bwDigiRecht
Rechtsinformationsstelle für die digitale Lehre

Integration verschiedener Dienste in das Lernmanagement-system

Eine Handreichung der Rechtsinformationsstelle für die digitale Lehre bwDigiRecht

25.08.2026

Maximilian Spehn, Jana Knecht

Executive Summary

Lernmanagementsysteme (LMS) spielen an Hochschulen eine zentrale Rolle in der digitalen Lehre.[1] Über Plugins oder Schnittstellen lassen sich zahlreiche weitere Dienste in das LMS einbinden. Diese Handreichung behandelt drei in der Praxis besonders relevante und rechtlich unterschiedlich gelagerte Dienste: KI-Chatbots, Learning-Analytics-Werkzeuge und Streaming-Konferenzdienste. Im Mittelpunkt der rechtlichen Betrachtung steht im Folgenden die Integrationshandlung selbst, d.h. die Einbindung des Dienstes in das LMS. Der nachfolgende Betrieb des integrierten Dienstes, bzw. die spätere Nutzung durch Lehrende und Studierende wird nur nachrangig betrachtet. Dabei soll der Fokus auf diejenigen Aspekte gelegt werden, die unmittelbar durch die Integration in das LMS bedingt sind. Die datenschutzrechtliche Bewertung des Betriebs selbst, insbesondere bei Learning Analytics, kann je nach Szenario weitere grundrechtsrelevante Fragen aufwerfen, die in dieser Handreichung nicht abschließend behandelt werden.[2]

Übergreifende Anforderungen

Der **Digital Services Act** verpflichtet Hochschulen zur Einrichtung von Melde- und Abhilfeverfahren für rechtswidrige Inhalte, sofern sie als Hosting-Dienst für studentische Uploads fungieren. Der **Cyber Resilience Act** adressiert primär die Cybersicherheit digitaler Angebote, wobei für

[1] Alle hier zitierten Online-Quellen wurden zuletzt am 25.08.2026 abgerufen. Frei zugängliche 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. Das bedeutet nicht, dass ZENDAS die Ausführungen vollumfänglich teilt.

Hochschulen insbesondere Pflichten als Verwaltende quelloffener Software relevant werden können, wenn sie die Entwicklung solcher Produkte systematisch und nachhaltig unterstützen.

Integration von KI-Chatbots

Bei der Einbindung von KI-Systemen in ein LMS agieren Hochschulen regelmäßig als **Betreiber** im Sinne der **KI-Verordnung**. Während allgemeine Chatbots meist als Systeme mit beschränktem Risiko eingestuft werden, gelten KI-Anwendungen zur Bewertung von Lernergebnissen oder zur Steuerung von Lernprozessen als **hochriskant**.

Urheberrechtlich stellt die Installation von Plugins eine **Vervielfältigung** dar, die aufgrund von Rechtsunsicherheiten bei gesetzlichen Schranken bevorzugt über Lizenzen oder Open-Source-Lösungen abgesichert werden sollte.

Aus datenschutzrechtlicher Sicht ist insbesondere zu beachten, dass bereits die technische Anbindung eines KI-Systems **Datenflüsse** auslösen kann. Dabei sind insbesondere die Grundsätze des Datenschutzes durch **Technikgestaltung** und datenschutzfreundliche Voreinstellungen zu berücksichtigen. Ob eine **satzungsrechtliche Grundlage** zwingend erforderlich ist, ist eine Betrachtung des Einzelfalls. Sofern durch die bloße technische Anbindung lediglich technische Nutzungsdaten verarbeitet werden, keine Auftragsverarbeitenden eingesetzt werden und kein Drittlandtransfer stattfindet, kann § 12 Abs. 1 S. 1 LHG als Rechtsgrundlage für diesen begrenzten Zweck bereits ausreichend sein.

Spezifika von Learning Analytics

Learning-Analytics-Werkzeuge dienen der datenbasierten Beobachtung und Bewertung von Lernverhalten und können je nach Funktionsumfang ebenfalls als **Hochrisiko-KI** im Sinne der KI-Verordnung eingestuft werden, insbesondere wenn Lernergebnisse bewertet oder Lernprozesse gesteuert

werden. Die Einordnung sollte daher im Einzelfall sorgfältig geprüft und dokumentiert werden.

Urheberrechtlich ist insbesondere zu beachten, dass die Analyse von studentischen Arbeiten, Forenbeiträgen oder Lehrmaterialien eigene Vervielfältigungshandlungen auslösen kann. Hier sind entsprechende Nutzungsrechte oder gesetzliche Schranken, insbesondere die **Text-und-Data-Mining-Schranken**, zu prüfen.

Datenschutzrechtlich ist Learning Analytics besonders sensibel, da personenbezogene Daten systematisch ausgewertet und teilweise **Profile über Studierende** erstellt werden. Erforderlich sind daher eine klare Rechtsgrundlage, die Beachtung von Zweckbindung, Datenminimierung und Verhältnismäßigkeit sowie eine **menschliche Letztentscheidung**, sollten aus den Analysen folgenreiche Entscheidungen abgeleitet werden. Eine Generaleinwilligung ist im Hochschulkontext regelmäßig problematisch. Angemessen erscheint vielmehr eine **klare satzungsrechtliche Regelung**, die insbesondere Zwecke, Datenkategorien, Pseudonymisierung, Löschfristen und technische Schutzmaßnahmen festlegt. Aufgrund des regelmäßig hohen Risikos für die Rechte und Freiheiten der Betroffenen ist zudem häufig eine **Datenschutz-Folgenabschätzung** erforderlich.

Integration von Streamingdiensten

Die Integration von Streaming- und Videokonferenzdiensten in ein LMS ist insbesondere für die **hybride Lehre** weit verbreitet. Rechtlich sind hierbei vor allem das Urheberrecht und das Datenschutzrecht relevant.

Urheberrechtlich ist zwischen der technischen Einbindung der Software und der Nutzung fremder Inhalte in Lehrveranstaltungen zu unterscheiden. Die Installation kann eine **Vervielfältigung** darstellen und richtet sich insbesondere nach der jeweiligen Lizenz. Für die **Nutzung fremder Werke** in der Lehre ist vor allem § 60a UrhG zu beachten. Aufzeichnungen sind

besonders kritisch, da sie zusätzliche urheber- und datenschutzrechtliche Anforderungen auslösen.

Datenschutzrechtlich kommt es entscheidend auf die **konkrete technische Ausgestaltung der Integration** an. Bereits die Anbindung kann zusätzliche Datenflüsse zwischen LMS, Authentifizierungsdienst und Videokonferenzsystem auslösen. Zu prüfen ist daher insbesondere, welche Daten wann und an wen übermittelt und im LMS gespeichert werden, wer für die jeweilige Verarbeitung verantwortlich ist und auf welcher Rechtsgrundlage sie erfolgt. Für baden-württembergische Hochschulen ist dabei insbesondere § 12 LHG relevant.

Bei der Gestaltung sollten **Datenminimierung, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen** berücksichtigt werden. Ziel sollte sein, unnötige Datenübermittlungen, insbesondere bereits beim bloßen Aufruf einer LMS-Seite, zu vermeiden.

Inhaltsverzeichnis

01 Allgemeine Anforderungen ... 3

1.1 Digital Services Act ... 4

1.2 Cyber Resilience Act ... 4

02 Integration von KI-Chatbots ... 8

2.1 KI-Verordnung ... 8

2.2 Urheberrecht ... 12

2.3 Datenschutzrecht ... 15

03 Integration von Learning Analytics ... 20

3.1 KI-Verordnung ... 20

3.2 Urheberrecht ... 21

3.3 Datenschutzrecht ... 22

04 Integration von Streamingdiensten ... 27

4.1 Urheberrecht ... 27

4.2 Datenschutzrecht ... 29

05 Fazit ... 39

06 Literaturverzeichnis ... 40

01 Allgemeine Anforderungen

An baden-württembergischen Hochschulen kommen verschiedene Lernmanagementsysteme zum Einsatz, darunter insbesondere Moodle und ILIAS. Die Einbindung zusätzlicher Dienste erfolgt typischerweise auf zwei Wegen: Mittels Plugins aus den jeweiligen Plugin-Verzeichnissen[3] oder über eigens entwickelte Softwarekomponenten und Schnittstellen (APIs) können verschiedene Dienste in das Lernmanagementsystem integriert werden. Beide Wege lösen je nach Ausgestaltung unterschiedliche rechtliche Pflichten aus, die in den folgenden Abschnitten erörtert werden.

Vorbereitend zu einer separaten Betrachtung der drei Dienstkategorien erfolgt zunächst eine Darstellung übergreifender Anforderungen. Diese stellen grundlegende, allgemeingültige Rahmenbedingungen dar, die für sämtliche nachfolgenden Anwendungsszenarien Relevanz besitzen. Aufgrund ihrer nicht-kontextspezifischen Natur bedürfen sie keiner vertieften Erörterung innerhalb der jeweiligen Abschnitte der einzelnen Dienstkategorien.[4]

[3] Für Moodle: *Moodle Pty Ltd.*, Moodle Plugins directory, Link; *ILIAS open source e-Learning e.V.*, Plugins und Erweiterungen, Link.

[4] Da Lernmanagementsysteme regelmäßig keinen zentralen Plattformdienst (core platform service) im Sinne des Art. 2 Nr. 2 DMA darstellen und Hochschulen als Betreiberinnen eines LMS regelmäßig nicht die Voraussetzungen für eine Einstufung als Torwächter (gatekeeper) nach Art. 3 DMA erfüllen, wird der DMA im Folgenden nicht weiter betrachtet; vgl. zum Anwendungsbereich des DMA insbesondere Art. 2 und 3 DMA; vgl. insb. zum Anwendungsbereich des DMA: *Podszun u. a.*, Neue Juristische Wochenschr. 2022, 3249 (3249 f.).

1.1 Digital Services Act

Der Digital Services Act (DSA)[5] dient dazu Risiken für den demokratischen Diskurs einzudämmen.[6] Dazu werden Onlineplattformen in Abhängigkeit ihrer Größe bestimmte Pflichten auferlegt.[7] Der DSA ist auch für Hochschulen im Kontext von Lernmanagementsystemen relevant: Diese können „Hosting-Dienste" im Sinne des DSA sein, wenn sie den Studierenden auf der E-Learning-Plattform erlauben, eigene Inhalte hochzuladen.[8] Wird das von der Hochschule betriebene LMS als „Hosting-Dienst" im Sinne des DSA eingestuft, trifft die Hochschule nach Art. 16 DSA insbesondere die Pflicht, ein **Melde- und Abhilfeverfahren** für rechtswidrige Inhalte einzurichten.[9] Weitergehende Pflichten für sehr große Online-Plattformen dürften für hochschulische LMS regelmäßig nicht einschlägig sein, da die hierfür maßgeblichen Schwellenwerte nicht erreicht werden. Der DSA entfaltet auch jenseits des Lernmanagementsystems Relevanz[10], etwa mittelbar im Kontext von Drittanbieterdiensten;[11] dies wird in der vorliegenden Handreichung jedoch nicht weiter vertieft.

