

In Kraft getreten: 01.10.2026

Richtlinie zur Nutzung von Künstlicher Intelligenz (KI) und zum Einsatz von KI-Systemen an der Anton Bruckner Privatuniversität (ABU)

Version 1.0

Historie der Dokumentversionen

Version	Datum	Autor*in	Freigabe durch	Änderungsgrund / Bemerkung
0.1	März 2026	Andreas Stuhlberger, DAT		Ersterstellung
0.2	Juni 2026	Andreas Stuhlberger, DAT		Überarbeitung
1.0	September 2026	Andreas Stuhlberger, DAT Markus Grimberger, VRR Markus Neuwirth, VRF	Präsidium 18.9.2026	Erstfassung nach Überarbeitung; Ergänzung um Rechtsgrundlagen (KI-VO), unzulässige Anwendungen, Vorfallsmeldung, Übergangsbestimmungen

Inhaltsverzeichnis

Historie der Dokumentversionen..... 2

1 Präambel 3

2 Zielsetzung 3

3 Anwendungsbereich 4

4 Begriffsbestimmungen 4

5 Grundsätze der KI-Nutzung 6

6 Typisierung von KI-Systemen zur dienstlichen Nutzung..... 8

6.1 Vertraulichkeitsklassen 8

6.2 KI-System-Typen..... 9

6.3 Anonymisierte Daten 10

7 Zulässige und unzulässige Anwendungen 11

8 Transparenz & Dokumentation 12

9 Schulung & Kompetenzentwicklung 13

10 Governance & Verantwortung 14

11 Inkrafttreten und Revision..... 15

1 Präambel

Die fortschreitende Entwicklung und Verbreitung von Systemen der Künstlichen Intelligenz (KI) eröffnet neue Möglichkeiten in Lehre, Forschung, Verwaltung und Organisation. Gleichzeitig ergeben sich daraus rechtliche, ethische und sicherheitstechnische Herausforderungen, insbesondere in Hinblick auf Datenschutz, Informationssicherheit, Transparenz, wissenschaftliche Integrität und Gleichbehandlung.

Diese Richtlinie schafft einen verbindlichen Rahmen für den verantwortungsvollen, rechtskonformen und sicheren Einsatz von KI-Systemen an der Anton Bruckner Privatuniversität (ABU). In ihrer ersten Ausbaustufe regelt sie den Einsatz von KI-Systemen im Verwaltungsbereich. Für die Nutzung von KI in Lehre, Studium, Prüfungswesen sowie in Forschung und künstlerischer Entwicklungsarbeit sind gesonderte Regelungen vorgesehen.

Diese Richtlinie konkretisiert insbesondere die Verpflichtungen gemäß Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (KI-Verordnung) in der aktuell gültigen Fassung. Die ABU ist Betreiberin von KI-Systemen im Sinne des Art. 3 Z 4 KI-Verordnung. Soweit sie KI-Systeme selbst entwickelt und unter eigenem Namen einsetzt, treffen sie zusätzlich die Pflichten eines Anbieters im Sinne des Art. 3 Z 3 der KI-Verordnung.

2 Zielsetzung

Ziel dieser Richtlinie ist es,

- die Pflichten der ABU als Betreiberin von KI-Systemen nach der Verordnung (EU) 2024/1689 (KI-Verordnung) in Bezug auf die organisatorische Umsetzung zu spezifizieren,
- einen klaren Orientierungsrahmen für den zulässigen Einsatz von KI-Systemen in der Verwaltung zu schaffen,
- die Einhaltung datenschutzrechtlicher und informationssicherheitsrechtlicher Vorgaben sicherzustellen,
- Risiken für Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu minimieren,
- Transparenz im Umgang mit KI-gestützten Verfahren herzustellen,

- Sensibilisierung und Kompetenzaufbau im Bereich KI zu fördern.

Die Richtlinie soll Rechtssicherheit für Mitarbeiter*innen schaffen und gleichzeitig Innovationsfähigkeit fördern.

Das Inkrafttreten dieser Richtlinie begründet keine Verpflichtung zur Nutzung von KI-Systemen. Die Nutzung ist grundsätzlich freiwillig und wird nicht erwartet; aus der Nichtnutzung dürfen keine Nachteile erwachsen. Ordnet eine vorgesetzte Stelle die Nutzung eines KI-Systems an, so trägt sie die vollumfängliche Verantwortung für die Zulässigkeit der Anordnung nach Maßgabe dieser Richtlinie.

