Jetzt kenn i mi aus

Künstliche Intelligenz -
Datenschutz

Mag. Elisabeth Eder-Janca – buero@medienbildung4.me

Was verstehen wir unter KI?

- Rechtlich kann man die Definition aus der EU-Verordnung für Künstliche Intelligenz nutzen (KI-VO).
- Ein „KI-System“ ist laut Artikel 3 Ziffer 1 KI-VO ein Computersystem.
  - Es arbeitet teilweise selbstständig und kann sich nach dem Start anpassen.
  - Aus Daten erstellt es Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen.
  - Diese Ergebnisse können reale oder digitale Umgebungen beeinflussen.
  - Einfacher gesagt sind es Computersysteme, die Aufgaben erledigen, die sonst menschliche Intelligenz brauchen.

Arten von Daten, auf die KI zugreift

Strukturierte Daten

Strukturierte Daten sind organisierte Daten, die leicht in Datenbanken gespeichert und analysiert werden können. Sie sind entscheidend für viele KI-Modelle.

Unstrukturierte Daten

Unstrukturierte Daten sind nicht in einem vordefinierten Format organisiert, wie z.B. Texte, Bilder oder Videos. Diese Daten stehen für eine Vielzahl von KI-Anwendungen zur Verfügung.

Datenquellen für KI

KI-Modelle benötigen verschiedene Datenquellen, um effektiver zu lernen. Daten können aus sozialen Medien, Sensoren, Webseiten und mehr stammen.

Risiken und Herausforderungen bei der Datennutzung

Datenschutzverletzungen

Datenschutzverletzungen sind ein zentrales Risiko bei der Nutzung von Daten in der KI, das schwerwiegende Folgen haben kann.

Diskriminierung

Die Verwendung von Daten kann zu Diskriminierung führen, insbesondere wenn Algorithmen voreingenommene Daten verwenden.

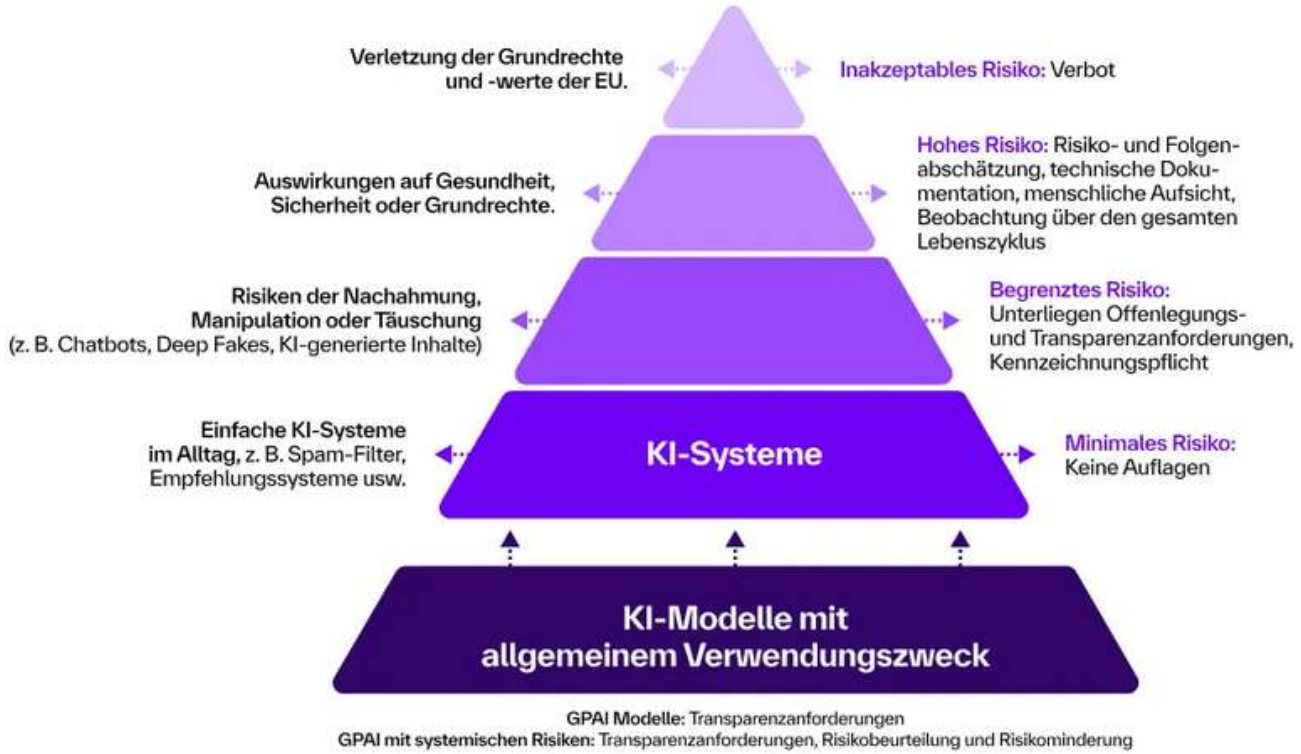
Risikominderung

Es ist wichtig, Strategien zur Minderung dieser Risiken zu entwickeln, um eine verantwortungsvolle Datennutzung zu gewährleisten.