1.2 Cyber Resilience Act

Der Cyber Resilience Act (CRA)[12] ist ein weiterer Rechtsakt im Kontext der europäischen Digitalstrategie.[13] Dieser Rechtsakt wurde soweit bekannt

[5] *Europäisches Parlament und Rat der Europäischen Union*, Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), Link.
[6] *Kalbhenn*, ZRP 2025 111 Ff 2025, 111 (111 f.).
[7] *Kalbhenn*, ZRP 2025 111 Ff 2025, 111 (112).
[8] *Rennert*, DFN-Infobrief Recht 2022, 9 (11).
[9] *Roth-Isigkeit*, Anforderungen an Hosting-Dienste, § 41 Datenwirtschaft, Rn. 103.
[10] Insb. zur mittelbaren Relevanz im Kontext von Drittanbieterdiensten: *Rennert*, DFN-Infobrief Recht 2022, 9 (11).
[11] Insb. zur mittelbaren Relevanz im Kontext von Drittanbieterdiensten: *Rennert*, DFN-Infobrief Recht 2022, 9 (11).
[12] *Europäisches Parlament und Rat der Europäischen Union*, Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), Link.
[13] *Heynike/Taraz*, CCZ 2025 92 Ff 2025, 92 (93).

bisher nicht im Kontext von Lernmanagementsystemen betrachtet.[14] Der CRA zielt darauf ab, die Cybersicherheit von digitalen Produkten und Dienstleistungen zu erhöhen und eine widerstandsfähige digitale Infrastruktur zu schaffen.[15] Dieser Rechtsakt gilt gem. Art. 2 Abs. 1 CRA für auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt. Da der CRA zwar bereits in Kraft getreten ist, seine Vorschriften jedoch erst zu unterschiedlichen Zeitpunkten anwendbar werden, besteht hinsichtlich seiner konkreten Auswirkungen und Anforderungen derzeit noch Klärungsbedarf.[16] Er sieht insbesondere für **Herstellende** solcher Produkte Pflichten vor.[17]

Damit der CRA im Kontext von Lernmanagementsystemen überhaupt relevant ist, müssen die Lernmanagementsysteme oder die zu integrierende Dienste als final entwickeltes Produkt frei erworben werden können.[18] Entwickelt eine Hochschule ein Lernmanagementsystem ausschließlich für den eigenen Bedarf und stellt dieses nicht auf dem Markt bereit, ist der Anwendungsbereich des CRA insoweit nicht eröffnet. Die Hochschule unterliegt in diesem Fall grundsätzlich nicht den Herstellerpflichten des CRA.[19] Davon zu unterscheiden ist jedoch die Nutzung eines am Markt verfügbaren Lernmanagementsystems, etwa ILIAS oder Moodle, das von der Hochschule lediglich selbst betrieben oder für den eigenen Betrieb

[14] Den CRA lediglich im Kontext der Weiterentwicklung rechtlicher Rahmenbedingungen nennend: *Hochschulrektorenkonferenz*, Handlungsdruck für Hochschulen, Länder und Bund – HRK-Empfehlungen zur Cybersicherheit, Link, Fn. 3.
[15] *Heynike/Taraz*, CCZ 2025 92 Ff 2025, 92 (92).
[16] Gemäß Art. 71 Abs. 2 CRA gilt die Verordnung ab dem 11.12.2027; einzelne Vorschriften gelten bereits früher, ab dem 11.06.2026.
[17] Vgl. zu Herstellerpflichten: *Teichmann*, Neue Z. Für Verwaltungsrecht 20, 1662 (1663).
[18] Zu den Tatbestandsmerkmalen, insb. zur Finalität: *Heckmann/Koloßa*, Allgemeines, S. CRA Art. 2 Rn. 3-5.
[19] Vgl. zu den Herstellerpflichten: *Teichmann*, Neue Z. Für Verwaltungsrecht 20, 1662 (1662 ff.).

angepasst wird. In diesem Fall ist für die Beurteilung des Anwendungsbereichs des CRA insbesondere darauf abzustellen, welcher Akteur das Produkt entwickelt bzw. unter seinem Namen auf dem Markt bereitstellt.

Im Hochschulkontext kommen allenfalls noch **Pflichten für Verwaltende quelloffener Software** in Betracht:[20] Art. 24 CRA enthält für solche Personen z.B. eine Pflicht zur Entwicklung einer Cybersicherheitsstrategie sowie Meldepflichten. Damit eine Hochschule hinsichtlich ihres Lernmanagementsystems oder zu integrierender Dienste Verwalterin quelloffener Software ist, müsste sie jedoch eine juristische Person sein, die nach Art. 3 Nr. 14 CRA den Zweck oder das Ziel hat, die Entwicklung spezifischer Produkte mit digitalen Elementen, die als freie und quelloffene Software gelten und für kommerzielle Tätigkeiten bestimmt[21] sind, systematisch und nachhaltig zu unterstützen, und die die Brauchbarkeit dieser Produkte sicherstellt. Damit es sich beim Lernmanagementsystem oder den zu integrierenden Diensten um freie und quelloffene Software handelt, müssten Hochschulen außerdem nach Art. 3 Nr. 48 CRA den Quellcode offen teilen und im Rahmen einer Open-Source-Lizenz zur Verfügung stellen, die alle Rechte vorsieht, um sie frei zugänglich, nutzbar, veränderbar und weiterverteilbar zu machen.[22] Teilen Hochschulen den Quellcode nicht offen oder nutzen sie eine Closed-Source-Lizenz, kommen sie somit nicht als Verwaltende quelloffener Software in Betracht. Die bloße Mitentwicklung an einem Open-Source-Lernmanagementsystem oder an integrierbaren Open-Source-Diensten wird ebenfalls nicht ausreichen, um in

[20] Die Einordnung von Hochschulen als Einführer oder Händler dürfte im Regelfall nicht einschlägig sein; vgl. hierzu: *Paschke/Fellenberg*, Z. Für Eur. Daten- Informationsrecht 2025, 198 (201).

[21] Fraglich ist bereits, ob Lernmanagementsysteme oder zu integrierende Dienste im Hochschulkontext überhaupt „für kommerzielle Tätigkeiten bestimmt“ sind. Hochschulen setzen solche Systeme grundsätzlich zur Erfüllung ihrer Aufgaben ein, sodass dieses Tatbestandsmerkmal regelmäßig nicht ohne Weiteres bejaht werden kann.

[22] Vgl. zu diesen Tatbestandsmerkmalen: *Paschke/Fellenberg*, Z. Für Eur. Daten-Informationsrecht 2025, 198 (201 f.).

diesem Kontext Pflichten auszulösen: Hier fehlt es bereits am Tatbestandsmerkmal des Zurverfügungstellens, da die Mitentwickelnden hierüber kaum entscheiden können; außerdem hatte der Gesetzgeber mit der Regelung im Sinn, die Verantwortlichen für gesamte Open-Source-Software-Projekte zu treffen, wie etwa die Linux Foundation oder die Python Software Foundation.[23]

[23] *Paschke/Fellenberg*, Z. Für Eur. Daten- Informationsrecht 2025, 198 (202).

02 Integration von KI-Chatbots

KI-Chatbots lassen sich über vorgefertigte Plugins (etwa *AI Chat* für Moodle[24] oder ein *AI Assistant* für ILIAS[25]) oder über eigene Schnittstellen in das LMS einbinden. Bei der Integration sind insbesondere die KI-Verordnung, das Urheberrecht und das Datenschutzrecht zu beachten. Die drei Rechtsgebiete werden im Folgenden getrennt dargestellt.

2.1 KI-Verordnung

Die KI-Verordnung ist bei der Integration von KI-Chatbots in ein Lernmanagementsystem regelmäßig eine der zentralen unionsrechtlichen Bezugspunkte. Sie enthält unter anderem Pflichten für Anbieter und Betreiber. Hochschulen können in bestimmten Konstellationen hierunter fallen.[26] Wird ein bereits vorhandener KI-Chatbot über ein Plugin oder eine Schnittstelle in ein Lernmanagementsystem eingebunden, wird die Hochschule typischerweise **zumindest als Betreiber** des KI-Systems gem. Art. 3 Nr. 4 KI-VO anzusehen sein, weil sie das System im Rahmen ihrer organisatorischen Verantwortung für die Lehre einsetzt.[27] Ob daneben auch eine Stellung als Anbieter in Betracht kommt, hängt davon ab, ob die Hochschule das System nur selbst verwendet oder ob sie es auch

[24] *ByCS-Lernplattform u. a.*, AI Chat, Link.
[25] *Leifos GmbH*, AI Assistant, Link.
[26] Mehr dazu in der Handreichung von bwDigiRecht: *Spehn*, Hochschulen im Kontext von Anbieter- und Betreiberpflichten, Link.
[27] Vgl. zu den Tatbestandsmerkmalen: *Kirschke-Biller/Füllsack*, Einzelne Begriffsmerkmale, KI-VO Art. 3 Rn. 119 ff.

entwickelte oder entwickeln ließ sowie eine weitere tatbestandliche Handlung nach Art. 3 Nr. 3 KI-VO vornahm.[28]

Um die konkreten Pflichten für Hochschulen zu bestimmen, ist zudem die **Risikoklasse des KI-Systems** maßgeblich, hier also die des zu integrierenden KI-Chatbots. Aus den Vorschriften zu verbotenen Praktiken im KI-Bereich nach Art. 5 KI-VO und zu Hochrisiko-KI-Systemen nach Art. 6 Abs. 2 i.V.m. Anhang III KI-VO lässt sich entnehmen, dass es dabei auf den Verwendungszweck ankommt. Im Rahmen der Integration in ein Lernmanagementsystem kommen im Hochrisiko-KI-Bereich allenfalls zwei Hochrisiko-Verwendungszwecke in Betracht:

- Gemäß Art. 6 Abs. 2 i.V.m. Anhang III Nr. 3 lit. b KI-VO gilt ein KI-System, das bestimmungsgemäß für die **Bewertung von Lernergebnissen** verwendet werden soll, einschließlich des Falles, dass diese Ergebnisse dazu dienen, den Lernprozess natürlicher Personen in Einrichtungen oder Programmen aller Ebenen der allgemeinen und beruflichen Bildung zu *steuern*, als hochriskant. Hierbei geht es typischerweise darum, dass Klausuren, Multiple-Choice-Tests und Hausarbeiten bewertet werden.[29] Das Tatbestandsmerkmal des *Steuerns* umfasst z.B. Einstufungstests, die Personen entsprechend ihres Lernniveaus auf Kurse mit unterschiedlichem Schwierigkeitsgrad verteilen[30] oder aber auch Learning Analytics.[31] Zu letzterem finden sich in Abschnitt 3 vertiefende Ausführungen. Geht es beim KI-System jedoch nicht um

[28] Diese tatbestandlichen Handlungen umfassen gem. Art. 3 Nr. 3 KI-VO das Inverkehrbringen unter eigenem Namen oder der Handelsmarke oder das Inbetriebnehmen unter eigenem Namen oder Handelsmarke unabhängig von der Entgeltlichkeit.
[29] *Klawonn*, Bewertung von Lernergebnissen, Link, KI-VO Anhang III Nr. 3 Rn. 54.
[30] *Klawonn*, Bewertung von Lernergebnissen, Link, KI-VO Anhang III Nr. 3 Rn. 53.
[31] *Ruschemeier*, Bewertung von Lernergebnissen, KI-VO Anhang III Rn. 37.

das konstitutive Merkmal des Bewertens von Lernergebnissen,[32] so kommt diese Vorschrift nicht in Betracht.

- Gemäß Art. 6 Abs. 2 i.V.m. Anhang III Nr. 3 lit. c KI-VO gilt ein KI-System, das bestimmungsgemäß zum Zweck der **Bewertung des angemessenen Bildungsniveaus**, das eine Person im Rahmen von oder innerhalb von Einrichtungen aller Ebenen der allgemeinen und beruflichen Bildung erhalten wird oder zu denen sie Zugang erhalten wird, verwendet werden sollen, als hochriskant. Der Unterscheid zu Anhang III Nr. 3 lit. b KI-VO besteht darin, dass lit. c sich nach seinem Wortlaut auf eine *Vorhersage* des möglichen Leistungspotenzials einer Person bezieht, bevor die Person überhaupt beginnt, an einer Bildungseinrichtung zu lernen.[33] Da die Personen, die mit einem in ein Lernmanagementsystem integrierten KI-System in Berührung kommen, in aller Regel bereits eingeschriebene Studierende sind, lernen die Personen bereits an Bildungseinrichtungen. Damit umfasst der Wortlaut dieser Norm nicht den Fall der Integration von KI-Systemen in Lernmanagementsysteme.

Sofern die Anwendung weder einer gesetzlich untersagten Praxis noch einem hochriskanten Einsatzszenario entspricht, kann das betreffende KI-System als **KI-System mit beschränktem Risiko** klassifiziert werden. Diese Einstufung trifft typischerweise auf allgemein gehaltene Chatbots zu.[34] Gleichwohl ist eine pauschale Einordnung nicht möglich. Eine erste Orientierung für die Einordnung können die Handreichungen von bwDigiRecht „Hochschulen im Kontext von Anbieter- und Betreiberpflichten“[35] und „Zusammenfassung der KI-Verordnung für den Kontext der Hochschullehre“[36] bieten. Gelangt die Hochschule zu der

[32] *Klawonn*, Bewertung von Lernergebnissen, Link, KI-VO Anhang III Nr. 3 Rn. 53.
[33] *Ruschemeier*, Bewertung von Lernergebnissen, KI-VO Anhang III Rn. 39.
[34] *Bundesnetzagentur*, Risk levels, Link.
[35] *Spehn*, Hochschulen im Kontext von Anbieter- und Betreiberpflichten, Link.
[36] Zu den Risiken s. insb.: *Knecht*, Zusammenfassung der KI-Verordnung für den Kontext der Hochschullehre, S. 6 ff.