3 Anwendungsbereich

Diese Richtlinie gilt für die Angehörigen der ABU gemäß § 24 Abs. 1 lit. c (Verwaltungspersonal) der Satzung der ABU. Sie gilt für jene OÖ. Landesbediensteten, die gemäß § 9 des Landesgesetzes über die Rechtsstellung des Bruckner-Konservatoriums zum Betrieb einer Privatuniversität, LGBI Nr. 14/2003, dem Bruckner-Konservatorium zur dauernden Dienstleistung im Bereich der Verwaltung zugewiesen wurden nur insoweit, als sie nicht mit den Bestimmungen des Landes OÖ (insbesondere § 4a OÖ. LVBG bzw. § 3a OÖ. LBG, dem OÖ. Archivgesetz und den darauf basierenden Regelungen) im Widerspruch stehen. Die genannten Personen werden in der Folge zusammenfassend als „Mitarbeiter*innen“ bezeichnet.

4 Begriffsbestimmungen

- **KI-System** gemäß Art. 3 Z 1 der KI-Verordnung bezeichnet ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist, das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können. Nicht als KI-System im Sinne dieser Richtlinie gelten einfache regelbasierte Programme ohne lernende oder probabilistische Komponenten.

- **Generative KI**

bezeichnet KI, die als Antwort auf einen Prompt oder die Anfrage eines Benutzers Inhalte wie Texte, Bilder, Video, Audio, Softwarecode oder strukturierte Daten generiert. Die Generierung erfolgt typischerweise auf Grundlage statistischer oder neuronaler Modelle, die auf umfangreichen Trainingsdaten basieren. Generative KI wird insbesondere zur Erstellung von Texten, Entwürfen, Zusammenfassungen, Analysen, Visualisierung oder Programmcode eingesetzt.

- **Personenbezogene Daten** gemäß Art 4 Abs. 1 DSGVO

bezeichnet „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“

- **Pseudonymisierung** gemäß Art 4 Z 5 DSGVO

bezeichnet „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“

- **Anonymisierung**

Bei der Anonymisierung fehlt die in der Pseudonymisierung erwähnte Zusatzinformation. Die Rückverfolgung ist somit nicht mehr möglich und ein Personenbezug nicht länger gegeben.

- **Anbieter** gemäß Art. 3 Z 3 KI-VO

ist eine natürliche oder juristische Person, die ein KI-System entwickelt oder entwickeln

lässt und es unter eigenem Namen oder eigener Handelsmarke in Verkehr bringt oder in Betrieb nimmt.

- **Betreiber** gemäß Art. 3 Z 4 KI-VO
ist eine natürliche oder juristische Person, die ein KI-System in eigener Verantwortung im Rahmen einer beruflichen Tätigkeit verwendet.
- **KI-Kompetenz** gemäß Art. 3 Z 56 KI-VO
bezeichnet Fähigkeiten, Kenntnisse und Verständnis, die es ermöglichen, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken bewusst zu werden.
- **Halluzination**
ist die sachlich unzutreffende (jedoch möglicherweise sprachlich plausibel formulierte) Ausgabe eines KI-Systems.

5 Grundsätze der KI-Nutzung

- KI-Systeme sind als unterstützende Werkzeuge einzusetzen. Sie dienen der Assistenz und Effizienzsteigerung. Sie dürfen und können jedoch menschliches Urteilsvermögen, fachliche Bewertung oder Entscheidungsverantwortung nicht ersetzen. Die Verantwortung für das Arbeitsergebnis verbleibt bei der handelnden Person; ordnet eine vorgesetzte Stelle die Nutzung eines bestimmten KI-Systems an, trägt sie die vollumfängliche Verantwortung für die Zulässigkeit dieser Anordnung.
- Der Schutz von Persönlichkeitsrechten sowie von vertraulichen und schutzwürdigen Informationen hat oberste Priorität. Vor der Nutzung eines KI-Systems ist zu prüfen, welche Daten in das jeweilige System eingegeben werden dürfen. Hierbei sind insbesondere die Vorgaben der „KI-Systemtyp / Vertraulichkeitsklassen-Matrix“ zu berücksichtigen. Alternativ können als Grundlage das Dokument „Whitelist für die unterschiedlichen Typen von KI-Systemen“ oder eine schriftliche Freigabe durch den Datenschutzbeauftragten bzw. den/die Datenschutzkoordinator*in dienen. Die Verantwortung für die Einhaltung dieser Vorgaben liegt bei der Person, die das KI-System nutzt.

