



University of
Applied Sciences

Allgemeine KI-Richtlinie für Mitarbeiter*innen und NBL

Recht & Verträge / IT Services

Datum 28.08.2026

FHR-1-0092_Vers. 02_Rev. 00

Medieninhaber und Herausgeber

IMC Hochschule für Angewandte Wissenschaften Krems GmbH

Piaristengasse 1

3500 Krems, Austria, Europe

+43 2732 802

office@imc.ac.at

www.imc.ac.at



Änderungen zur Vorversion

Ergänzung Transparenzpflichten und Aufzeichnung/Protokollierung von Gesprächen mit Hilfe von KI Tools.



Inhaltsverzeichnis

Änderungen zur Vorversion	2
1 Einleitung	5
1.1 Zweck	5
1.2 Geltungsbereich	6
1.3 Verpflichtung zur Einhaltung der Gesetze	6
1.4 Eigenverantwortung	7
1.5 Vermeidung von Diskriminierung	7
1.6 Konsequenzen	8
1.7 Abkürzungen	8
2 Grundsätze des KI-Einsatzes	9
2.1 Nutzer*innen Verantwortung	9
2.2 Rechtmäßigkeit und Transparenz	9
2.3 Datenschutz und Betriebs- und Geschäftsgeheimnisse	11
2.4 Urheberrecht & Co	12
2.5 KI-Katalog des IMC Krems	13
2.6 Risikoanalyse und -management	13
2.7 Forschung und Entwicklung	13
2.8 Beurteilung von Studierendenleistungen	14
2.9 KI-Einsatz im Bewerbungsprozess und bei Aufnahmen	14
3 Referenzen	15
3.1 Mitgeltende Unterlagen	15
4 Gesetzliche Vorgaben	15
5 Anhang	16
5.1 Begriffsdefinition	16



5.2 Risikoabschätzung beim Einsatz von KI-Werkzeugen im Organisationsalltag	18
Keines oder geringes Risiko	18
Begrenztes Risiko	19
Hohes Risiko	19
Verbotene Praktiken	20



1 Einleitung

1.1 Zweck

Innovation ist einer der Kerne der Strategie des IMC Krems. In diesem Sinne steht das IMC Krems dem verantwortungsvollen Einsatz von Künstlicher Intelligenz (KI) in sämtlichen Bereichen offen gegenüber. Die Richtlinie dient dazu, um eine einheitliche und richtige Anwendung von KI-Systemen am IMC Krems zu gewährleisten und stellt die Verantwortlichkeiten in diesem Zusammenhang dar.

In den folgenden Bestimmungen sollen ausgewählte wichtige Punkte für den Einsatz von KI aufgezeigt werden, jedoch bleibt in jedem Fall die KI verwendende Person dafür verantwortlich, dass die KI-Verwendung in Übereinstimmung mit bestehenden Gesetzen, IMC-Richtlinien und gemäß der guten wissenschaftlichen Praxis erfolgt. Der Mensch trägt die Verantwortung für das Ergebnis, unabhängig von der Art der verwendeten Werkzeuge.

Die Hochschule nimmt regelmäßige Überprüfung und Anpassung dieser Richtlinie vor. Darüber hinaus werden notwendige Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter*innen und Studierende bereitgestellt.

Diese Richtlinie wurde unter Zuhilfenahme von KI-Werkzeugen erstellt. Konkret kam dabei M365 Copilot als auch die „Editor“-Funktion von Microsoft Word zur Verwendung, um für eine schriftliche Prägnanz und einfache Lesbarkeit zu sorgen.



1.2 Geltungsbereich

Sobald etwas im Namen des IMC Krems geschrieben wird oder Inhalte/Daten des IMC Krems verarbeitet werden ist diese Richtlinie anzuwenden.

Es wird darauf hingewiesen, dass die Richtlinie FHR-5-004 'Richtlinie zur Verwendung von KI durch Studierende' abweichende und zum Teil strengere Regelungen, insbesondere zum Verbot der Text- und Medienerstellung, enthält. Die genannte Richtlinie gilt ausschließlich für Studierende und somit grenzen sich die Geltungsbereiche dieser beiden Richtlinien streng voneinander ab.

Diese Richtlinie tritt mit Veröffentlichung in Kraft.