Einschätzung, dass es sich um ein KI-System mit beschränktem Risiko handelt, müssen die folgenden Pflichten nach der KI-Verordnung befolgt werden:

- **KI-Kompetenz** (Art. 4 KI-VO): Anbieter und Betreiber müssen Maßnahmen ergreifen, um ein ausreichendes Maß an KI-Kompetenz ihres mit Betrieb und Nutzung befassten Personals sicherzustellen.[37]
- **Transparenz** (Art. 50 KI-VO): Bei KI-Systemen, die zur Interaktion mit natürlichen Personen bestimmt sind, ist sicherzustellen, dass die betroffenen Personen darüber informiert werden, dass sie mit einem KI-System interagieren, soweit dies nicht aus den Umständen ohnehin offensichtlich ist.
- **Evaluation** (Art. 25 KI-VO): Die Risikoklasse von KI-Systemen muss regelmäßig reevaluiert werden: Wenn sich beispielsweise. die Zweckbestimmung so ändert, dass das KI-System zu einem Hochrisiko-KI-System wird gem. Art. 25 Abs. 1 lit. c KI-VO i.V.m. Art. 6 KI-VO können nach Art. 25 Abs. 1 KI-VO Betreiber zu Anbietern von Hochrisiko-KI-Systemen werden. Daraus folgt jedenfalls mittelbar eine Pflicht zur erneuten Evaluierung, die sich mit einer Überwachung des KI-Systems bzw. einer technischen Absicherung auf Compliance-Ebene organisieren ließe.

Sinnvoll ist im Ergebnis, die Einsatzszenarien im Lernmanagementsystem differenziert freizugeben. Ein Chatbot, welcher allgemeine technische Fragen zur Bedienung des Lernmanagementsystems beantwortet, ist rechtlich anders zu bewerten als ein KI-System, das Lernstände bewertet, um die Zulassung in einen E-Learning-Kurs zu organisieren oder in

[37] *Europäische Kommission*, Verordnung (EU) 2026/1744 des Europäischen Parlaments und des Rates vom 8. Juli 2026 zur Änderung der Verordnungen (EU) 2024/1689, (EU) 2018/1139 und (EU) 2023/1230 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), S. 3, Link, Nr. (8); Vgl. hierzu die Handreichung von bwDigiRecht: *Knecht*, KI-Kompetenz Qualifizierungsanforderungen für Hochschulangehörige.

Prüfungsumgebungen eingebunden wird. Die Hochschule sollte daher keine pauschale Freigabe für KI im Lernmanagementsystem erteilen, sondern konkrete Anwendungsfälle bewerten und dokumentieren.

2.2 Urheberrecht

Die Integration eines KI-Chatbots in ein Lernmanagementsystems selbst ist kein urheberrechtlich neutraler Vorgang, sondern kann mehrere den Rechtsinhabenden vorbehaltene Verwertungshandlungen berühren. Bereits die Bereitstellung eines Plugins oder einer sonstigen Integrationskomponente auf dem Webserver oder Applikationsserver der Hochschule stellt typischerweise eine **Vervielfältigung** im Sinne des Urheberrechts dar. Gleiches gilt für Installationskopien, Backups, temporäre Zwischenspeicherungen im Arbeitsspeicher (RAM[38]), Container-Images, Update-Stände und Testumgebungen.[39] Aus der eventuell bestehenden technischen Notwendigkeit folgt nicht automatisch die rechtliche Zulässigkeit. Vielmehr ist zu prüfen, ob die Hochschule aufgrund einer (Open-Source-)Lizenz, eines Nutzungsvertrages oder anderweitig gesetzlich zur Installation und zum Betrieb berechtigt ist. Wichtig ist außerdem, dass dabei auch die konkrete Betriebsform, etwa der produktive Servereinsatz, eine Anpassung, Weiterentwicklung oder Einbindung in ein hochschulweit genutztes LMS, umfasst ist. Als gesetzliche Schranke kommt insb. § 69d Abs. 5 UrhG in Betracht, wonach die Vervielfältigung von Computerprogrammen unter weiteren Maßgaben und unter Verweis auf § 60a UrhG erlaubt wird. Maßgeblich hierfür ist, dass Vervielfältigung des Computerprogramms der **Veranschaulichung der Lehre** dient[40] und die Nutzung auf Bildungseinrichtungen beschränkt und die elektronische Lehr- und Lernumgebung gesichert ist, z.B. durch ein Authentifizierungsverfahren.[41] Liegen diese Voraussetzungen vor, so darf

[38] Random Access Memory
[39] Vgl. Urheberrechtsgesetz, Link, §69c UrhG, Rn. 5-11; Praxiskommentar Urheberrecht, Link, § 69c UrhG, Rn. 5-9.
[40] Ergibt sich aus § 69d Abs. 5 UrhG i.V.m. § 60a Abs. 1 UrhG.
[41] *Spies*, Veranschaulichung von Unterricht und Lehre (Abs. 5), UrhG § 69d Rn. 20.

das Computerprogramm gem. § 69d Abs. 5 Nr. 3 UrhG vollständig und nicht nur wie in § 60a Abs. 1 UrhG zu 15% genutzt werden.[42] Nicht abschließend geklärt ist jedoch, wann konkret Software in Lernmanagementsystemen der Veranschaulichung der Lehre nach § 69d Abs. 5 Nr. 4 UrhG i.V.m. § 60a Abs. 1 UrhG dient: Nach der Vorstellung des Gesetzgebers reicht es nicht aus, wenn Textverarbeitungssoftware installiert wird, um im Deutschunterricht das Erstellen von Texten zu üben.[43] Diese gesetzliche Schranke sollte angesichts der bestehenden Rechtsunsicherheit hinsichtlich der Auslegung des Merkmals der Veranschaulichung der Lehre restriktiv gehandhabt werden und im besten Falle auf die anderen Möglichkeiten wie eine Lizenzvereinbarung oder Open-Source-Lizenz zurückgegriffen werden.

Die Integration ist zudem oft mit **Anpassungen** verbunden: Etwa an die hochschuleigene Systemarchitektur, Änderungen am Quellcode, Lokalisierungen, Sicherheitspatches, API-Anbindungen, Erweiterungen von Rollen- und Rechtemodellen oder die Verbindung mit Authentifizierungsdiensten (Single Sign-on). Solche Eingriffe können als grundsätzlich zustimmungsbedürftige Bearbeitung oder Umgestaltung gem. § 69c Nr. 2 UrhG einzuordnen sein. Die Schranke des § 69d Abs. 1 UrhG i.V.m. § 60a UrhG ist grundsätzlich anwendbar; jedoch verbleibt Rechtsunsicherheit hinsichtlich der Reichweite des Tatbestandsmerkmals *Veranschaulichung der Lehre*. Die Schranke sollte daher mit Vorsicht und eher restriktiv verwendet werden. Hochschulen sollten prüfen, ob ihre Lizenz nicht nur die Nutzung, sondern auch die technische Anpassung erlaubt. Bei Open-Source-Komponenten bestehen regelmäßig weitergehende Bearbeitungsrechte, die jedoch an die jeweiligen Lizenzbedingungen geknüpft sind[44], etwa hinsichtlich Copyleft-Effekten,

[42] *Spies*, Veranschaulichung von Unterricht und Lehre (Abs. 5), UrhG § 69d Rn. 22.
[43] *Dreier*, Text und Data Mining, Unterricht und Lehre, vergriffene Werke (Abs. 4–7), UrhG § 69d Rn. 27.
[44] Vgl. hierzu die Open Source Definition der Open Source Initiative, insbesondere Ziff. 3 zu Bearbeitungen und abgeleiteten Werken, *open source initiative*, The Open Source Definition, Link; Exemplarisch: *open source initiative*, GNU General Public License version 3, Link.

Hinweis- und Dokumentationspflichten oder der Pflicht, abgeleitete Fassungen unter denselben Bedingungen weiterzugeben.

Soweit die Integration des KI-Chatbots hochschuleigene Inhalte einschließt, etwa indem Systemprompts, FAQ-Sammlungen, Lehrmaterialien oder sonstige Dokumente in den Dienst eingebunden werden, stellt sich zusätzlich die Frage, ob diese Inhalte vervielfältigt, in Datenbanken überführt oder technisch aufbereitet werden dürfen. Auch insoweit ist zunächst die Integrationshandlung maßgeblich: Schon das Einspeisen solcher Materialien in einen Retrieval-Index oder eine serverseitige Wissensbasis kann eine urheberrechtlich relevante Vervielfältigung darstellen.[45] Hochschulen sollten deshalb nicht erst den späteren Chatbot-Output betrachten, sondern bereits die vorgelagerte Systembefüllung rechtlich absichern. Das gilt besonders dann, wenn Materialien von Lehrenden, Studierenden oder Verlagen stammen und nicht ausschließlich von der Hochschule selbst erstellt wurden. In Bezug auf die Nutzung des KI-Systems, insbesondere hinsichtlich des Umgangs mit und des Schutzes von Eingabe- und Ausgabedaten, wird auf die Handreichung von bwDigiRecht „Rechtsbereichsspezifische Betrachtung von KI: Urheberrecht“[46] verwiesen.

Für die Praxis folgt daraus, dass urheberrechtliche Prüfungen bei der Integration von KI-Chatbots in das LMS als Teil des technischen Freigabeprozesses organisiert werden sollten. Vor der Installation ist zu klären, unter welcher Lizenz die Integrationskomponente steht, welche Nutzungsrechte für Serverbetrieb und Anpassung eingeräumt sind, ob Begleitpflichten aus Open-Source-Lizenzen bestehen und ob zusätzliche Inhalte in das System eingespeist werden sollen. Erst auf einer zweiten Ebene stellt sich dann die Frage nach der Nutzung der mit dem integrierten Dienst erzeugten oder verarbeiteten Inhalte. Zuvörderst geht es jedoch um

[45] Vgl. *LG München*, Gewerbl. Rechtsschutz Urheberrecht 2025, (179 ff.), Link.
[46] *Knecht*, Rechtsbereichsspezifische Betrachtung von KI: Urheberrecht, Link.

die urheberrechtliche Zulässigkeit der Integration als solcher, also um Installation, Vervielfältigung, Anpassung und Bereitstellung im LMS-Betrieb.

2.3 Datenschutzrecht

Auch datenschutzrechtlich spielt die Integration selbst eine zentrale Rolle. Im Folgenden steht weniger die Art der später eingegebenen Chat-Inhalte im Fokus, sondern vielmehr die bereits durch die **technische Einbindung des Dienstes** ausgelöste Verarbeitung personenbezogener Daten. Schon die Implementierung eines Plugins, einer externen API-Anbindung oder einer eingebetteten Benutzendenoberfläche kann dazu führen, dass z.B. beim Login personenbezogene Daten zwischen Systemen übermittelt oder auf den Servern der Hochschule verarbeitet werden. Die datenschutzrechtliche Bewertung muss daher bereits auf Ebene der Systemarchitektur beginnen. Es wird im Folgenden davon ausgegangen, dass der KI-Dienst von keinem externen Anbieter erbracht wird und dass keine Daten in ein Drittland übermittelt werden, sondern dass ein vollständiges lokales Hosting der KI-Dienste an der Hochschule stattfindet. Andernfalls müssten die Vorschriften zur Auftragsverarbeitung nach Art. 28 DSGVO bzw. zum Drittlandtransfer nach Art. 44 ff. DSGVO beachtet werden.

Bereits beim Aufruf einer LMS-Seite mit integriertem KI-Dienst werden regelmäßig technische Nutzungsdaten verarbeitet, etwa IP-Adressen, Zeitstempel, Session-Informationen und Identifikationsnummer. Wird der Dienst über ein Plugin eingebunden, kann es zur Übermittlung von Authentifizierungsdaten oder pseudonymisierten Kennungen an den integrierten Dienst kommen. Diese Daten können personenbezogene Daten im Sinne des Art. 4 Nr. 1 DSGVO darstellen.[47] Damit kann der **Anwendungsbereich** der DSGVO eröffnet sein, und zwar unabhängig davon, ob Nutzende bereits Daten (z.B. einen Prompt) eingegeben haben.