- Die Verantwortung für Qualität, Richtigkeit und Rechtmäßigkeit von Inhalten, die unter Einbindung von KI-Systemen erstellt werden, liegt bei den Mitarbeiter*innen. KI-generierte Inhalte sind vor ihrer Verwendung eigenständig und kritisch zu prüfen.
- Der Einsatz von KI-Systemen erfolgt transparent und nachvollziehbar. Soweit gesetzlich erforderlich oder für Betroffene relevant, werden diese über den Einsatz von KI informiert.
- Der Einsatz von KI hat verhältnismäßig und zweckgebunden zu erfolgen. KI-Systeme dürfen nur dann verwendet werden, wenn ihr Einsatz einen sachlichen Mehrwert bietet und die verbleibenden Risiken für Datenschutz, Informationssicherheit und Grundrechte durch die Vorgaben dieser Richtlinie und ergänzende Maßnahmen auf ein vertretbares Maß begrenzt sind..
- Der Einsatz von KI-Systemen muss ethisch vertretbar sein und darf keine Diskriminierung, Voreingenommenheit oder andere unerwünschte Auswirkungen auf Studierende, Mitarbeiter*innen oder Nutzer*innen bzw. Dritte haben. Die Nutzung von KI-Systemen darf nicht zu ungleicher Behandlung führen.
- Die ABU stellt ihren Mitarbeiter*innen die erforderlichen Informationen für eine sichere, verantwortungsvolle, ethisch vertretbare und rechtskonforme Nutzung von KI-Systemen zur Verfügung. Sie bietet unterstützende Schulungsmaßnahmen an und benennt eine zentrale Ansprechstelle für Fragen im Zusammenhang mit der Nutzung von KI-Systemen.
- Entscheidungen, die gegenüber Personen rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen, dürfen nicht ausschließlich auf einer automatisierten Verarbeitung einschließlich Profiling beruhen (Art. 22 DSGVO). Ergebnisse von KI-Systemen dürfen solche Entscheidungen vorbereiten, nicht jedoch ersetzen; die inhaltliche Prüfung und die Entscheidung selbst sind von einer dafür zuständigen Person vorzunehmen und nachvollziehbar zu dokumentieren.
- Die urheber- und leistungsschutzrechtlichen Anforderungen an die Eingabe fremder Werke in KI-Systeme sowie an die Verwendung KI-generierter Ergebnisse werden in einer gesonderten Richtlinie geregelt. Bis zu deren Inkrafttreten sind die Rechte Dritter jedenfalls zu wahren; in Zweifelsfällen ist vor der Eingabe geschützten Materials Rücksprache zu halten.

6 Typisierung von KI-Systemen zur dienstlichen Nutzung

6.1 Vertraulichkeitsklassen

- **C1: Öffentlich**

Definition: Daten sind für jedermann, auch außerhalb der ABU, zugänglich.

Beispiele: Inhalte der öffentlichen Website, Publizierungen, Stellenausschreibungen, allgemein zugängliche Studienpläne

- **C2: Intern**

Definition: Daten sind lediglich den Mitarbeiter*innen der ABU zugänglich.

Beispiele: Internes Rundschreiben, Unterlagen in „V:\(Alle)“, allgemeine Organisationsunterlagen, Entwürfe von Richtlinien

- **C3: Vertraulich**

Definition: Daten sind lediglich einer begrenzten Anzahl an Mitarbeiter*innen zugänglich.

Beispiele: Bewerbungsunterlagen, Personalakten, Kalkulationen, Prüfungsaufgaben vor dem Prüfungstermin, Vertragsentwürfe, Gutachten, Unterlagen zu Förder- und Sponsoringverhandlungen

- **C4: Streng vertraulich**

Definition: Daten sind lediglich punktuell und ausschließlich bestimmten definierten Personen zugänglich. Die Weitergabe könnte die ABU nachhaltig schädigen.