	ÖSTERREICH / AUSTRIA	TPP
Studierende	Nein	Nein
Mitarbeitende	Ja	Nein
Lehrende (NBL)	Ja	Nein
INFORMATION		
Gültig ab	28.08.2026	
Kohorte		
Studiengang		
...	...	

1.3 Verpflichtung zur Einhaltung der Gesetze

Diese Richtlinie soll den verantwortungsvollen und gesetzeskonformen Einsatz von Künstlicher Intelligenz (KI) am IMC Krems gewährleisten. Der Einsatz von KI-Werkzeugen hat sich in Lehre, Forschung und Verwaltung als wertvoll erwiesen, bringt jedoch auch Herausforderungen in Bezug auf Datenschutz, ethische Verantwortung

und den Schutz personenbezogener und sensibler Daten mit sich. Diese Richtlinie orientiert sich an den Vorgaben der Datenschutz-Grundverordnung (DSGVO), dem EU AI Act und weiteren relevanten österreichischen und europäischen Rechtsvorschriften.

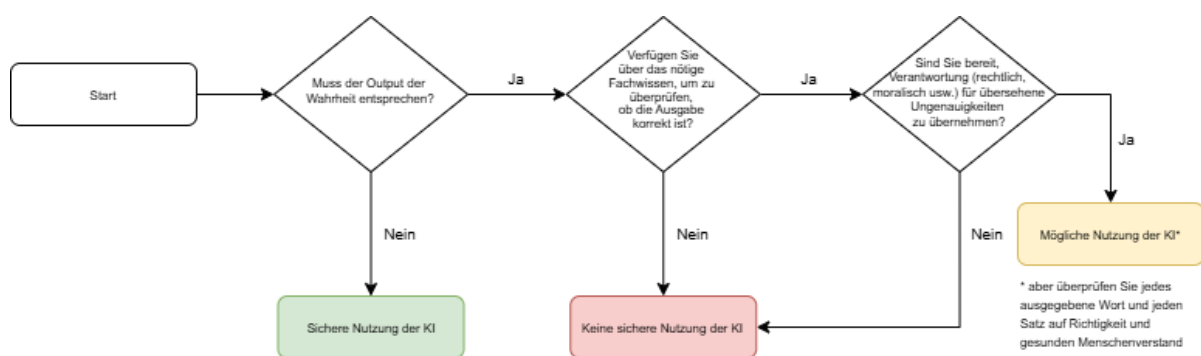
1.4 Eigenverantwortung

Die Hochschule verankert Innovation als zentralen Bestandteil ihrer Strategie und befürwortet den verantwortungsvollen Einsatz von KI in sämtlichen Bereichen. Dies ist nur möglich, wenn sämtliche Stakeholder (Lehrende, Forschende und Verwaltung) Eigenverantwortung für den Einsatz von KI übernehmen.

Die Verantwortung für die Richtigkeit von Texten oder Medien liegt nach wie vor bei der*dem Verwender*in. Derzeit verfügbare KI-Modelle produzieren regelmäßig Inhalte, die falsch sind. Dies ist bei der Verwendung zu beachten. Sämtliche Ergebnisse müssen kritisch auf inhaltliche Richtigkeit und ethische Angemessenheit geprüft werden.

Folgendes Flowchart liefert ein gutes Beispiel für die Abwägungsschritte, welche vor Verwendung einer KI vollzogen werden sollen:

Abbildung 1: Abwägung Einsatz von KI-System



Quelle: Eigene Darstellung nach Tulkanov (2023)

1.5 Vermeidung von Diskriminierung

KI-Systeme müssen so entwickelt und eingesetzt werden, dass sie keine diskriminierenden Entscheidungen treffen. Die Hochschule verpflichtet sich zur Einhaltung der ethischen Grundsätze der Fairness, Nicht-Diskriminierung und Inklusion.



1.6 Konsequenzen

Werden fremde Rechte durch das Ergebnis einer KI-Verwendung verletzt, so haftet man für diese Verletzung, als hätte man sie selbst begangen. Dies betrifft insbesondere Urheberrechte und Markenrechte.