[47] Zur IP-Adresse: *Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, https://www.zendas.de/themen/personenbezogene_daten/ipadresse.html, Link; *Pohl/Winter*, Z. Für Datenschutzrecht 2026, 244 (246 ff.); Zur Nutzerkennung: *European Data Protection Board*, Datenschutzgrundlagen, Link.

Die Rechtmäßigkeit der Verarbeitung richtet sich nach Art. 6 Abs. 1 DSGVO. In der baden-württembergischen Hochschulpraxis werden vergleichbare KI-Chatbots auf verschiedene Rechtsgrundlagen gestützt: Eine Stützung auf **Einwilligung** (Art. 6 Abs. 1 Satz 1 lit. a DSGVO) ist im Hochschulverhältnis häufig problematisch, weil es angesichts des strukturellen Über-/Unterordnungsverhältnisses regelmäßig an der Freiwilligkeit fehlt.[48] In der Rechtsliteratur wird diese Option insbesondere für „*Zusatz*angebote in der Lehre wie z.B. *optionale* Kursangebote, die für die Erreichung von berufsqualifizierenden Abschlüssen *keine notwendige Voraussetzung* sind"[49] in Betracht gezogen. In der baden-württembergischen Hochschulpraxis wird die Einwilligung bereits z.B. für die Verarbeitung durch nutzungswidrige Eingabe verwendet.[50]

Für Hochschulen als öffentliche Stellen kommt alternativ Art. 6 Abs. 1 Satz 1 lit. e DSGVO **Wahrnehmung einer Aufgabe im öffentlichen Interesse** in Betracht. Sollen die personenbezogenen Daten zwecks Wahrnehmung einer Aufgabe im öffentlichen Interesse verarbeitet werden, bedarf es einer nach Maßstäben von Art. 6 Abs. 3 DSGVO ausgestalteten nationalen Rechtsgrundlage. Der Erwägungsgrund zu Art. 6 DSGVO zählt zu diesen Maßstäben die Vorhersehbarkeit im Sinne der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte.[51] Eine Vorschrift ist dann vorhersehbar, wenn sie mit hinreichender Bestimmtheit formuliert ist, so dass jede Person, bei Bedarf mit angemessener Beratung, in der Lage ist, sich entsprechend zu

[48] Die Freiwilligkeit im Kontext der Aufzeichnung von Lehrverstaltungen erörternd: *Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, Zulässigkeit der Aufzeichnung von Lehrveranstaltungen, Link.
[49] *Seckelmann/Horstmann*, Ordn. Wiss. 2024, 169 (177).
[50] *HTWG Konstanz*, Nutzungsbedingungen und Datenschutzhinweise zur Nutzung von bwGPT by Kersta an der HTWG Konstanz, S. 4, Link.
[51] Erwägungsgrund 41 DSGVO: Die entsprechende Rechtsgrundlage oder Gesetzgebungsmaßnahme sollte jedoch klar und präzise sein und ihre Anwendung sollte für die Rechtsunterworfenen gemäß der Rechtsprechung des Gerichtshofs der Europäischen Union und des Europäischen Gerichtshofs für Menschenrechte vorhersehbar sein.

verhalten.[52] Als Rechtsgrundlage kommt hierfür in Baden-Württemberg § 12 Abs. 1 S. 1 LHG in Frage. Sie erlaubt die Datenverarbeitung, „wenn und soweit die Verarbeitung zur Erfüllung der Aufgaben der Hochschule erforderlich ist."[53] Die Aufgaben der Hochschulen ergeben sich aus § 2 LHG. In Betracht können folgende Aufgaben kommen: Pflege und Entwicklung von Studium und Lehre sowie Vorbereitung auf berufliche Tätigkeit. Für die Beurteilung, ob die Datenverarbeitung auf § 12 Abs. 1 S. 1 LHG allein gestützt werden kann, wäre eine Einzelfallprüfung erforderlich, da es entscheidend auf den Nutzungszweck ankommt. Zweifelhaft ist, ob § 12 Abs. 1 S. 1 LHG die Datenverarbeitung im Rahmen der KI-Anwendungen im LMS hinreichend vorhersehbar regelt. Nach § 12 Abs. 3 LHG ist es jeder Hochschule jedoch unbenommen, in einer Satzung entsprechende Datenverarbeitungen bestimmt, klar und vorhersehbar zu regeln. In jedem Fall wäre zu prüfen, ob die Verarbeitung der personenbezogenen Daten für die Erreichung des Zwecks erforderlich ist und kein gleichgeeignetes aber weniger datenintensives Mittel vorhanden ist.

Von besonderer Bedeutung im Rahmen der **Datenverarbeitung** sind die Grundsätze der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO sowie des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sowie weitere Maßnahmen nach Art. 25 Abs. 1, Abs. 2 DSGVO. Bei der Integration von KI-Chatbots in das LMS ist, neben den allgemeinen datenschutzrechtlichen Anforderungen, § 3a LDSG Baden-Württemberg in den Blick zu nehmen.[54] Die Vorschrift verlangt, dass automatisierte Datenverarbeitungssysteme von vornherein so gestaltet werden müssen, dass sie **den Datenschutz durch Technikgestaltung** und

[52] *Agentur der Europäischen Union für Grundrechte und Europarat*, Handbuch zum europäischen Datenschutzrecht, S. 44 f., Link.
[53] § 12 Abs. 1 S. 1 LHG
[54] § 3a LDSG BW konkretisiert den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c DSGVO, indem er technische und organisatorische Maßnahmen bereits bei der Systemgestaltung verlangt.

datenschutzfreundliche Voreinstellungen fördern.[55] Dies hat direkte Auswirkungen auf die Art und Weise der technischen Anbindung des Chatbots an das LMS.

Konkret bedeutet dies, dass bereits die **Integrationshandlung selbst** sicherstellen muss, dass der Chatbot **nur die für seine Funktionalität unbedingt notwendigen Daten verarbeitet**. Dazu gehören technische Vorkehrungen wie die deaktivierte Protokollierung von Nutzendendaten oder die automatische Löschung von Chatverläufen nach einer vordefinierten Frist, sofern keine gesetzliche oder vertragliche Speicherpflicht besteht.[56] Darüber hinaus sind **anonyme oder pseudonyme Nutzungsoptionen** für Studierende und Lehrende vorzuhalten,[57] um die Datenminimierung (§ 3a LDSG BW i. V. m. Art. 5 Abs. 1 lit. c DSGVO) zu gewährleisten.

Die datenschutzfreundliche **Grundkonfiguration des Chatbots** muss daher bereits im Rahmen der Integration erfolgen. Dies umfasst auch die **klare Information der Nutzenden** über Art, Umfang und Zweck der Datenverarbeitung durch den Chatbot, z.B. durch Hinweise im Chatinterface oder in den Nutzungsbedingungen des LMS.[58] Sofern der Chatbot auch Dienste von Dienstleistenden nutzt, die außerhalb der EU ansässig sind, ist zudem zu prüfen, ob zusätzliche Anforderungen (z. B. zu Drittlandtransfers) zu beachten sind.

Zur Erfüllung weiterer Pflichten, insbesondere der Transparenzpflichten nach Art. 13 f. DSGVO und der Aufnahme in das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO), sowie zu nutzungsbezogenen

---

[55] Vgl. *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*, KI-Einsatz durch die Verwaltung: Wie ist § 3a LDSG anzuwenden?, Link.

[56] Anonyme oder pseudonyme Nutzungsmöglichkeiten sind z. B. durch Nutzung von Session-Tokens oder die Deaktivierung der Speicherung von IP-Adressen umsetzbar.

[57] Vgl. Art. 32 DSGVO: "Technische Maßnahmen zur Datensicherheit" umfassen auch die Löschung personenbezogener Daten, sobald diese nicht mehr benötigt werden.

[58] Die Information der Nutzenden kann z. B. durch Pop-up-Hinweise im LMS oder automatische Bestätigungen nach Chatbeginn erfolgen.

Fragen wird auf die Handreichung von bwDigiRecht „Rechtsbereichsspezifische Betrachtung von KI: KI und Datenschutz“ verwiesen.[59]

[59] Zu den Grundsätzen der Datenverarbeitung finden sich v.a. ab S. 9 Ausführungen: *Knecht*, Rechtsbereichsspezifische Betrachtung von KI: KI und Datenschutz, S. 9 ff., Link.

03 Integration von Learning Analytics

Learning-Analytics-Werkzeuge werten Nutzungs- und Lerndaten aus, um Aussagen über Lernverhalten, Leistungsstand, Teilnahmeintensität oder Unterstützungsbedarf abzuleiten.[60] Sie sind über das LMS einbindbar. Bei der Integration von Learning-Analytics-Werkzeugen in das LMS verschieben sich in rechtlicher Perspektive die Schwerpunkte gegenüber der KI-Chatbot-Integration deutlich: Im Vordergrund stehen die KI-Verordnung, soweit ein KI-System vorliegt, und vor allem das Datenschutzrecht. Gegenstand dieses Kapitels ist nicht allein die rechtliche Bewertung der Integration von Learning-Analytics-Werkzeugen in das LMS, sondern auch deren Betrieb.

3.1 KI-Verordnung

Learning-Analytics-Dienste dienen der systematischen Erfassung und Auswertung von Daten über Lernprozesse, um daraus Erkenntnisse über Lernverhalten, Leistungsstand oder Lernfortschritt zu gewinnen. Solche Dienste müssen nicht zwingend KI-Funktionalitäten enthalten. Da jedoch zunehmend KI-basierte Verfahren eingesetzt werden, ist im Folgenden insbesondere die rechtliche Einordnung von Learning-Analytics-Diensten mit integrierten KI-Funktionen zu betrachten.

Wie bereits im Abschnitt zu KI-Chatbots dargestellt, kann Learning Analytics einen **Hochrisiko-Zweck** nach Art. 6 Abs. 2 i. V. m. Anhang III Nr. 3 lit. b KI-VO darstellen, wenn das System *Lernergebnisse bewertet* oder den

[60] Ein Beispiel für ein Learning-Analytics-Werkzeug ist LeAP von der Universität Mannheim: *Universität Mannheim*, LeAP – Learning Analytics Profiles, Link.

Lernprozess steuert. Ob ein konkretes Learning-Analytics-System hochriskant ist, hängt stark von Funktionsumfang und Einsatzkontext ab. Eine erste Orientierung bietet ein Rechtsgutachten im Auftrag der HU Berlin, das verschiedene Szenarien analysiert und bewertet.[61] Denkbar ist auch eine Einordnung als System mit beschränktem oder minimalem Risiko: Das wäre etwa bei einem niedrigschwelligen, auf personalisiertes Feedback in der Studienorientierung beschränkten Funktionsumfang, bei dem eine Beeinflussung des Lernprozesses und der Zulassung zu Bildungseinrichtungen ausgeschlossen werden kann gegeben.[62] Voraussetzung ist mithin, dass das System die für die Hochrisiko-Einstufung konstitutiven Merkmale gerade nicht erfüllt. Angesichts der weitreichenden Folgen der Klassifizierung als Hochrisiko-KI-System[63] sollte die Einordnung sorgfältig begründet und dokumentiert werden.

3.2 Urheberrecht

Urheberrechtlich werfen Learning-Analytics-Anwendungen auf den ersten Blick geringere Probleme auf als generative KI-Systeme, weil sie typischerweise keine Inhalte erzeugen, sondern Daten auswerten. Hinsichtlich der Vervielfältigung der Software und ihrer Bereitstellung gelten die Ausführungen zum KI-Chatbot in Abschnitt 2.2 zu §§ 69c f. UrhG entsprechend.