Wie ist der rechtliche Rahmen ?

- EU-Verordnung über Künstliche Intelligenz
  - Die EU hat diese Verordnung am 22. Mai 2024 angenommen. Sie soll **umfassende Regeln dafür schaffen, wie KI-Systeme in der EU auf den Markt kommen, angeboten und genutzt werden dürfen**.
- Wichtig sind auch die Regeln zur Produkthaftung.
  - Dazu gehört ein Entwurf für eine Richtlinie. Diese Richtlinie soll das Haftungsrecht an die Künstliche Intelligenz anpassen. Sie ist noch in Bearbeitung. Auch die Bestimmungen zum Urheberrecht sind wichtig.
    Richtlinie über KI-Haftung »
- Wenn man KI nutzt, verarbeitet man oft personenbezogene Daten.
  - Das sind alle Informationen, die sich auf bestimmte oder bestimmbare Personen beziehen, wie **in Artikel 4 Absatz 1 der DSGVO** definiert.
  - Verarbeitet man solche Daten, gelten die **DSGVO und das österreichische Datenschutzgesetz (DSG).**

EU AI Act: Risikobasierter Ansatz



Quelle: EU-Kommission

Wie ist der Datenschutz laut AGB´s geregelt?

- https://openai.com/de-DE/policies/eu-privacy-policy/ (Chatgpt)
- https://learn.microsoft.com/de-de/copilot/microsoft-365/microsoft-365-copilot-privacy Co-Pilot
- https://www.whatsapp.com/legal/privacy-policy-eea#ea2SG9qUySboIlMvL
- https://www.facebook.com/help/contact/481841188140300
- https://values.snap.com/privacy/privacy-policy?lang=de-DE
- https://www.ombudsstelle.at/blog/facebook-und-instagram-so-widersprechen-sie-der-verwendung-ihrer-daten-fuer-ki-training/

Was ist das Verhältnis zwischen DSGVO und KI-VO?

- Artikel 2 Absatz 7:
- DSGVO –
  - Aufgaben der Datenschutzbehörde
  - Pflichten von Anbietern und Betreibern von KI-Systemen als Verantwortliche oder Auftragsverarbeiter
  - **bleiben unverändert bestehen.**
- **Die DSGVO gilt weiterhin, wenn personenbezogene Daten verarbeitet werden.**
- Für Datenschutzfragen bei KI-Systemen ist die Datenschutzbehörde zuständig.

Wer ist zuständig?

- Eine oder mehrere Behörden überwachen die KI-Systeme.
- Vor allem Hochrisiko-KI-Systeme die Regeln der KI-Verordnung einhalten.
- In Österreich noch unklar.
- EU-Kommission erhält ebenfalls einige Befugnisse zur Durchsetzung.

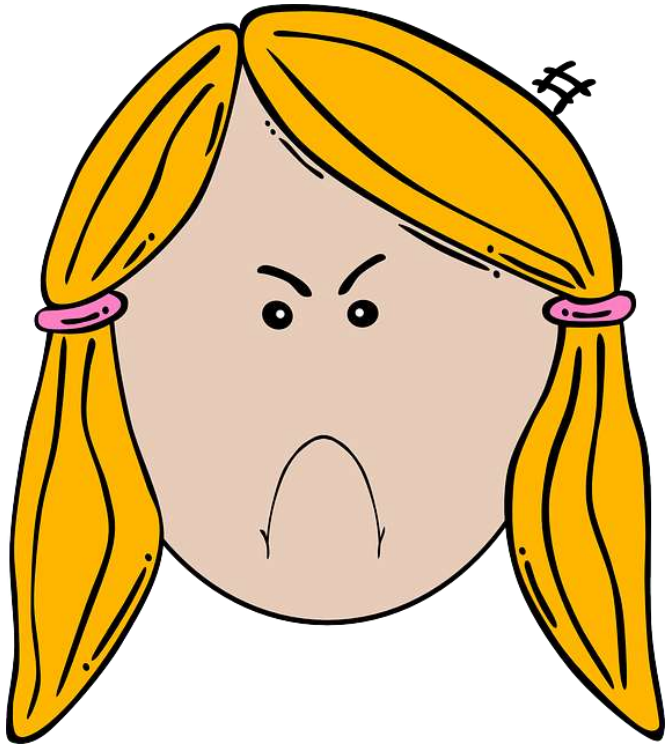
  Zur Vorbereitung auf die Umsetzung der **KI-Verordnung gibt es eine KI-Servicestelle bei der RTR GmbH**.