1.7 Abkürzungen

ABKÜRZUNG	BEZEICHNUNG
DSGVO	Datenschutz-Grundverordnung
KI	Künstliche Intelligenz

2 Grundsätze des KI-Einsatzes

2.1 Nutzer*innen Verantwortung

Alle Nutzer*innen sind dafür verantwortlich, sich mit den geltenden Vorschriften zum Datenschutz und zur Nutzung von KI-Werkzeugen vertraut zu machen. Verstöße gegen diese Richtlinie können disziplinarische Maßnahmen nach sich ziehen.

Die Nutzer*innen von KI-Tools sind selbst dafür verantwortlich, dass dies in Übereinstimmung mit den jeweiligen Nutzungsbedingungen dieser Tools erfolgt. Dabei ist zu beachten, dass eine Verwendung zu Arbeitszwecken am IMC Krems in der Regel eine gewerbliche Nutzung darstellt. Die gewerbliche Nutzung von „Gratis-Lizenzen“ ist in den Nutzungsbedingungen oftmals untersagt oder mit besonderen Auflagen verbunden. Für die Nutzung von privat erworbenen Tools kann vom IMC Krems keine Haftung übernommen werden.

Bei allen erlaubten (KI-Katalog) und darüber hinaus genehmigten KI-Tools kann die IMC-E-Mailadresse zur Anmeldung verwendet werden. Bei kostenpflichtigen Tools sind die üblichen Anforderungs- und Freigabe Prozesse einzuhalten (siehe Prozess FHP-1-0040 „Software anfordern“).

2.2 Rechtmäßigkeit und Transparenz

Die Nutzung von KI muss stets gemäß den geltenden Gesetzen erfolgen, insbesondere in Übereinstimmung mit der DSGVO und dem EU AI Act, dessen Transparenzpflichten nach Art. 50 seit 2. August 2026 anwendbar sind. Es ist sicherzustellen, dass der Einsatz von KI-Werkzeugen transparent ist und die betroffenen Personen über die Nutzung informiert werden.

Nicht jeder mit Unterstützung von KI erstellte Inhalt ist zu kennzeichnen. Eine Kennzeichnungspflicht besteht in drei Fallgruppen: erstens bei Chatbots und Sprachassistenten in der Kommunikation mit Studierenden, Bewerber*innen und Partnerinstitutionen, wobei der Hinweis in der ersten Nachricht des Dialogs zu erteilen ist; zweitens bei fotorealistischen Bildern, Videos und Stimmen, die reale Personen, Orte oder Ereignisse abbilden oder abzubilden scheinen, obwohl die dargestellte Situation nicht stattgefunden hat (z.B. generierte Campus- und Lehrsituationen mit Personen, KI-Avatare, Stimmklone, Retuschen mit verändertem Aussagegehalt); drittens bei veröffentlichten Texten zu Angelegenheiten von öffentlichem Interesse –



etwa aus den Bereichen Bildung, Wissenschaft, Gesundheit, Wirtschaft oder Politik –, die ohne inhaltliche Prüfung veröffentlicht werden; erfasst sind auch automatisierte Übersetzungen und automatisiert erzeugte Meldungen.

Bei Texten entfällt die Kennzeichnung, wenn zwei Voraussetzungen kumulativ erfüllt sind: Der Inhalt wurde vor der Veröffentlichung inhaltlich geprüft – auf Richtigkeit, Plausibilität und Quellen, mit der tatsächlichen Möglichkeit der Änderung oder Ablehnung –, und eine benannte Person trägt die redaktionelle Verantwortung für die Veröffentlichung. Eine reine Rechtschreib- oder Formalprüfung genügt nicht. Diese Ausnahme gilt ausschließlich für Texte; Bilder, Videos und Audioinhalte sind stets eigenständig zu beurteilen.

Keiner Kennzeichnung bedürfen insbesondere die interne Nutzung (E-Mails, Protokolle, Präsentationen, Entwürfe, Recherchen und Zusammenfassungen), der Einsatz von KI zur Korrektur oder Verbesserung selbst geschriebener Texte (z.B. Microsoft Editor, DeepL), Anwendungen in der Verwaltung wie interne Übersetzungen und Datenanalysen sowie erkennbar künstliche Illustrationen, Symbolbilder und Grafiken ohne Realitätsbezug. Ebenso wenig kennzeichnungspflichtig ist Bildbearbeitung, die den Aussagegehalt nicht verändert (Farbkorrektur, Helligkeit, Zuschchnitt).