Eigenständige Fragen entstehen jedoch, wenn Inhalte in die Analyse einbezogen werden. Dies ist trifft dann zu, wenn das KI-System eingereichte Arbeiten wie Essays und Hausarbeiten oder Lernmanagementsystem-Foreneinträge sowie sonstige hochgeladene Dokumente verwendet. Solche von Studierenden erstellten Beiträge können urheberrechtlich geschützt sein, sofern sie die erforderliche Schöpfungshöhe (§ 2 Abs. 2 UrhG)

[61] Eine Übersicht der Szenarien findet sich unter: *Geminn u. a.*, Beurteilung von Learning Analytics nach Datenschutzrecht und KI-Verordnung an Hochschulen in Berlin, S. 4, Link.
[62] *Geminn u. a.*, Beurteilung von Learning Analytics nach Datenschutzrecht und KI-Verordnung an Hochschulen in Berlin, S. 4, Link.
[63] *Spehn*, Hochschulen im Kontext von Anbieter- und Betreiberpflichten, Link.

erreichen.[64] Dieser Grundsatz ist auf Lehrmaterialien, Vorlesungsskripte, Videos oder Foliensätze von Lehrenden übertragbar.[65] Die inhaltliche Analyse setzt regelmäßig Vervielfältigungen und gegebenenfalls Umformatierungen voraus und bedarf daher einer urheberrechtlichen Rechtfertigung. Diese liegt nicht schon deshalb vor, weil die Inhalte ins LMS eingestellt wurden. Zu prüfen ist insbesondere, ob eine **wirksame urheberrechtliche Einwilligung bzw. Nutzungserlaubnis** vorliegt, ob satzungsrechtliche Nutzungsrechte bestehen oder ob eine urheberrechtliche Schranke greift. Für letzteres kommt insbesondere die wissenschaftliche Text-und-Data-Mining-Schranke (TDM-Schranke) nach § 60d UrhG oder die allgemeine TDM-Schranke § 44b UrhG, bei der ein etwaiger Nutzungsvorbehalt der Rechtsinhabenden zu beachten ist, in Betracht. Zur TDM-Schranke enthält die Handreichung von bwDigiRecht „Verhältnis von Data Crawling und Urheberrecht“[66] vertiefende Hinweise.

3.3 Datenschutzrecht

Die Integration und Nutzung von Learning-Analytics sind datenschutzrechtlich relevant. Personenbezogene Daten von Studierenden werden systematisch erhoben, zusammengeführt, ausgewertet und zur Ableitung von Aussagen über individuelle Bildungsprozesse genutzt. Anders als bei rein administrativen LMS-Funktionen geht es damit um eine **datenbasierte Beobachtung und Bewertung**. Hochschulen sollten daher von Beginn an von einem erhöhten Prüfungsmaßstab ausgehen.

Derzeit ist uns keine Rechtsprechung bekannt, die sich mit der Rechtmäßigkeit der Datenverarbeitung beim Einsatz von Learning-Analytics befasst hätte. Als nationale Rechtsgrundlage für die Verarbeitung personenbezogener Daten könnte § 12 Abs. 1 LHG herangezogen werden.[67]

---

[64] Zur Qualifikation einer Vorlesung als Sprachwerk: Münchener Kommentar zum StGB, UrhG § 106 Rn. 26.
[65] Mehr dazu: *Schlotfeldt*, Rechtsfragen rund um die Lehrveranstaltung, S. 5 f., Link.
[66] *Knecht*, Verhältnis von Data Crawling und Urheberrecht im Hochschulkontext, Link.
[67] Zu Einordnung und Anforderungen an eine nationale Rechtgrundlage s. unter 2.3

Hierfür müsste diese Rechtgrundlage den unionsrechtlichen Grundsätzen der Klarheit, Präzision, Verhältnismäßigkeit und Vorhersehbarkeit entsprechen. Es reicht aus, wenn der Zweck der Verarbeitung erforderlich ist, um eine Aufgabe zu erfüllen, die im öffentlichen Interesse liegt.[68] Zu klären wäre, ob die Auswertung von Nutzungs- und Lerndaten, um Aussagen über Lernverhalten, Leistungsstand, Teilnahmeintensität oder Unterstützungsbedarf abzuleiten, zu Aufgaben der Hochschule gehört und ob dies für die Studierenden hinreichend klar und vorhersehbar ist. Aus der Aufgabe der Pflege und Entwicklung der Wissenschaften durch Forschung, Lehre und Studium, § 2 Abs. 1 LHG, könnte eine entsprechende Aufgabe im öffentlichen Interesse abgeleitet werden. Dagegen spricht jedoch, dass diese allgemeine Erlaubnis zur Datenverarbeitung zu unbestimmt ist, um eingriffsintensive Datenverarbeitung beim Einsatz von Learning-Analytics (z.B. Datenzusammenführung und Profiling) zu legitimieren.

Zusätzlich zu diesen datenschutzrechtlichen Erwägungen ist zu beachten, dass die datenschutzrechtliche Bewertung des Einsatzes von Learning Analytics nicht auf die bloße Integrationshandlung beschränkt bleiben darf, sondern **den tatsächlichen Betrieb des Systems** umfassen muss. Je nach Einsatzszenario kann der Betrieb von Learning Analytics einen so grundrechtsintensiven Eingriff darstellen,[69] dass zu prüfen ist, ob die satzungsrechtliche Ermächtigung aus § 12 Abs. 3 LHG ausreicht, oder ob aufgrund des **Parlamentsvorbehalts** bzw. der **Wesentlichkeitstheorie** eine gesetzliche Rechtsgrundlage erforderlich ist.[70] Die Frage, ob sich aus dem

[68] *Kühling/Buchner*, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG.

[69] Eingriffsintensive Maßnahmen wie Profilbildung, systematische Überwachung oder automatisierte Entscheidungen können Grundrechte wie die informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) oder die Berufsfreiheit (Art. 12 GG) betreffen. *Der Landesbeauftragte für Datenschutz und Informationssicherheit Baden-Württemberg*, Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, v. 2, c.

[70] Der Parlamentsvorbehalt verlangt, dass wesentliche Entscheidungen mit Grundrechtsrelevanz vom Parlament selbst geregelt werden müssen. Die Wesentlichkeitstheorie unterstreicht dies und fordert, dass insbesondere Eingriffe in Grundrechte wie die informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1

Parlamentsvorbehalt oder der Wesentlichkeitstheorie zusätzliche Anforderungen an die Rechtsgrundlage des Einsatzes von Learning Analytics ergeben, wird im Rahmen dieser Handreichung nicht vertieft untersucht.

Ferner käme studienbegleitende Beratung der Studierenden in allen studienbezogenen Angelegenheiten, § 2 Abs. 2 LHG, als öffentliche Aufgabe in Betracht. Entscheidend wäre jedoch zum einen, ob im Falle von Learning Analytics-Systemen eine solche Datenverarbeitung für die Studierenden vorhersehbar wäre. Zum anderen wäre zu klären, ob sie erforderlich wäre, um diese Aufgabe zu erfüllen. Aus der Beratungsaufgabe der Hochschulen ergibt sich nicht zwingend für Studierende vorhersehbar die Befugnis, ihr Lernverhalten kontinuierlich zu überwachen.

Zu prüfen ist, ob die betreffende Aufgabe nicht ebenso durch eine weniger datenintensive Maßnahme erfüllt werden kann. In diesem Zusammenhang ist insbesondere der Grundsatz der Datenminimierung zu berücksichtigen, wonach personenbezogene Daten nur in dem Umfang verarbeitet werden sollten, der zur Erreichung des jeweiligen Zwecks erforderlich ist. Learning Analytics können zwar zur Unterstützung der Aufgabenerfüllung beitragen, stellen hierfür jedoch keine zwingende Voraussetzung dar. Sofern der verfolgte Zweck auch mit weniger oder weniger sensiblen personenbezogenen Daten erreicht werden kann, wäre einer solchen weniger datenintensiven Maßnahme grundsätzlich der Vorzug zu geben. Es wäre daher empfehlenswert entsprechende Aufgaben und Verarbeitungszwecke in einer Hochschulsatzung entsprechend der Ermächtigung nach § 12 Abs. 3 LHG zu regeln. Inhaltlich sollte eine solche

---

Abs. 1 GG einer expliziten gesetzlichen Grundlage bedürfen. Bei Learning Analytics-Systemen, die über reine Nutzungsanalysen hinausgehen und z.B. Profilbildung oder automatisierte Bewertungen vornehmen, ist fraglich, ob § 12 Abs. 3 LHG als ausreichende Ermächtigungsgrundlage dienen kann. Falls Learning Analytics-Systeme Profilbildung, automatisierte Entscheidungen oder die Weitergabe von Daten an Dritte ermöglichen, könnte dies den Parlamentsvorbehalt aktivieren und eine gesetzliche Regelung erforderlich machen. *Rux*, GG Art. 20; *Spellbrink*, Wesentlichkeitstheorie, BVerfG.

Satzung insbesondere Aufgaben und Zweck sowie die zu verarbeitenden Daten beschreiben und darüber hinaus Aussagen bzgl. der Datenminimierung, Pseudonymisierung, Löschfristen, Zweckbindung treffen sowie technische und organisatorische Maßnahmen festlegen. Eine **Generaleinwilligung** ist im Hochschulverhältnis kaum praktikabel, da ihre Freiwilligkeit angesichts des Abhängigkeitsverhältnisses[71] und der Notwendigkeit eines gleichwertigen Angebots für Nichteinwilligende schwer darstellbar ist. Denkbar sind stattdessen **Opt-in- oder Opt-out-Modelle**, bei denen sich die Entscheidung der betroffenen Person auf eine konkret bezeichnete Verarbeitung oder einen bestimmten Verarbeitungszweck bezieht. Beim Opt-in erfolgt die Verarbeitung nur nach ausdrücklicher Zustimmung, während sie beim Opt-out grundsätzlich erfolgt, sofern die betroffene Person nicht widerspricht oder die Teilnahme ablehnt.

Besondere Bedeutung hat der Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO: Daten, die ursprünglich zu einem anderen Zweck erhoben wurden, dürfen nicht ohne Weiteres für eine Verhaltensanalyse weiterverwendet werden. Eine Zweckänderung ist nur unter den Voraussetzungen des Art. 6 Abs. 4 DSGVO bzw. einer spezifischen Rechtsgrundlage zulässig. Hinzu treten die Grundsätze der Erforderlichkeit und Verhältnismäßigkeit: Je eingriffsintensiver die Auswertung, desto höher die Anforderungen an ihre Rechtfertigung.

Soweit Learning Analytics die betroffenen Personen bewertet, liegt regelmäßig ein **Profiling** im Sinne des Art. 4 Nr. 4 DSGVO vor.[72] Führt das System zu einer ausschließlich automatisierten Entscheidung mit rechtlicher Wirkung oder ähnlich erheblicher Beeinträchtigung, etwa zu einer automatisierten Zulassungs- oder Ausschlussentscheidung, ist diese

[71] S. Abschnitt 2.3.
[72] Vgl. zum Profiling im Kontext von Learning Analytics: *Geminn u. a.*, Beurteilung von Learning Analytics nach Datenschutzrecht und KI-Verordnung an Hochschulen in Berlin, S. 40 ff., Link.

nach Art. 22 Abs. 1 DSGVO grundsätzlich unzulässig, sofern keine Ausnahme nach Art. 22 Abs. 2 DSGVO greift. In der Praxis sollte daher eine **wesentliche menschliche Letztentscheidung** sichergestellt sein, damit gerade keine ausschließlich automatisierte Entscheidung vorliegt. Werden besondere Kategorien personenbezogener Daten verarbeitet, sind zusätzlich die Vorgaben des Art. 9 DSGVO sowie die engeren Grenzen des Art. 22 Abs. 4 DSGVO zu beachten. Eine solche Verarbeitung könnte beispielsweise bei Gesundheitsdaten von Studierenden mit Beeinträchtigungen in Betracht kommen, sofern deren Berücksichtigung erforderlich ist, um eine Verzerrung der Auswertung des Lernfortschritts zu vermeiden.

Angesichts der systematischen und umfassenden Bewertung persönlicher Aspekte sowie der Verarbeitung von Daten in einem Verhältnis struktureller Unterlegenheit liegt häufig ein voraussichtlich hohes Risiko vor, sodass eine Datenschutz-Folgenabschätzung durchzuführen ist: In der Rechtsliteratur wird diese im Kontext der Learning Analytics für erforderlich erachtet.[73]

Manche Anbieter von Learning Analytics-Anwendungen werben mit der Datenschutzfreundlichkeit ihrer Lösung.[74] Eine solche Selbstauskunft entbindet die Hochschule als Verantwortliche nicht von ihrer eigenständigen Prüfungs- und Dokumentationspflicht (Art. 5 Abs. 2, Art. 24 DSGVO). Zu weiteren KI-spezifischen datenschutzrechtlichen Vorschriften wird auf die ergänzende Handreichung von bwDigiRecht „Rechtsbereichsspezifische Betrachtung von KI: KI und Datenschutz“[75] verwiesen.