Beispiele: Daten zu laufenden arbeitsrechtlichen oder gerichtlichen Verfahren, Sicherheitslücken, Zugangsdaten, kryptographische Schlüssel, Meldungen nach dem Hinweisgeber*innenschutz

Enthält ein Dokument oder ein Sachverhalt Informationen unterschiedlicher Vertraulichkeitsklassen, ist die höchste enthaltene Klasse maßgeblich.

Bestehen Zweifel hinsichtlich der Zuordnung zu einer Vertraulichkeitsklasse, ist die nächsthöhere Klasse anzunehmen. Zweifelsfragen können der*dem KI-Beauftragten zur Klärung vorgelegt werden; die Klärung kann anonymisiert als Anwendungsbeispiel in die Whitelist aufgenommen.

6.2 KI-System-Typen

- **Universitätseigene KI-Systeme (Typ 1):**

KI-Systeme, die vollständig von und innerhalb der ABU betrieben werden und bei denen ausgeschlossen ist, dass Daten in externe Systeme abfließen. Diese KI-Systeme verarbeiten Daten ausschließlich innerhalb universitärer Infrastruktur und dürfen nach Freigabe des Systems durch das Rektorat für die Eingabe von Informationen aller Vertraulichkeitsklassen einschließlich streng vertraulicher Informationen (C4) verwendet werden.

Diese Systeme müssen über entsprechende technische Maßnahmen verfügen, um zu gewährleisten, dass sensible Daten nicht in Logdateien, Telemetrie oder Backups ungeschützt gespeichert werden. Zugriff auf das System ist ausschließlich autorisierten Personen vorbehalten.

- **Vertraglich eingebundene externe KI-Systeme mit datenschutzfreundlichen Einstellungen und Enterprise-Verträgen (z. B. Academic AI) (Typ 2):**

KI-Systeme, die von externen Anbietern betrieben werden und deren Nutzung auf Grundlage einer vertraglichen Vereinbarung mit der ABU (insbesondere Auftragsverarbeitungsvertrag) erfolgt. Die Anmeldung wird mithilfe des Universitätsaccounts durchgeführt und bietet standardmäßig datenschutzfreundliche Voreinstellungen. Mitarbeiter*innen dürfen Informationen der Vertraulichkeitsklassen C1 und C2 in diese Systeme eingeben. Die Verarbeitung der Vertraulichkeitsklasse C3 ist erlaubt, sofern eine entsprechende Risikobewertung durch den Datenschutzbeauftragten oder Datenschutzkoordinator*in durchgeführt wurde. Eine Eingabe von Informationen der Vertraulichkeitsklassen C4 ist nicht erlaubt.

- **Nicht geprüfte öffentliche KI-Systeme (z.B. Chat GPT Free) (Typ 3):**

Mitarbeiter*innen dürfen nur Informationen der Vertraulichkeitsklasse C1 in diese Systeme eingeben. Die Eingabe von Informationen der Vertraulichkeitsklassen C2, C3 und C4 ist strikt untersagt.

6.3 Anonymisierte Daten

Die Eingabe von Daten, die zuvor vollständig und irreversibel anonymisiert wurden, ist zulässig, sofern eine Re-Identifizierung betroffener Personen auch unter Berücksichtigung zusätzlicher verfügbarer Informationen ausgeschlossen werden kann.

Pseudonymisierte Daten gelten nicht als anonymisiert.

Die Anonymisierung beseitigt den Personenbezug, nicht jedoch die Vertraulichkeit der Information. Die Einstufung nach Kapitel 6.1 bleibt unberührt; anonymisierte Inhalte der Klassen C3 und C4 unterliegen weiterhin den Beschränkungen der Matrix.

Bestehen Zweifel am Ausschluss der Re-Identifizierung, ist von einer Anonymisierung nicht auszugehen.

6.4 KI-Funktionen in bestehenden Anwendungen und Systeme mit eigenständigem Datenzugriff

(1) KI-Funktionen werden zunehmend in bereits eingesetzte Anwendungen integriert oder greifen eigenständig auf Postfächer, Dateiablagen, Kalender, Besprechungsinhalte oder Webinhalte zu. In diesen Fällen erfolgt keine bewusste Eingabe durch die Mitarbeiter*innen.