Der Hinweis – etwa „Mit KI erzeugtes Bild“ – muss spätestens zum Zeitpunkt der ersten Wahrnehmung erkennbar sein, unmittelbar am Inhalt platziert werden, in verständlicher Sprache abgefasst und barrierefrei zugänglich sein. Ein Vermerk im Footer, im Impressum oder in den Nutzungsbedingungen erfüllt die Anforderung nicht.

Diese Transparenzpflichten gelten in sämtlichen Bereichen: Lehre, Forschung und Verwaltung. Allenfalls bestehende gesetzliche oder vertragliche Kennzeichnungspflichten (z.B. Vorgaben von Fördergebern) sind jedenfalls zu beachten. Ebenso sind die Vorgaben sozialer Netzwerke zur Deklaration von KI-Inhalten einzuhalten.

Insbesondere in Forschung und Lehre ist eine nachvollziehbare Dokumentation der KI-Verwendung notwendig (verwendetes KI-Tool, Version, Prompt etc.). Eine nähere Auseinandersetzung zum Einsatz von KI-Systemen im Studienalltag finden sich in der mitgeltenden Unterlage FHR-5-004 „Richtlinie zur Verwendung von KI basierten Systemen“.



2.3 Datenschutz und Betriebs- und Geschäftsgeheimnisse

Es sind geeignete technische und organisatorische Maßnahmen zu ergreifen (siehe mitgeltende Unterlage FHR-1-0072 „Technische und organisatorische Maßnahmen (TOMs) i.S.d.Art.32 DSGVO“), um den Schutz von sämtlichen IMC-Daten zu gewährleisten (z.B. Anonymisierung/Pseudonymisierung von Daten vor Eingabe in das KI-System).

Die Nutzung von KI-Systemen muss in jedem Fall den datenschutzrechtlichen Bestimmungen entsprechen. Die Verarbeitung von personenbezogenen Daten mit Hilfe von KI-Systemen ist in jedem Fall vor Eingabe der Daten mit der Abteilung Recht & Verträge abzustimmen.

Es ist grundsätzlich unzulässig Betriebs- und Geschäftsgeheimnisse (sogenannte sensible Daten) in KI-Systemen zu verarbeiten. Ob ein Betriebs- und Geschäftsgeheimnis vorliegt, ist im Zweifelsfall mit der*dem direkten Vorgesetzten abzuklären. Ausnahmen von diesem Verbot müssen in jedem Fall durch die Hochschulleitung vorab schriftlich genehmigt werden. Diesbezügliche Anfragen sind an die Abteilung Recht & Verträge zu richten.

Der Einsatz von KI-Systemen zur Aufzeichnung von Gesprächen sowie zur automatisierten Erstellung von Transkripten und Protokollen (z.B. Besprechungen, Online-Meetings, Telefonate, Interviews) ist datenschutzrechtlich besonders sensibel. Verarbeitet werden dabei regelmäßig personenbezogene Daten sämtlicher Gesprächsteilnehmer*innen, häufig auch Inhalte Dritter sowie Betriebs- und Geschäftsgeheimnisse. Der Umstand, dass eine Aufzeichnungs- oder Transkriptionsfunktion technisch zur Verfügung steht, begründet für sich genommen keine Zulässigkeit ihrer Nutzung.

Eine Aufzeichnung oder automatisierte Protokollierung ist nur zulässig, wenn sämtliche Teilnehmer*innen vor Beginn der Aufzeichnung darüber informiert wurden, dass ein KI-System eingesetzt wird, zu welchem Zweck die Aufzeichnung erfolgt, wer Zugriff auf das Ergebnis erhält und wie lange Aufzeichnung und Transkript gespeichert werden. Der Hinweis ist zu Beginn des Gesprächs zu erteilen und in der Einladung oder im Protokoll zu dokumentieren. Widerspricht eine teilnehmende Person, hat die Aufzeichnung zu unterbleiben; der Widerspruch darf keine Nachteile nach sich ziehen.