[73] *Geminn u. a.*, Beurteilung von Learning Analytics nach Datenschutzrecht und KI-Verordnung an Hochschulen in Berlin, S. 54, Link.
[74] Die eigene Lösung als „Privacy-friendly“ bezeichnend: *Dondorf u. a.*, Learning Analytics, Link.
[75] *Knecht*, Rechtsbereichsspezifische Betrachtung von KI: KI und Datenschutz, Link.

04 Integration von Streamingdiensten

Die Integration von Streaming- und Videokonferenzdiensten in das LMS ist bereits gelebte Praxis. Sie dient beispielsweise zur Unterstützung im Rahmen hybrider Lehre.[76] Ein Beispiel für ein solches System ist etwa BigBlueButton, das über Plugins in Moodle und ILIAS eingebunden werden kann und so das Lernmanagementsystem mit Konferenztools verbindet.[77] Rechtlich berührt eine solche Integration insbesondere das Datenschutzrecht und das Urheberrecht.

4.1 Urheberrecht

Urheberrechtlich sind bei der Verbindung von Streamingdiensten mit dem LMS zwei Ebenen zu unterscheiden: die Einbindung der Software in das LMS (Integrationsebene) und die Nutzung fremder Werke in der Lehrveranstaltung (Nutzungsebene).

Auf der ersten Ebene der **Einbindung** der Streaming-Software in das LMS gelten die Ausführungen in Abschnitt 2.2 entsprechend: Bereits die Installation und der Betrieb der Software auf den Servern der Hochschule stellen eine Vervielfältigung dar (§§ 16, 69c Nr. 1 UrhG). Anpassungen, also Branding, Konfiguration, Anbindung an den Authentifizierungsdienst oder Sicherheitspatches, können eine zustimmungsbedürftige Bearbeitung sein, soweit sie über die bestimmungsgemäße Benutzung im Sinne des § 69d

[76] Vgl. zu diesem Thema die Handreichung von bwDigiRecht: *Spehn*, Streaming im Rahmen hybrider Lehre, Link.
[77] *Dixon/Federico*, BigBlueButton BN, Link; *ILIAS open source e-Learning e.V.*, BigBlueButton, Link.

UrhG hinausgehen (§ 69c Nr. 2 UrhG). Maßgeblich ist die jeweilige Lizenz. Praktisch besonders bedeutsam ist dies bei selbst gehosteten Open-Source-Lösungen: *BigBlueButton* steht beispielsweise unter der Lesser General Public License (LGPL)-Version 3.0.[78] Die Integration in eine eigene, auch hochschulische, Anwendung ist danach zulässig, solange die Bedingungen der LGPL eingehalten werden: bei Veränderung und Weitergabe der lizenzierten Komponenten sind die Copyleft-Pflichten der LGPL[79] zu beachten. Hinzu kommt eine vom Urheberrecht zu trennende markenrechtliche Schranke: Der Name und das Logo „BigBlueButton" sind markenrechtlich geschützt und nicht von der Open-Source-Lizenz erfasst; ihre Verwendung richtet sich nach den gesonderten Markenrichtlinien.

Auf der zweiten Ebene betrifft die **Nutzung** von Streamingdiensten vor allem die Verwendung fremder Werke in der Lehre. Werden in einer Live-Sitzung Präsentationen, Texte, Bilder, Filmausschnitte oder Musik verwendet, ist zu prüfen, ob diese Nutzung urheberrechtlich gedeckt ist. Bereits die Live-Wiedergabe geschützter Werke im Stream ist eine öffentliche Wiedergabe im Sinne des § 15 Abs. 2 UrhG und damit rechtfertigungsbedürftig.

Zentrale **Schranke** ist § 60a UrhG. Nach § 60a Abs. 1 UrhG dürfen zur Veranschaulichung des Unterrichts und der Lehre an Bildungseinrichtungen zu nicht kommerziellen Zwecken bis zu 15 Prozent eines veröffentlichten Werkes vervielfältigt, verbreitet, öffentlich zugänglich gemacht und in sonstiger Weise öffentlich wiedergegeben werden. Dies gilt zugunsten von Lehrenden und Teilnehmenden der jeweiligen Veranstaltung (Nr. 1), für Lehrende und Prüfende an derselben Einrichtung (Nr. 2) sowie für Dritte, soweit dies der Präsentation des Unterrichts oder von Unterrichts- bzw. Lernergebnissen dient (Nr. 3). Nach § 60a Abs. 2 UrhG dürfen bestimmte

[78] Lesser General Public License (LGPL), *BigBlueButton Inc.*, License, Link.

[79] Eine abschließende Übersicht der jeweiligen Pflichten ergibt sich aus der LGPL Version 3.0; *open source initiative*, GNU Lesser General Public License version 3, Link; für BigBlueButton stellt das Projekt zudem eine eigene Dokumentation zur Installation, Administration und Integration bereit: *BigBlueButton Inc.*, FAQs, Link.

Werkarten – insbesondere Abbildungen, einzelne Beiträge aus derselben Fach- oder wissenschaftlichen Zeitschrift, Werke geringen Umfangs und vergriffene Werke – vollständig genutzt werden. Darüber hinaus nimmt § 60a Abs. 3 UrhG bestimmte Nutzungen von der Schrankenregelung aus. Für die hochschulische Nutzung ist daher insbesondere zu prüfen, ob die konkrete Nutzung unter die in § 60a Abs. 3 genannten Ausschlusstatbestände fällt; ist dies nicht der Fall, kann die Nutzung grundsätzlich nach Maßgabe der Absätze 1 und 2 zulässig sein.

Für die urheberrechtliche Bewertung der Verwendung geschützter Werke im Rahmen eines Videokonferenzdienstes ist die Unterscheidung zwischen dem Live-Streaming z.B. einer Lehrveranstaltung auf der einen und der Aufzeichnung einer Sitzung auf der anderen Seite zentral: Aus einer flüchtigen Wiedergabe wird durch Aufzeichnung eine dauerhafte Vervielfältigung und bei späterer Bereitstellung des Videos im LMS eine öffentliche Zugänglichmachung. Damit treten neben die datenschutzrechtliche Frage nach der Zulässigkeit der Aufzeichnungen weitere urheberrechtliche Herausforderungen in Bezug auf die Beiträge der Teilnehmenden. Siehe hierzu vertiefend die Handreichung von bwDigiRecht „Streaming im Rahmen hybrider Lehre“.[80]

4.2 Datenschutzrecht

Bei der Integration von Streaming- und Videokonferenzdiensten in ein LMS ist zwischen den Datenverarbeitungen des LMS, des Authentifizierungsdienstes und des jeweils eingesetzten Streaming- bzw. Videokonferenzdienstes zu unterscheiden. Gegenstand der nachfolgenden Betrachtung ist dabei nicht die allgemeine datenschutzrechtliche Zulässigkeit des Einsatzes eines Videokonferenz- oder Streamingdienstes. Vielmehr wird betrachtet, **welche zusätzlichen Datenverarbeitungen** gerade durch dessen technische oder funktionale Einbindung in das LMS entstehen und welche datenschutzrechtlichen Anforderungen an diese Integration zu

[80] *Spehn*, Streaming im Rahmen hybrider Lehre, Link.

stellen sind. Es wird im Folgenden davon ausgegangen, dass keine Aufzeichnung, sondern ein Streaming stattfindet,[81] d.h. „das gleichzeitige Empfangen und Wiedergeben von Video- oder Audiodateien aus einem Rechnernetz“.[82]

Eine solche Integration kann technisch unterschiedlich ausgestaltet sein. Denkbar ist insbesondere, dass das LMS lediglich einen Link zu einem virtuellen Konferenzraum bereitstellt und die eigentliche Nutzung anschließend beim Videokonferenzdienst erfolgt.

Möglich ist aber auch eine weitergehende Integration, bei der der Dienst unmittelbar aus dem LMS heraus aufgerufen wird und Informationen aus dem LMS an den Videokonferenzdienst übermittelt werden. So ermöglicht beispielsweise das Moodle-Plugin für BigBlueButton die Anlage und Verwaltung von BigBlueButton-Konferenzräumen unmittelbar innerhalb eines Moodle-Kurses. Die BigBlueButton-API sieht für den Beitritt zu einer Konferenz unter anderem die Übermittlung eines Namens zur Identifizierung der teilnehmenden Person gegenüber den anderen Konferenzteilnehmenden, einer Meeting-ID sowie einer Rolleninformation vor.[83]

Daraus folgt zugleich, dass bei einer Integration nicht ohne Weiteres davon ausgegangen werden kann, dass zwischen LMS und Videokonferenzdienst überhaupt keine personenbezogenen Daten ausgetauscht werden.

Für die datenschutzrechtliche Bewertung ist daher zunächst die **konkrete technische Ausgestaltung der Integration** zu ermitteln. Insbesondere ist zu prüfen, ob es sich lediglich um eine Verlinkung handelt oder ob eine technische Schnittstelle zwischen LMS und Videokonferenzsystem besteht, ob eine Authentifizierung über das LMS bzw. einen zentralen

[81] Für detaillierte Auseinandersetzung mit Streaming: *Spehn*, Streaming im Rahmen hybrider Lehre, Link.
[82] *Raue/Stang*, Streaming aus technologischer Sicht, A. § 3 II.1.b.ee. Rn. 35.
[83] Zur Integration von BigBlueButton als Aktivität innerhalb eines Moodle-Kurses: *Moodle Pty Ltd.*, Moodle Plugins directory, Link, BigBlueButton BN.

Identitätsdienst erfolgt und welche Attribute dabei an den Videokonferenzdienst übermittelt werden. Bei einer technischen Integration können beispielsweise ein Name, eine E-Mail-Adresse, eine Nutzenden- oder pseudonymisierte Kennung, eine Kurs- oder Veranstaltungszuordnung sowie eine Rolleninformation übermittelt werden. Welche dieser Daten tatsächlich verarbeitet werden, ist anhand der konkreten Implementierung und der jeweiligen Konfiguration des LMS und des Videokonferenzdienstes festzustellen.

Besonders relevant ist dabei die Frage, ob bereits **durch den Aufruf** der entsprechenden Funktion im LMS **eine Verarbeitung durch den externen Dienst** ausgelöst wird oder ob **eine Datenübermittlung** erst beim **tatsächlichen Beitritt** zu einer Videokonferenz erfolgt. Eine pauschale Aussage, wonach bereits die bloße Einbindung eines Videokonferenzdienstes stets eine Übermittlung der IP-Adresse oder anderer personenbezogener Daten an den Dienstanbieter bewirkt, lässt sich ohne Kenntnis der konkreten technischen Implementierung nicht treffen. Vielmehr ist anhand der eingesetzten Integrationsform zu prüfen, wann eine Verbindung zum Server des Dienstanbieters hergestellt wird und welche Daten hierbei verarbeitet werden.[84] Gerade bei eingebetteten Diensten ist deshalb zu untersuchen, ob bereits beim Laden einer LMS-Seite externe Inhalte oder Funktionen des Videokonferenzdienstes geladen werden oder ob die Kommunikation mit dem Drittanbieter erst nach einer bewussten Aktivierung durch die nutzende Person beginnt.[85]

Von Bedeutung ist ferner die **Übermittlung von Identifikations- und Authentifizierungsdaten**. Wird beispielsweise eine Anmeldung über einen zentralen Identitätsdienst oder ein Single-Sign-on-Verfahren ermöglicht, ist

[84] Zur Notwendigkeit, die konkrete technische Implementierung zu untersuchen, vgl. die technische Dokumentation der jeweiligen Integration, hier beispielhaft: *Moodle Pty Ltd.*, Moodle Plugins directory, Link; *BigBlueButton Inc.*, License, Link.

[85] Für die konkrete Frage, wann bei einer Einbettung eine Verbindung zu einem externen Dienst hergestellt wird, ist die konkrete Implementierung maßgeblich; eine pauschale Aussage lässt sich ohne technische Prüfung nicht treffen.

zu prüfen, welche Informationen vom LMS bzw. vom Identitätsdienst an das Videokonferenzsystem übermittelt werden. Dabei sollte insbesondere geprüft werden, ob für die Teilnahme an der Videokonferenz eine unmittelbar personenbezogene Kennung erforderlich ist oder ob eine weniger eingriffsintensive, etwa pseudonymisierte Kennung verwendet werden kann. Für die übergreifenden Anforderungen gelten weitgehend die Ausführungen zum Datenschutzrecht in Abschnitt 2.3 entsprechend: Dies betrifft insbesondere die Grundsätze der Datenminimierung und den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen.