(2) Die Aktivierung solcher Funktionen erfolgt ausschließlich zentral durch die zuständige Organisationseinheit für IT nach dem Verfahren gemäß Kapitel 11. Die eigenmächtige Aktivierung durch Mitarbeiter*innen ist unzulässig.

(3) Maßgeblich für die Zulässigkeit ist die höchste Vertraulichkeitsklasse jener Daten, auf die die Funktion zugreifen kann – nicht jene der jeweils bearbeiteten Datei.

(4) Die automatisierte Aufzeichnung, Transkription, Zusammenfassung oder Auswertung von Besprechungen ist nur zulässig, wenn alle Teilnehmenden vorab darüber informiert wurden.

Sitzungen sowie Besprechungen mit Inhalten der Vertraulichkeitsklasse C3 bedürfen einer Prüfung und Freigabe durch den Datenschutzkoordinator und/oder Datenschutzbeauftragten, jene mit Vertraulichkeitsklasse C4 dürfen nicht KI-gestützt verarbeitet werden.

7 Zulässige und unzulässige Anwendungen

7.1 Matrix / Vertraulichkeitsklassen

Folgende Matrix zeigt, welche Informationen welcher Vertraulichkeitsklasse in welche Typen von KI-Systemen eingegeben werden dürfen und in welchen Fällen zuvor eine zusätzliche Prüfung erforderlich ist. Der konkrete Anwendungsfall ist jeweils zulässig, wenn die gewählte Kombination von Systemtyp und Vertraulichkeitsklasse dies erlaubt.

Solang unklar ist, welchem Typ ein KI-System zuzuordnen ist, dürfen nur öffentliche Daten (C1) in dieses KI-System eingegeben werden.

KI-Systemtyp / Vertraulichkeitsklasse	Typ 1	Typ 2	Typ 3
C1 – Öffentlich	✓ erlaubt	✓ erlaubt	✓ erlaubt
C2 – Intern	✓ erlaubt	✓ erlaubt	● nicht erlaubt
C3 – Vertraulich	✓ erlaubt	Prüfung erforderlich	● nicht erlaubt
C4 – Streng vertraulich	✓ erlaubt	● nicht erlaubt	● nicht erlaubt

7.2 Jedenfalls unzulässige Anwendungen

Unabhängig von Systemtyp und Vertraulichkeitsklasse sind unzulässig:

- der Einsatz von KI-Systemen zur Ableitung von Emotionen von Mitarbeiter*innen oder Studierenden (Art. 5 KI-VO);
- die biometrische Kategorisierung von Personen sowie Systeme zur sozialen Bewertung von Personen (Art. 5 KI-VO);
- die KI-gestützte Leistungs- oder Verhaltenskontrolle von Mitarbeiter*innen;

- d) das Treffen von Entscheidungen mit rechtlicher Wirkung oder erheblicher Beeinträchtigung für Personen ausschließlich auf Grundlage automatisierter Verarbeitung (Art. 22 DSGVO);
- e) die Eingabe von Zugangsdaten, kryptographischen Schlüsseln und vergleichbaren Sicherheitsinformationen in KI-Systeme jeglichen Typs;
- f) die Eingabe von Meldungen und Unterlagen aus dem Hinweisgeber*innensystem sowie von Unterlagen zu laufenden arbeitsrechtlichen oder gerichtlichen Verfahren in KI-Systeme der Typen 2 und 3.

8 Transparenz & Dokumentation

- **Die Transparenzpflichten des Art. 50 KI-Verordnung sind einzuhalten.**

Insbesondere gilt:

- Werden KI-Systeme eingesetzt, die unmittelbar mit natürlichen Personen interagieren (etwa Chatbots auf der Website der ABU), ist sicherzustellen, dass diese Personen darüber informiert werden, dass sie mit einem KI-System interagieren.
- KI-generierte oder KI-manipulierte Bild-, Ton- und Videoinhalte, die bestehenden Personen, Gegenständen oder Ereignissen täuschend ähnlich sind, sind als künstlich erzeugt oder manipuliert offenzulegen.
- KI-generierte Texte, die veröffentlicht werden, um die Öffentlichkeit über Angelegenheiten von öffentlichem Interesse zu informieren, sind als KI-generiert offenzulegen, es sei denn, die Inhalte wurden einer menschlichen Überprüfung unterzogen und eine Person der ABU trägt die redaktionelle Verantwortung.