Unzulässig ist eine Aufzeichnung jedenfalls bei Gesprächen mit besonderem Vertraulichkeitscharakter (z.B. Mitarbeiter*innengespräche, Personal- und Betriebsratsangelegenheiten, Prüfungs-, Beschwerde- und Disziplinarverfahren, Gespräche mit Studierenden zu persönlichen Anliegen) sowie bei der Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DSGVO. Ausnahmen bedürfen der vorherigen Abstimmung mit der Abteilung Recht & Verträge.

Für die Verarbeitung von IMC-Daten dürfen ausschließlich KI-Systeme verwendet werden, die vom IMC Krems direkt beschafft und freigegeben wurden (siehe KI-Katalog sowie Prozess FHP-1-0040 „Software anfordern“). Die Nutzung privat erworbener, kostenfrei registrierter oder eigenständig hinzugebuchter Dienste ist für IMC-Daten untersagt. Dies gilt ausdrücklich auch für Aufzeichnungs-, Transkriptions- und Zusammenfassungsfunktionen, die in Videokonferenz- oder Kommunikationssysteme integriert sind, sowie für Notiz-Assistenten, die sich als eigene Teilnehmer in Online-Meetings einwählen. Werden solche Funktionen durch externe Gesprächspartner eingesetzt, ist auf deren Deaktivierung hinzuwirken.

2.4 Urheberrecht & Co

Vom IMC Krems lizenziertes Material (z.B. personenbezogene Daten, sensible Daten oder sonstige Daten (z.B. Datenbankinhalte etc.)) darf nur nach vorheriger Prüfung und Freigabe durch die Hochschulleitung mit einem KI-System verarbeitet werden. Diesbezügliche Anfragen sind an die Abteilung Recht & Verträge zu richten.



2.5 KI-Katalog des IMC Krems

Das IMC Krems stellt einen KI-Katalog mit geprüften und für tauglich befundenen KI-Werkzeugen für die Organisation zur Verfügung. Auch bei der Verwendung von KI-Werkzeugen aus dem KI-Katalog ist das Risiko der konkreten Nutzung gemäß Kapitel 2.6 abzuschätzen. Der Katalog wird laufend ergänzt. Findet sich kein passendes Werkzeug im KI-Katalog, dann sind die üblichen Anforderungs- und Freigabe Prozesse einzuhalten (siehe Prozess FHP-1-0040 „Software anfordern“; Prozess FHP-1-0033 „Organisatorische Bereitstellung von Soft- und Hardware für Lehrveranstaltungen“ einzuhalten).

2.6 Risikoanalyse und -management

Der Einsatz von KI-Systemen bedarf einer persönlichen Risikoabschätzung, insbesondere im Hinblick auf potenzielle negative Auswirkungen auf Einzelpersonen oder Gruppen. Die Nutzung von KI-Systemen mit einem minimalen oder keinem Risiko gemäß der Klassifizierung kann frei erfolgen. All jene Nutzungen von KI Systemen, welche über ein minimales oder kein Risiko hinausgehen – also ein begrenztes Risiko beinhalten - bedürfen einer Freigabe durch die dafür übergeordnete Stelle (in der Regel die*der direkte Vorgesetzte*r). Die Risikoeinstufung nach diesem Kapitel und nach Kapitel 5.2 steuert ausschließlich die interne Freigabe. Ob und in welcher Form ein Inhalt zu kennzeichnen ist, richtet sich ausschließlich nach Kapitel 2.2.

All jene Nutzungen, welche unter „Hohes Risiko“ fallen sind ausnahmslos von der Hochschulleitung freizugeben. Diesbezügliche Anfragen sind an die Abteilung Recht & Verträge zu richten. Gemäß dem EU AI Act verbotene Praktiken, sind jedenfalls verboten. Eine Hilfestellung zur Abschätzung des Risikos findet sich im Anhang (siehe 5.2) dieser Richtlinie.

2.7 Forschung und Entwicklung

Werden am IMC Krems KI-Systeme entwickelt oder angepasst, sind jedenfalls die gesetzlichen Vorgaben einzuhalten. Dies trifft auch zu, wenn KI-Systeme Gegenstand der Forschung sind (das KI-System also nicht nur ein Hilfsmittel). Die Einhaltung des „EU AI-Act“, einer diesbezüglichen EU-Verordnung, muss in jedem Fall durch die Abteilung Recht & Verträge vorab geprüft werden.