Die technische Integration kann darüber hinaus dazu führen, dass **Nutzungs- und Veranstaltungsdaten zwischen LMS und Videokonferenzsystem ausgetauscht oder im LMS gespeichert werden**. Dies ist von der eigentlichen Datenverarbeitung im Rahmen der Videokonferenz zu unterscheiden. Beispielsweise können Informationen darüber verarbeitet werden, welche virtuelle Veranstaltung angelegt wurde, welcher Kurs einem Konferenzraum zugeordnet ist oder – im Falle einer Aufzeichnung – welche Aufzeichnungen zu einer LMS-Veranstaltung gehören. Bei bestimmten Integrationen können auch Metadaten zur Konferenz im LMS vorgehalten werden. Bei Moodle wird etwa dokumentiert, dass bei einer BigBlueButton-Integration Metadaten zu Aufzeichnungen im LMS gespeichert werden können, während die eigentlichen Aufzeichnungen beim BigBlueButton-System verbleiben.[86]

Eine solche Verarbeitung ist datenschutzrechtlich nicht bereits deshalb zulässig, weil die zugrunde liegende Videokonferenz ihrerseits rechtmäßig durchgeführt werden darf. Vielmehr ist für jeden weiteren Verarbeitungsvorgang eine eigenständige datenschutzrechtliche Prüfung vorzunehmen. Dabei ist insbesondere zu bestimmen, **welchem konkreten**

[86] Vgl. MoodleDocs, „Upgrading“, zu im LMS gespeicherten Metadaten von BigBlueButton-Aufzeichnungen: *Moodle.com*, Documentation, Link.

Zweck die Verarbeitung dient, ob sie zur Erreichung dieses Zwecks **erforderlich** ist und auf **welche Rechtsgrundlage** sie gestützt werden kann. Für baden-württembergische Hochschulen ist hierbei insbesondere § 12 Abs. 1 LHG zu berücksichtigen. Danach dürfen Hochschulen personenbezogene Daten verarbeiten, wenn und soweit die Verarbeitung zur Erfüllung der Aufgaben der Hochschule erforderlich ist. Nach § 12 Abs. 3 LHG regeln die Hochschulen die Verarbeitung personenbezogener Daten, insbesondere Erhebung, Nutzung, Übertragung sowie Aufbewahrungsdauer und Löschung, durch Satzung. Die Vorschrift ist daher insbesondere dann relevant, wenn die Integration zu zusätzlichen Übermittlungen oder einer zusätzlichen Speicherung personenbezogener Daten im LMS führt.

Die datenschutzrechtliche Verantwortlichkeit ist ebenfalls **für die konkrete Verarbeitung und nicht allein anhand der technischen Bezeichnung „Integration“** zu bestimmen. Werden LMS und Videokonferenzsystem von unterschiedlichen Stellen betrieben, ist für die jeweils stattfindende Verarbeitung zu prüfen, welche Stelle über Zwecke und Mittel entscheidet. Die Begriffe der Verantwortlichen, der Auftragsverarbeitenden und der gemeinsam Verantwortlichen sind nach den tatsächlichen Umständen der Verarbeitung zu bestimmen. Der Europäische Datenschutzausschuss betont insoweit den funktionalen Charakter dieser Begriffe und stellt für die Abgrenzung insbesondere darauf ab, wer über Zwecke und wesentliche Mittel der Verarbeitung entscheidet. Für die konkrete Gestaltung bedeutet dies, dass insbesondere zu prüfen ist, ob der Betreiber des Videokonferenzsystems die Daten ausschließlich im Auftrag der Hochschule verarbeitet oder ob er für einzelne Verarbeitungsvorgänge eigene Zwecke verfolgt.[87]

Bei einem Videokonferenzdienst, der auch Dienstleistungen enthält, die eine Auftragsverarbeitung darstellen, sind darüber hinaus die Anforderungen

[87] *European Data Protection Board*, Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Link, Rn. 30 ff..

des Art. 28 DSGVO zu beachten.[88] Dies betrifft insbesondere die Festlegung des Gegenstands und der Dauer der Verarbeitung, der Art und des Zwecks der Verarbeitung, der Art der personenbezogenen Daten und der Kategorien betroffener Personen sowie der Rechte und Pflichten des Verantwortlichen.[89] Die datenschutzrechtliche Einordnung kann jedoch nicht allein durch eine vertragliche Bezeichnung als Auftragsverarbeitung erfolgen; entscheidend bleibt die tatsächliche Ausgestaltung der Verarbeitung.

Von den zusätzlichen Verarbeitungen aufgrund der LMS-Integration sind diejenigen Datenverarbeitungen abzugrenzen, die durch die eigentliche **Nutzung des Streaming- oder Videokonferenzdienstes** entstehen. Wird beispielsweise bei einer Videokonferenz das Mikrofon oder die Kamera aktiviert, werden Audio- und Videodaten verarbeitet und an die anderen Teilnehmenden übermittelt. Bei BigBlueButton können darüber hinaus Chatinhalte, IP-Adresse sowie Geräte- bzw. Hardwareinformationen verarbeitet werden.[90] Auch für Webex können bei der Nutzung insbesondere Name, E-Mail-Adresse, Beginn und Ende der Teilnahme sowie die Teilnahmedauer verarbeitet werden; außerdem können Audio- und Videodaten verarbeitet werden, wenn Mikrofon und Kamera aktiviert sind.[91]

Diese Verarbeitungsvorgänge sind grundsätzlich Bestandteil der datenschutzrechtlichen Bewertung des jeweiligen Streaming- bzw. Videokonferenzdienstes. Sie sind von denjenigen Verarbeitungsvorgängen

---

[88] Da Videokonferenzdienste grundsätzlich als Telekommunikationsdienste im Hinblick auf die Audio- und Videoübertragung einzuordnen sein können, erfolgt die Verarbeitung insoweit nicht im Rahmen einer Auftragsverarbeitung, sondern in eigener Verantwortlichkeit des Dienstleisters. Die Auftragsverarbeitung sollte daher ggf. auf sonstige, hiervon abgrenzbare Dienstleistungen beschränkt werden. Vgl. hierzu *Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, Sind Videokonferenzdienste Telekommunikationsdienste im Sinne des TKG?, Link.

[89] Zur funktionalen Bestimmung der Rollen von Verantwortlichem und Auftragsverarbeiter: *European Data Protection Board*, Leitlinien zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, Link, Rn. 15 ff., Rn. 73 ff..

[90] *Karlsruher Institut für Technologie (KIT)*, Datenschutzerklärung Videokonferenzen mit BigBlueButton (BBB), Link.

[91] *Universität Stuttgart*, Informationen zum Umgang mit Webex, Link.

zu unterscheiden, die **erst aufgrund der Anbindung an das LMS** entstehen. Für die vorliegende Betrachtung ist deshalb insbesondere zu fragen, welche Daten bereits im LMS vorhanden sind und aufgrund der Integration an den Videokonferenzdienst übermittelt werden und welche Informationen umgekehrt vom Videokonferenzdienst an das LMS zurückübermittelt oder dort gespeichert werden.

Diese Abgrenzung ist auch für die Frage der **Teilnahme- und Nutzungsprotokollierung** relevant. So können Videokonferenzsysteme Informationen über Teilnehmende, Beginn und Ende der Teilnahme oder die Teilnahmedauer erzeugen. Die Universität Stuttgart weist beispielsweise darauf hin, dass bei Webex automatisch Berichte mit entsprechenden Teilnahmeinformationen erstellt werden können.[92] Werden solche Informationen zusätzlich in das LMS übertragen und dort mit dem Studien- oder Kurskonto einer Person verknüpft, entsteht eine zusätzliche Verarbeitung im LMS, die gesondert hinsichtlich des Zwecks, der Erforderlichkeit, der Rechtsgrundlage, der Speicherdauer und der Zugriffsberechtigung zu prüfen ist.

Dies gilt insbesondere dann, wenn aus den Nutzungsdaten **Verhaltens- oder Aktivitätsprofile** gebildet werden. Eine bloße technische Information darüber, dass eine Person an einer Videokonferenz teilgenommen hat, ist von einer weitergehenden Auswertung zu unterscheiden, bei der etwa Teilnahmehäufigkeit, Aktivität in einzelnen Veranstaltungen oder sonstige Nutzungsdaten systematisch zusammengeführt und zur Bewertung oder Personalisierung des Lernangebots verwendet werden. Eine solche weitergehende Nutzung kann nicht ohne Weiteres mit der technischen Bereitstellung des Videokonferenzdienstes gleichgesetzt werden und bedarf einer eigenständigen Prüfung insbesondere anhand der Zweckbindung und Datenminimierung nach Art. 5 Abs. 1 lit. b und c DSGVO.

[92] Vgl., insbesondere zu den verarbeiteten Teilnahme- und Nutzungsdaten: *Universität Stuttgart*, Informationen zum Umgang mit Webex, Link.

Für die datenschutzrechtliche Bewertung der Integration ist außerdem zu prüfen, ob der eingesetzte Dienst Daten **außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums** verarbeitet oder dorthin übermittelt. Dies kann insbesondere bei extern betriebenen Videokonferenzdiensten relevant sein. Die Universität Stuttgart weist beispielsweise für Webex ausdrücklich auf Verarbeitungen personenbezogener Daten außerhalb der EU bzw. des EWR hin und behandelt diese im Rahmen der Regelungen über internationale Datenübermittlungen. Für eine konkrete LMS-Integration ist daher zu prüfen, ob und welche Daten aufgrund der Integration an einen solchen Dienst übermittelt werden und ob hierfür die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.[93]

Für die technische Gestaltung der Integration ergeben sich daraus insbesondere Anforderungen an **Datenminimierung und datenschutzfreundliche Voreinstellungen**. Eine datenschutzfreundliche Lösung sollte möglichst vermeiden, dass bereits beim bloßen Aufruf einer LMS-Seite ohne tatsächliche Nutzung des Videokonferenzdienstes personenbezogene Daten an einen externen Dienst übertragen werden. Ebenso sollte geprüft werden, welche Identifikationsdaten für die Teilnahme tatsächlich erforderlich sind und ob auf die Übermittlung zusätzlicher Profil- oder Kursinformationen verzichtet werden kann. Soweit eine Funktion auch mit einer weniger personenbezogenen oder pseudonymisierten Kennung bereitgestellt werden kann, ist diese Möglichkeit unter dem Gesichtspunkt der Datenminimierung zu berücksichtigen.

Für die konkrete Prüfung einer Integration sollten daher insbesondere folgende Fragen beantwortet werden:

[93] Für die konkrete Beurteilung sind insbesondere die Datenschutzerklärung und die Angaben zur Datenübermittlung des jeweils eingesetzten Dienstes heranzuziehen.

1. Welche Integrationsform wird verwendet? Handelt es sich um eine bloße Verlinkung, eine technische Schnittstelle, eine Einbettung oder eine Integration mit Single-Sign-on?
2. Wann findet eine Datenübermittlung statt? Bereits beim Aufruf einer LMS-Seite, erst beim Aktivieren des Dienstes oder erst beim Beitritt zu einem virtuellen Raum?
3. Welche Daten werden vom LMS bzw. Authentifizierungsdienst an den Videokonferenzdienst übermittelt?
4. Welche Daten erhält das LMS vom Videokonferenzdienst zurück?
5. Werden Teilnahme-, Nutzungs- oder Veranstaltungsdaten im LMS gespeichert?
6. Werden die Daten aus dem LMS und dem Videokonferenzsystem miteinander verknüpft?
7. Wer ist hinsichtlich der jeweiligen Verarbeitung Verantwortlicher, Auftragsverarbeitender oder gegebenenfalls gemeinsam Verantwortlicher?
8. Auf welcher Rechtsgrundlage erfolgt die jeweilige zusätzliche Verarbeitung bzw. Übermittlung?
9. Ist die jeweilige Datenverarbeitung zur Erfüllung der Hochschulaufgabe erforderlich?
10. Ist für die konkrete Verarbeitung eine Regelung durch Hochschulsatzung nach § 12 Abs. 3 LHG erforderlich?
11. Werden Daten an Stellen außerhalb der EU bzw. des EWR übermittelt?[94]

[94] Zur Übermittlung personenbezogener Daten an Drittländer: *Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, Übermittlung personenbezogener Daten an Drittländer, Link.