  – Sie ist Anlaufstelle und Informationszentrum zum Thema KI.
  https://www.rtr.at/

- **Die Datenschutzbehörde** ist für Fragen des Datenschutzes bei KI-Systemen zuständig.
- Artikel 74 Absatz 8 der KI-Verordnung bestimmt außerdem, dass die Aufsichtsbehörden, die für die DSGVO oder die Richtlinie Polizei und Justiz zuständig sind, die Marktüberwachung für Risiko-KI-Systeme übernehmen.
- Dies gilt unter anderem für die Bereiche Strafverfolgung, Grenzverwaltung, Justiz und Demokratie.
- In Österreich ist die **Datenschutzbehörde gemäß den Paragraphen 18 und 31 des Datenschutzgesetzes (DSG) aktuell hierfür zuständig.**

Kann ich eine Beschwerde bei der Datenschutzbehörde einbringen?

- Wenn jemand meint,
  dass bei einem KI-System oder der Verarbeitung seiner persönlichen Daten Regeln der DSGVO oder des DSG verletzt wurden, kann er sich bei der **Datenschutzbehörde** beschweren.
- https://dsb.gv.at/



Welche datenschutzrechtlichen Besonderheiten gibt es in der KI-VO?

- Die KI-Verordnung verweist oft auf die DSGVO, zum Beispiel für Definitionen von Begriffen wie **„personenbezogene Daten“, „biometrische Daten“ oder „Profiling“.**
- Die KI-Verordnung erlaubt **unter bestimmten Bedingungen die Verarbeitung sensibler Daten** gemäß Artikel 9 DSGVO.
- Dies dient dazu, Verzerrungen in KI-Systemen zu finden. Die Daten, die dafür nötig sind, sowie die Begründung, warum andere Daten dieses Ziel nicht erreichen, muss man im Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DSGVO eintragen (Artikel 10 Absatz 5 KI-Verordnung).
- Es muss eine Erklärung vorliegen, dass die Vorgaben der DSGVO oder der Richtlinie für Polizei und Justiz entspricht

KI-Verordnung (AI Act):

- **KI-Verordnung (AI Act)**:
- **Verboten**: Social Scoring durch Behörden, wenn:
  - es diskriminierend ist,
  - Verhalten außerhalb des Kontexts bewertet wird,
  - es zu unfairer Behandlung führt.

- **Privater Social Score** ist erlaubt, **aber stark reguliert**:
  - Transparenzpflicht
  - Datenschutz-Folgenabschätzung
  - Nachvollziehbarkeit der Kriterien

- **Österreichisches Datenschutzgesetz (DSG)**
- **Stärkt DSGVO**: Zusätzliche Aufsichts- und Kontrollmechanismen
- **Datenschutzbehörde** (DSB) äußert sich klar ablehnend zu Social Scoring ohne Rechtsgrundlage.

Welche datenschutzrechtlichen Verpflichtungen zu beachten?

- Die DSGVO ist **technologieunabhängig**.
- Die Verarbeitung personenbezogener Daten ist für viele KI-Systeme zentral. Besonders bei Systemen, die auf maschinellem Lernen basieren, verarbeitet man oft personenbezogene Daten, sowohl beim Training als auch im Betrieb.

  Die DSGVO enthält Grundsätze, die man bei jeder Verarbeitung personenbezogener Daten einhalten muss. Der Verantwortliche muss diese Einhaltung nachweisen können (Art. 5 Abs. 1 und 2 DSGVO):

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

  Diese Grundsätze sind auch beim Einsatz von KI-Systemen und der damit verbundenen Verarbeitung personenbezogener Daten zu beachten.

„Sensible Daten" sind:

- Informationen über die Herkunft, die politische oder religiöse Einstellung eines Menschen.
- Daten zur Mitgliedschaft in einer Gewerkschaft.
- Genetische oder biometrische Daten, die jemanden identifizieren.
- Informationen über die Gesundheit.
- Daten zum Sexualleben oder zur sexuellen Orientierung eines Menschen.

Verarbeitung nach Treu und Glauben; Transparenz:

- Die Verarbeitung von Daten muss fair erfolgen.
- Nicht für Person ungerecht, benachteiligend, überraschend oder irreführend ist
- Dieser Grundsatz hängt eng mit dem Transparenzgrundsatz zusammen. Dieser verlangt, dass man die betroffene Person darüber informiert, wie ihre persönlichen Daten verarbeitet werden (siehe auch „Betroffenenrechte“).