- **Grundsatz:** Der Einsatz von KI-Systemen ist so transparent zu gestalten, dass für Betroffene nachvollziehbar ist, wann, wie und mit welchem Zweck KI genutzt wurde. Wird KI-generierter Inhalt ohne menschliche Prüfung direkt weiterverwendet oder zur Beantwortung von Anfragen eingesetzt, etwa im Kontakt mit Studierenden oder externen Personen, muss dies klar zu erkennen sein.

- **Geringfügige Nutzung:** Wird ein KI-System nur in geringem Umfang genutzt (z. B. zur Einholung von Formulierungsvorschlägen, Rechtschreib- oder Grammatikhilfe, Layout- oder Strukturvorschlägen), ist keine gesonderte Kennzeichnung erforderlich, sofern die KI-Nutzung nicht Inhalt oder Ergebnis wesentlich geprägt hat.
- **Substanzielle Nutzung:** Bei der Nutzung von KI-Systemen, die einen wesentlichen Anteil am Ergebnis haben (z. B. KI-generierte Bilder, Veröffentlichung eines KI-generierten Textes ohne persönliche Anpassung), ist die Verwendung der KI eindeutig zu dokumentieren. Diese Dokumentation sollte mindestens folgende Angaben enthalten: Betreiber, eingesetztes KI-System / Tool, Modell (z. B. „OpenAI – ChatGPT – GPT-5“), Zweck der Nutzung (z. B. „Zusammenfassung der Kapitel 3 bis 5“). Diese Angaben stellen sicher, dass die Arbeit oder der Inhalt für Dritte nachvollziehbar bleibt.
- **Prozessdokumentation:** KI-Gestützte Prozesse, insbesondere wenn KI in Abläufe oder automatisierbare Auswertungen eingebunden wird, sind entsprechend zu dokumentieren. Diese Dokumentation dient der Nachvollziehbarkeit, Verantwortungszuweisung und ggf. späteren Revisionen der Vorgehensweise.

9 Schulung & Kompetenzentwicklung

Mitarbeiter*innen sollen in die Lage versetzt werden, KI-Systeme sicher, verantwortungsvoll, ethisch vertretbar und rechtskonform zu nutzen. Der Umgang mit KI-Systemen erfordert neben technischem Verständnis auch Wissen über Datenschutz, Informationssicherheit, Urheberrecht, akademische Integrität und ethische Fragestellungen.

Die Universität stellt regelmäßige Schulungen, Workshops oder E-Learning-Module zur Verfügung. Inhalte umfassen mindestens:

- die Funktionsweise von KI-Systemen,
- Vertraulichkeits- und Datenschutzerfordernungen,
- Risiken, Biases, Halluzination, Diskriminierung und Fehlanwendungen von KI,
- Richtige Kennzeichnung und Dokumentation der KI-Nutzung und

- Handlungsempfehlungen für unterschiedliche KI-Systemtypen.