12. Kann die Integration technisch so gestaltet werden, dass weniger personenbezogene Daten verarbeitet oder übermittelt werden?

Für die datenschutzrechtliche Bewertung der Integration ist damit entscheidend, **nicht die gesamte Verarbeitung im Videokonferenzsystem erneut zu bewerten, sondern die zusätzlichen Datenflüsse zwischen LMS, Authentifizierungsdienst und Streaming- bzw. Videokonferenzsystem herauszuarbeiten**. Erst wenn diese Datenflüsse und Verantwortlichkeiten feststehen, lässt sich beurteilen, ob die konkrete Integrationslösung datenschutzrechtlich zulässig und datenschutzgerecht ausgestaltet ist.

Für eine detaillierte Auseinandersetzung mit Streaming wird auf die Handreichung von bwDigiRecht „Streaming im Rahmen hybrider Lehre“ verwiesen.[95] Hierbei muss insbesondere geprüft werden, welche Art von Lehrveranstaltung vorliegt, da davon abhängt, inwiefern Studierende im Live-Stream sicht- oder hörbar sein dürfen.[96] Auf eine Aufzeichnung sollte mangels nicht abschließend geklärter Rechtsgrundlage verzichtet werden.[97]

[95] *Spehn*, Streaming im Rahmen hybrider Lehre, Link.
[96] *Spehn*, Streaming im Rahmen hybrider Lehre, S. 16, Link.
[97] ZENDAS vertritt die Auffassung, „[f]ür die Aufzeichnung von Daten der Teilnehmerinnen und Teilnehmer bei Lehrveranstaltungen gibt es derzeit in Baden-Württemberg keine Rechtsgrundlage“ (*Zentrale Datenschutzstelle der baden-württembergischen Universitäten*, Zulässigkeit der Aufzeichnung von Lehrveranstaltungen, Link; eine davon abweichende Auffassung auf Basis der Einwilligung (jedoch nicht im baden-württembergischen Kontext) vertritt z.B. *Scholz*, Aufzeichnung von Lehrveranstaltungen.

05 Fazit

Die Integration zusätzlicher Dienste in das LMS ist rechtlich kein einheitlicher Vorgang, sondern verlangt eine nach Dienstkategorie differenzierte Betrachtung. Bei *KI-Chatbots* stehen die Rollen- und Risikoeinordnung nach der KI-Verordnung, die lizenz- und urheberrechtliche Zulässigkeit der Integration sowie die datenschutzrechtliche Absicherung im Vordergrund. Bei *Learning Analytics* verschiebt sich der Schwerpunkt auf das Datenschutzrecht: Zweckbindung, Erforderlichkeit, Profiling und automatisierte Entscheidungen sowie häufig eine Datenschutz-Folgenabschätzung prägen die Bewertung. Bei *Streaming-Diensten* treten die Nutzung fremder Werke in der Lehre (§ 60a UrhG) und die besonderen Risiken von Aufzeichnungen in den Mittelpunkt. Übergreifend gelten die Anforderungen aus DSA und CRA. Allen Konstellationen gemeinsam ist, dass die rechtliche Prüfung bereits bei der Integrationshandlung ansetzen muss. Ein dokumentierter Freigabeprozess ist daher der zentrale Baustein einer rechtssicheren Dienstintegration. Zentral ist außerdem, dass es insbesondere bei der urheberrechtlichen Bewertung zu Rechtsunsicherheiten in Bezug auf die Auslegung von § 69d Abs. 5 UrhG kommt; diese Vorschrift sollte daher restriktiv angewandt werden und auf andere Optionen wie Open-Source-lizenzierte Dienste zurückgegriffen werden.

06 Literaturverzeichnis

Agentur der Europäischen Union für Grundrechte und Europarat, Handbuch zum europäischen Datenschutzrecht, 2019, Link

BigBlueButton Inc., License, License, Link

BigBlueButton Inc., FAQs, License Link

Bundesnetzagentur, Risk levels, AI Service Desk o.J., Link

ByCS Lernplattform / Garske, Tobias / Memmel, Philipp, AI Chat, Plugins o.J., Link

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, KI-Einsatz durch die Verwaltung: Wie ist § 3a LDSG anzuwenden?, 2026, Link

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

Dixon, Fred / Federico, Jesus, BigBlueButton BN, Link

Dondorf, Thomas / Decker, Bernd / Schilling, Sebastian, Learning Analytics, Plugins o.J., Link

Dreier, Thomas, Text und Data Mining, Unterricht und Lehre, vergriffene Werke (Abs. 4–7), Urheberrechtsgesetz 2025,

Dreier, Thomas / Schulze, Gernot (Hrsg.), Urheberrechtsgesetz, 2025, Link

Erb, Volker / Schäfer, Jürger (Hrsg.), Münchener Kommentar zum StGB, 2023,

Europäische Kommission, Verordnung (EU) 2026/1744 des Europäischen Parlaments und des Rates vom 8. Juli 2026 zur Änderung der Verordnungen (EU) 2024/1689, (EU) 2018/1139 und (EU) 2023/1230 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), 2026, Link

Europäisches Parlament und Rat der Europäischen Union, Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über

einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. L 2022, Link

Europäisches Parlament und Rat der Europäischen Union, Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung), ABl. L 2024, Link

European Data Protection Board, Leitlinien zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, 2021, Link

European Data Protection Board, Datenschutzgrundlagen, Datenschutzgrundlagen oJ, Link

Geminn, Christian L. / Johannes, Paul C. / Nebel, Maxi / Bile, Tamer, Beurteilung von Learning Analytics nach Datenschutzrecht und KI-Verordnung an Hochschulen in Berlin, 2025, 1–119Link

Heckmann, Dirk / Koloßa, Stephan, Allgemeines, Cyber Resilience Act Kommentar 2025,

Heynike, Francois Maartens / Taraz, Daniel, Der Cyber Resilience Act, CCZ 2025 92 Ff 2025, 92–96

Hochschulrektorenkonferenz, Handlungsdruck für Hochschulen, Länder und Bund – HRK-Empfehlungen zur Cybersicherheit, 2025, Link

HTWG Konstanz, Nutzungsbedingungen und Datenschutzhinweise zur Nutzung von bwGPT by Kersta an der HTWG Konstanz, 2025, Link

ILIAS open source e-Learning e.V., Plugins und Erweiterungen, Plugins Link

ILIAS open source e-Learning e.V., BigBlueButton, Plugins Link

Kalbhenn, Jan Christopher, Plattformregulierung als politische Aufgabe der Zeit, ZRP 2025 111 Ff 2025, 111–114

Karlsruher Institut für Technologie (KIT), Datenschutzerklärung Videokonferenzen mit BigBlueButton (BBB), Dienste 2024, Link

Kirschke-Biller, Jonathan / Füllsack, Anna Lena, Einzelne Begriffsmerkmale, BeckOK KI-Recht 2025,

Klawonn, Thilo, Bewertung von Lernergebnissen, BeckOK KI-recht 2026, Link

Knecht, Jana, KI-Kompetenz Qualifizierungsanforderungen für Hochschulangehörige, 2025, 1–15, Handreichungen - Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg

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

Knecht, Jana, Rechtsbereichsspezifische Betrachtung von KI: KI und Datenschutz, 2025, 1–25, Link

Knecht, Jana, Rechtsbereichsspezifische Betrachtung von KI: Urheberrecht, 2025, 1–27, Link

Knecht, Jana, Verhältnis von Data Crawling und Urheberrecht im Hochschulkontext, 2026, Link

Kühling, Jürgen / Buchner, Benedikt, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, Link

Leifos GmbH, AI Assistant, Extending ILIAS by plugins 2026, Link

LG München, LG München I: Unzulässige Vervielfältigung durch Memorisierung von Werken im und durch KI-Sprachmodell - GEMA/Open AI, Gewerbl. Rechtsschutz Urheberrecht 2025, Link

Moodle Pty Ltd., Moodle Plugins directory, Moodle Plugins directory, Link

Moodle.com, Documentation, 2026, Link

open source initiative, The Open Source Definition, 2006, Link

open source initiative, GNU General Public License version 3, 2007, Link

open source initiative, GNU Lesser General Public License version 3, 2007, Link

Paschke, Anne / Fellenberg, Pauline, Einblick in die Regelungsinhalte des Cyber Resilience Act, Z. Für Eur. Daten- Informationsrecht 2025, 198–203

Podszun, Rupprecht / Bongartz, Philipp / Kirk, Alexander, Digital Markets Act – Neue Regeln für Fairness in der Plattformökonomie, Neue Juristische Wochenschr. 2022, 3249–3254

Pohl, Jan / Winter, Nico, Personenbezug als Frage der Perspektive, Z. Für Datenschutzrecht 2026, 244–250

Raue, Peter / Stang, Felix Laurin, Streaming aus technologischer Sicht, Münchener Anwalts Handbuch Urheber- und Medienrecht 2023,

Rennert, Justin, Brüssel reguliert das schon, EU-Institutionen einigen sich final auf DMA und DSA, DFN-Infobrief Recht 2022, 9–11

Roth-Isigkeit, David, Anforderungen an Hosting-Dienste, Handbuch des EU-Wirtschaftsrechts 2025,

Ruschemeier, Hannah, Bewertung von Lernergebnissen, KI-VO: Verordnung über Künstliche Intelligenz 2026,

Rux, Johannes, GG Art. 20, BeckOK Grundgesetz 2026, Link

Schlotfeldt, Andrea, Rechtsfragen rund um die Lehrveranstaltung, 2026, Link

Scholz, Friederike, Aufzeichnung von Lehrveranstaltungen, Bildungsrecht in der Corona-Krise 2021

Seckelmann, Margrit / Horstmann, Jan, Künstliche Intelligenz im Hochschulbereich und Datenschutz, Ordn. Wiss. 2024, 169–183

Spehn, Maximilian, Streaming im Rahmen hybrider Lehre, 2025, 1–21, Link

Spehn, Maximilian, Hochschulen im Kontext von Anbieter- und Betreiberpflichten, 2025, Link

Spellbrink, Wolfgang, SGB I § 31 Vorbehalt des Gesetzes, Kasseler Kommentar SGB I 2018, Link

Spies, Benjamin, Veranschaulichung von Unterricht und Lehre (Abs. 5), Urheberrecht 2026

Teichmann, Fabian, Der Cyber Resilience Act der EU, Neue Z. Für Verwaltungsrecht 20, 1662–1669

Universität Mannheim, LeAP – Learning Analytics Profiles, Area Economic and Business Education o.J., Link

Universität Stuttgart, Informationen zum Umgang mit Webex, 2021, Link

Wandtke, Artur-Axel / Bullinger, Winfried (Hrsg.), Praxiskommentar Urheberrecht, 2022, Link

Zentrale Datenschutzstelle der baden-württembergischen Universitäten, https://www.zendas.de/themen/personenbezogene_daten/ipadresse.html, ZENDAS 2017, Link

Zentrale Datenschutzstelle der baden-württembergischen Universitäten, Sind Videokonferenzdienste Telekommunikationsdienste im Sinne des TKG?, ZENDAS 2024, Link

Zentrale Datenschutzstelle der baden-württembergischen Universitäten, Übermittlung personenbezogener Daten an Drittländer, ZENDAS 2024, Link

Zentrale Datenschutzstelle der baden-württembergischen Universitäten, Zulässigkeit der Aufzeichnung von Lehrveranstaltungen, ZENDAS 2025, Link

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: *Spehn, Maximilian & Knecht, Jana*, Handreichung Digitale Anwesenheitspflicht, Rechtsinformationsstelle für die digitale Lehre (bwDigiRecht) im Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg, Karlsruhe, 2026.

bwDigiRecht ist eine Struktureinrichtung im Hochschulnetzwerk Digitalisierung der Lehre Baden-Württemberg (HND-BW) in Trägerschaft baden-württembergischer Hochschulen.

Diese Handreichung ist ausschließlich zur Nutzung durch die Trägerhochschulen bestimmt, eine Weitergabe an Dritte oder sonstige Verbreitung, ohne vorherige ausdrückliche Einwilligung der Koordination von bwDigiRecht, ist unzulässig.