2.8 Beurteilung von Studierendenleistungen

Der Einsatz von KI-Systemen zur Beurteilung von Studien- und Prüfungsleistungen ist mit besonderen Risiken verbunden. Systeme, die für die Bewertung von Lernergebnissen herangezogen werden, fallen gemäß dem EU AI Act unter die Kategorie "Hohes Risiko".

Die vollständig automatisierte Beurteilung von Studien- oder Prüfungsleistungen durch ein KI-System ist jedenfalls verboten.

Jede Form der KI-Unterstützung, die über eine reine Rechtschreib- und Grammatikprüfung hinausgeht (z.B. für die inhaltliche Vorbewertung), muss vor der Anwendung mit der jeweiligen Studiengangsleitung (in Abstimmung mit der Abteilung Recht & Verträge) abgeklärt und von dieser genehmigt werden.

2.9 KI-Einsatz im Bewerbungsprozess und bei Aufnahmen

Der Einsatz von Systemen der Künstlichen Intelligenz ist im gesamten Prozess der Personalauswahl sowie bei der Aufnahme von Studienwerber*innen am IMC Krems grundsätzlich untersagt. Dieses Verbot umfasst insbesondere Anwendungen zur automatisierten Vorauswahl oder Filterung, zur Bewertung der Qualifikation oder zur Analyse des Bewerberverhaltens, da solche Systeme gemäß dem EU AI Act ein erhebliches Risiko für die Grundrechte darstellen.

Ausnahmen von dieser Regelung sind nur in begründeten Einzelfällen zulässig und bedürfen einer ausdrücklichen schriftlichen Genehmigung durch die Hochschulleitung. Entsprechende Anträge müssen vorab zur rechtlichen Prüfung an die Abteilung Recht & Verträge übermittelt werden. Im Falle einer genehmigten Nutzung sind alle betroffenen Personen vorab umfassend über den Einsatz und die Funktionsweise des jeweiligen KI-Systems zu informieren.



3 Referenzen

3.1 Mitgeltende Unterlagen

- FHR-1-0068 IT Sicherheitsrichtlinie „IT Policy“
- FHR-1-0072 Technische und organisatorische Maßnahmen (TOMs)
i.S.d.Art.32 DSGVO
- FHR-5-004 Richtlinie für die Verwendung KI durch Studierende
- FHP-1-0040 Prozess „Software anfordern“
- FHP-1-0033 Prozess „Organisatorische Bereitstellung von Soft- und Hardware für Lehrveranstaltungen“

4 Gesetzliche Vorgaben

- DSGVO (Verordnung - 2016/679 - DE - Datenschutz Grundverordnung - EUR-Lex (europa.eu))
- EU AI Act (Verordnung - EU - 2024/1689 - DE - EUR-Lex (europa.eu))

5 Anhang

5.1 Begriffsdefinition

In diesem Kapitel werden zentrale Begriffe erklärt und abgegrenzt, um ein einheitliches Verständnis zu erzeugen. Diese spielen in der Ausarbeitung eine zentrale Rolle und werden sowohl in der Literatur als auch in der Praxis oftmals unterschiedlich ausgelegt.

5.1.1 Betriebs- und Geschäftsgeheimnisse

Betriebs- und Geschäftsgeheimnisse sind vertrauliche Informationen eines Unternehmens, die wirtschaftlichen Wert haben und nicht allgemein bekannt oder ohne Weiters zugänglich sind. Sie unterliegen besonderem Schutz, da ihre Offenlegung oder Nutzung dem Unternehmen erheblichen Schaden zufügen kann (z.B. Interne Arbeitsabläufe und Prozessoptimierungen, Kunden- und Lieferantendaten, Vertragsinhalte und Verhandlungsstrategien etc.)

5.1.2 Künstliche Intelligenz

Künstliche Intelligenz (KI) ist ein vielschichtiger Begriff, der verschiedene Technologien, Konzepte und Anwendungen umfasst.