10 Governance & Verantwortung

- Die Verantwortung für die richtlinienkonforme Nutzung von KI-Systemen liegt bei den nutzenden Mitarbeiter*innen. Wurde die Nutzung durch eine vorgesetzte oder übergeordnete Stelle angeordnet, trägt diese die Verantwortung für die Zulässigkeit der Anordnung.
- Das Rektorat benennt eine zentrale Ansprechperson als „KI-Beauftragte/n“. Diese ist zuständig für die Ausarbeitung und Weiterentwicklung von Richtlinien im Zusammenhang mit der Nutzung von KI-Systemen, die Organisation und Durchführung von Schulungen für Mitarbeiter*innen, die Vorabprüfung und fachliche Bewertung neuer KI-Systeme vor deren Einführung und Inbetriebnahme, die Einstufung von KI-Systemen gemäß der festgelegten Typen- und Vertraulichkeitsmatrix, die Durchführung bzw. Koordination von Risikobewertungen im Zusammenhang mit dem Einsatz von KI-Systemen sowie die Planung und Durchführung regelmäßiger Audits zur Überprüfung der Einhaltung dieser Richtlinie.
- In der „Whitelist für die unterschiedlichen Typen von KI-Systemen“, einem von dem*der KI-Beauftragten gepflegten, fortlaufend aktualisierten Dokument, werden die vom Rektorat freigegeben KI-Systeme aufgeführt. Zusätzlich zu den Systemen werden außerdem Fallbeispiele und deren Einstufung bzw. Freigabe gepflegt. Dieses Dokument kann jederzeit von Mitarbeiter*innen eingesehen werden.
- Die Einführung eines neuen KI-Systems erfordert die verpflichtende Einbindung der*des KI-Beauftragten, der Stabsstelle Datenschutz und Informationssicherheit sowie der zuständigen Organisationseinheit für IT (ZID). Im Rahmen dieses Prüfprozesses sind insbesondere datenschutzrechtliche, informationssicherheitsrechtliche, technische und organisatorische Anforderungen zu bewerten. Die formale Freigabe zur Einführung und zum produktiven Einsatz des KI-Systems erfolgt durch das Rektorat.

- **Meldung und Konsequenzen von Vorfällen**

- Wird festgestellt oder besteht der Verdacht, dass Informationen entgegen dieser Richtlinie in ein KI-System eingegeben wurden, dass ein KI-System unbefugt auf Daten der ABU zugegriffen hat oder dass ein KI-gestütztes Ergebnis zu nachteiligen Auswirkungen geführt hat, ist dies unverzüglich, längstens innerhalb von 24 Stunden, der Stabsstelle Datenschutz und Informationssicherheit sowie der bzw. dem*der KI-Beauftragten zu melden.
Die Meldung erfolgt an datenschutz@bruckneruni.at bzw. ki@bruckneruni.at.
- Die unverzügliche Selbstmeldung ist ausdrücklich erwünscht. Sie wird bei der Beurteilung allfälliger Konsequenzen zugunsten der meldenden Person berücksichtigt.
- Betrifft der Vorfall personenbezogene Daten, prüft die Stabsstelle Datenschutz und Informationssicherheit unverzüglich, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt, und veranlasst erforderlichenfalls die Meldung an die Datenschutzbehörde gemäß Art. 33 DSGVO sowie die Verständigung der betroffenen Personen gemäß Art. 34 DSGVO.
- Vorfälle werden dokumentiert und in anonymisierter Form in die Weiterentwicklung der Schulungsinhalte und der Whitelist einbezogen.
- Verstöße gegen diese Richtlinie können dienst- und arbeitsrechtliche Konsequenzen nach sich ziehen. Die Bestimmungen der Dienstordnung der ABU sowie die allgemeinen arbeitsrechtlichen Vorschriften bleiben unberührt. Bei erstmaligen und fahrlässigen Verstößen stehen die Beratung und Schulung im Vordergrund.

11 Inkrafttreten und Revision

(1) Die vorliegende Richtlinie tritt mit 01.10.2026 in Kraft.

(2) Innerhalb von drei Monaten ab Inkrafttreten sind alle zum Zeitpunkt des Inkrafttretens bereits dienstlich genutzten KI-Systeme der bzw. dem KI-Beauftragten zu melden. Diese Meldung bleibt ohne dienstrechtliche Folgen. Nach Ablauf der Frist ist die dienstliche Nutzung nicht gemeldeter und nicht freigegebener KI-Systeme unzulässig.

(3) Solange die Whitelist nicht veröffentlicht ist, gilt jedes nicht ausdrücklich freigegebene KI-System als System des Typs 3.

(4) Diese Richtlinie wird mindestens einmal jährlich zu Beginn des Studienjahres sowie anlassbezogen bei wesentlichen Änderungen der Rechtslage, insbesondere der KI-Verordnung, auf ihre Gültigkeit überprüft und bei Bedarf angepasst. Die erste Überprüfung erfolgt spätestens sechs Monate nach Inkrafttreten.

(5) Vorschläge, Anwendungsbeispiele oder Fragen zur Weiterentwicklung der Richtlinie oder deren Anwendung können an die E-Mail-Adresse ki@bruckneruni.at gerichtet werden.