuGH stuft Schufa-Score als automatische Entscheidungsfindung ein – Auswirkungen auch auf KI-Anwendugen, 2023, Aktuelles - Universität Regensburg

*TÜV Süd*, Automatisierte Einzelentscheidungen, Automatisierte Entscheidung im Einzelfall einschließlich Profiling

*Universität Osnabrück*, Handlungsempfehlungen zum Umgang mit KI-basierten Anwendungen, virtUOS | Zentrum für Digitale Lehre, Campus-Management und Hochschuldidaktik, Handlungsempfehlungen zum Umgang mit KI-basierten Anwendungen: virtUOS | Zentrum für Digitale Lehre, Campus-Management und Hochschuldidaktik

*Wilmer, Thomas*, KI-Verordnung: Datenschutzrechtliche Herausforderungen, BvD 2024

*Zeitschrift für Datenschutz*, Drittlanddatentransfer nach EU-US Data Privacy Framework, ZD 2024, 222–225

*Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, Was sind personenbezogene Daten?, ZENDAS 2023, *Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, Was sind personenbezogene Daten?, ZENDAS Was sind personenbezogene Daten? (Datenschutz in der Hochschule)

## Kontakt

Rechtsinformationsstelle für die digitale Lehre (bwDigiRecht)
im Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg (HND-BW)
Karlsruher Institut für Technologie (KIT)
Adenauerring 12
76131 Karlsruhe
bwDigiRecht@hnd-bw.de

**Zitiervorschlag:** *Knecht, Jana,* Handreichung Rechtsbereichsspezifische Betrachtung von KI: Datenschutz, Rechtsinformationsstelle für die digitale Lehre (bwDigiRecht) im Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg, Karlsruhe, 2025.

**bwDigiRecht ist ein kooperatives Umsetzungsvorhaben von:**

HND BW Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg

UNIVERSITÄT HEIDELBERG ZUKUNFT SEIT 1386

KIT Karlsruher Institut für Technologie

HAW BW Hochschulen für Angewandte Wissenschaften Baden-Württemberg

Gefördert vom Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg

Baden-Württemberg
MINISTERIUM FÜR WISSENSCHAFT, FORSCHUNG UND KUNST