KI-Systeme lassen sich auf Basis ihrer Funktionalität und Struktur in verschiedene Kategorien einteilen:

- **Regelbasierte Systeme** basieren auf festgelegten Regeln und Entscheidungsbäumen. Sie arbeiten deterministisch und sind besonders geeignet für klar definierte Probleme. Beispiele sind Expertensysteme oder Entscheidungsunterstützungssysteme (z.B. vordefinierte, Wenn-Dann-Regeln).
- **Maschinelles Lernen (Machine Learning, ML)** bezeichnet Systeme, die aus Daten lernen und Muster erkennen, ohne explizit programmiert zu sein. Unterkategorien sind:
 - **Supervised Learning:** Lernen mit gelabelten Daten (z.B. Klassifikationsaufgaben bei einem E-Mail-Spam-Filter: „Spam“ oder „Nicht-Spam“).
 - **Unsupervised Learning:** Lernen aus unstrukturierten Daten (z.B. Ein Algorithmus gruppiert Songs anhand gemeinsamer Merkmale wie



Genre, Tempo oder Hörempfehlungen anderer Nutzer, ohne zuvor gelabelte Daten zu verwenden).

- **Reinforcement Learning:** Lernen durch Belohnung und Bestrafung (z.B. Durch Versuch und Irrtum lernt das System, welche Aktionen am besten zum Ziel führen).
- **Neuronale Netze und Deep Learning** sind inspiriert von der Struktur des menschlichen Gehirns und kommen insbesondere bei Deep Learning zum Einsatz. Deep Learning nutzt mehrschichtige neuronale Netze für komplexe Aufgaben wie Bild- oder Spracherkennung (z.B. Gesichtserkennung am Smartphone).
- **Symbolische KI** verwendet logische Regeln und Wissensrepräsentationen, um Schlussfolgerungen zu ziehen. Diese Methode wird häufig in Kombination mit maschinellem Lernen eingesetzt (z.B. „Wenn Tatbestand A und Tatbestand B erfüllt, dann Straftatbestand C“).
- **Hybrid-KI** Hybridansätze kombinieren verschiedene KI-Technologien, z.B. regelbasierte Systeme mit maschinellem Lernen, um Stärken verschiedener Methoden zu vereinen (z.B. Chatbot im Kundenservice)

5.1.3 Privacy by Design

Ein Konzept zur Integration von Datenschutz und Privatsphäre als grundlegende Prinzipien in die Gestaltung und Entwicklung von Systemen, Prozessen und Technologien. Ziel ist es, Datenschutzbedenken proaktiv zu adressieren und zu minimieren, bevor es zu Problemen kommt.

Schlüsselprinzipien:

- Proaktiv, nicht reaktiv: Datenschutz wird von Anfang an berücksichtigt und nicht erst nachträglich.
- Datenschutz als Standard: Schutzmaßnahmen sind standardmäßig implementiert.
- Ganzheitlicher Ansatz: Datenschutz wird über den gesamten Lebenszyklus von Daten hinweg gewährleistet.
- Minimierung der Datenerhebung: Nur die notwendigsten Daten werden erfasst.
- Transparenz und Benutzerfreundlichkeit: Nutzer*innen können nachvollziehen, wie ihre Daten verarbeitet werden.



5.1.4 Privacy by Default

Ein Datenschutzkonzept, das sicherstellt, dass die höchsten Datenschutzstandards standardmäßig aktiviert sind, ohne dass Nutzer*innen manuelle Einstellungen vornehmen müssen. Dieses Prinzip stellt sicher, dass nur die für den jeweiligen Zweck minimal erforderlichen Daten verarbeitet werden.

Schlüsselmerkmale:

- Minimale Datenerfassung: Systeme sammeln nur die Daten, die für die Nutzung unbedingt notwendig sind.
- Datensparsamkeit: Daten werden nur für spezifische Zwecke verarbeitet.
- Einfache Kontrolle für Nutzer*innen: Nutzer*innen haben die Möglichkeit, den Umgang mit ihren Daten einfach zu verwalten und anzupassen.
- Standardmäßige Sicherheit: Sicherheits- und Datenschutzeinstellungen sind standardmäßig aktiv.

5.2 Risikoabschätzung beim Einsatz von KI-Werkzeugen im Organisationsalltag

Keines oder geringes Risiko

Keines oder geringes Risiko liegt vor, wenn generative KI zur Unterstützung dient und die Ergebnisse keinen direkten Einfluss auf wichtige Entscheidungen oder Bewertungen haben.

Beispiele hierfür:

- das Brainstormen von Ideen, aus denen eigene Resultate entstehen
- Spam Filter
- Schreibassistenten, um Texte zu editieren oder zu übersetzen (z.B. DeepL etc.)
- Automatische Textvorschläge (z.B. in MS Word Editor)



Begrenztes Risiko

Begrenztes Risiko sind Risiken, die durch mangelnde Transparenz bei der Nutzung von KI entstehen können. Die Einstufung als begrenztes Risiko begründet für sich genommen keine Kennzeichnungspflicht. Ob und in welcher Form eine Kennzeichnung erforderlich ist, richtet sich ausschließlich nach Kapitel 2.2. Die nachstehenden Beispiele betreffen allein die Freigabe nach Kapitel 2.6.

Beispiele hierfür:

- Verwendung von generativer KI (z.B. Microsoft Copilot, ChatGPT) zur Erstellung von Texten und sonstigen Medien (Bilder, Videos, Musik etc.)

Hohes Risiko

Hochrisiko-KI-Systeme im Sinne des EU AI Act sind solche, die ein erhebliches Risiko für die Grundrechte und Freiheiten von Personen darstellen. Diese Systeme unterliegen strengen Anforderungen an Transparenz, Sicherheit und Datenschutz. Unter den hochriskanten Anwendungsfällen ist für das IMC Krems besonders wichtig:

Allgemeine und berufliche Bildung:

- a) KI-Systeme, die zur Feststellung des Zugangs oder der Zulassung oder zur Zuweisung natürlicher Personen zu Bildungseinrichtungen verwendet werden sollen.
- b) KI-Systeme, die für die Bewertung von Lernergebnissen verwendet werden sollen.
- c) KI-Systeme, die zum Zweck der Bewertung des angemessenen Bildungsniveaus, verwendet werden sollen.
- d) KI-Systeme, die zur Überwachung und Erkennung von verbotenen Verhalten von Schülern bei Prüfungen verwendet werden sollen.

Beschäftigung und Personalmanagement:

- a) KI Systeme um gezielte Stellenanzeigen zu schalten
- b) KI Systeme, um Bewerbungen zu sichten oder filtern oder Bewerber bewerten
- c) KI Systeme, die über Beförderungen, Kündigungen oder die Zuweisung von Aufgaben entscheidet. Auch Systeme, die das Verhalten und die Leistung von Mitarbeiter*innen am Arbeitsplatz überwachen oder beurteilen, fallen unter diesen Punkt.



Verbotene Praktiken

Zu den verbotenen Praktiken im Zusammenhang mit KI-Systemen sind folgende erwähnenswert:

- **Unterschwellige Beeinflussung:** KI-Systeme, die das Verhalten von Personen manipulieren, ohne dass diese es merken, und somit die Entscheidungsfähigkeit beeinträchtigen, wodurch erheblicher Schaden entsteht.
- **Ausnutzung von Vulnerabilität:** KI-Systeme, die Schwachstellen von Personen aufgrund ihres Alters, Behinderungen oder sozialer/ökonomischer Situation ausnutzen, um deren Verhalten zu ändern und dadurch Schaden zufügen.
- **Soziale Bewertung:** KI-Systeme, die Personen über längere Zeit basierend auf sozialen Verhalten oder persönlichen Eigenschaften bewerten und dadurch ungerechtfertigte Benachteiligungen verursachen.
- **Risikobewertung von Straftaten:** KI-Systeme, die allein durch Profiling das Risiko einer Straftat bewerten oder vorhersagen, es sei denn, sie unterstützen menschliche Bewertungen auf Basis objektiver Fakten.
- **Gesichtserkennung:** KI-Systeme, die Gesichtserkennungsdatenbanken durch ungezieltes Auslesen von Bildern aus dem Internet oder Überwachungsaufnahmen erweitern.
- **Emotionserkennung:** KI-Systeme zur Ableitung von Emotionen am Arbeitsplatz oder in Bildungseinrichtungen, es sei denn, sie dienen medizinischen oder Sicherheitszwecken.
- **Biometrische Kategorisierung:** KI-Systeme zur biometrischen Kategorisierung von Personen basierend auf Rasse, politischen Einstellungen, Religion, Sexualleben oder sexueller Orientierung, es sei denn, sie dienen der rechtmäßigen Datensortierung oder Strafverfolgung.