Beispiel

- *Auf einer Versicherungs-Website wird ein „intelligenter Chatbot“ für den Kundenservice verwendet, bei welchem Kund:innen in ihren Anfragen auch regelmäßig personenbezogene Daten preisgeben. Es muss sichergestellt werden, dass die Kund:innen transparent darüber informiert werden, wie genau eingegebene personenbezogene Daten verarbeitet werden. Die Interaktion mit dem Chatbot hat für die betroffene Person zudem keine unvorhergesehenen oder nachteiligen Folgen.*

Zweckbindung, Datenminimierung und Speicherbegrenzung:

- Personenbezogene Daten brauchen immer einen klaren Zweck.
- Die genutzten Daten müssen dafür wirklich notwendig und wichtig sein.
- Sie dürfen nur so lange gespeichert und verarbeitet werden, wie es für diesen Zweck nötig ist.

Beispiel

- *Es soll ein KI-System bei einem medizinischen Forschungsprojekt verwendet werden. Dabei kommt es auch zur Verarbeitung personenbezogener Daten von Probanden. Die gesammelten Daten werden ausschließlich für diesen spezifischen Zweck und nicht für andere Zwecke, wie etwa Werbung oder Weiterverkauf an Dritte, verwendet. Es werden dabei nur die für das Forschungsprojekt notwendigen Daten verarbeitet, nicht erforderliche Informationen werden entfernt oder pseudonymisiert. Die gesammelten Daten werden für einen begrenzten Zeitraum gespeichert, um die Produktempfehlungen zu ermöglichen. Nach einer bestimmten Zeit, wenn die Daten nicht mehr relevant sind oder keine Rechtsgrundlage mehr vorhanden ist, werden sie anonymisiert oder gelöscht.*

Richtigkeit:

- Daten müssen stimmen und aktuell sein. Wir müssen sofort falsche persönliche Daten löschen oder korrigieren.

  Das ist bei Systemen, die Texte oder andere Inhalte erzeugen, schwierig. Diese Systeme erstellen oft Ergebnisse, die statistisch am wahrscheinlichsten sind. Diese Ergebnisse müssen aber nicht immer richtig sein.

  Deshalb müssen wir Nutzer darauf hinweisen, dass die Ergebnisse solcher Systeme falsch oder irreführend sein können.

Integrität und Vertraulichkeit (Sicherheit):

- Bei der Verarbeitung mit KI-Systemen muss Sicherheit vorhanden sein.
- Dies schützt vor unerlaubter oder falscher Verarbeitung und vor unbeabsichtigtem Datenverlust.
- Das verwendete Tool muss Sicherheitsstandards erfüllen. Verarbeitete Daten dürfen nicht an Dritte gelangen.

Beispiel

- *Es wird ein KI-unterstütztes Übersetzungs-Tool einer Drittanbieterin bzw. eines Drittanbieters verwendet, um verschiedenste Dokumente (Schriftsätze, Urkunden etc.) übersetzen zu lassen. Die eingespielten Dokumente werden auf Servern der Anbieterin bzw. des Anbieters gespeichert, deren Sicherheitsvorkehrungen nicht den aktuellen Standards entsprechen. Dadurch erlangen Dritte Zugriff auf die gespeicherten Dokumente und die darin enthaltenen Informationen bzw. personenbezogenen Daten.*

Betroffenenrechte

- Die Rechte der betroffenen Person sind grundsätzlich wie bei jeder anderen Verarbeitung personenbezogener Daten zu gewährleisten.

  Nähere Informationen zu den Betroffenenrechten sind zu finden unter:
- Betroffenenrechten »

Können KI-Systeme genutzt werden, um automatisierte Entscheidungen durchzuführen, die Auswirkungen auf Personen haben?

- Wenn KI-Systeme automatisch Entscheidungen treffen und dabei persönliche Daten verarbeiten, müssen die Regeln von Artikel 22 der Datenschutz-Grundverordnung (DSGVO) beachtet werden.
- **Personen haben nach Artikel 22 DSGVO das Recht, dass Entscheidungen, die sich stark auf sie auswirken, nicht nur von Computern getroffen werden.** Dies gilt auch für Entscheidungen, die auf einer Profilerstellung basieren.

- Artikel 22 DSGVO bezieht sich also nicht auf alle automatischen Entscheidungen, sondern nur auf solche, die die Rechte der betroffenen Personen erheblich beeinflussen.
  In Erwägungsgrund 71 der DSGVO stehen **Beispiele** dafür: **die automatische Ablehnung eines Online-Kreditantrags** oder Online-Bewerbungsverfahren, bei denen kein Mensch eingreift.

- **Stichwort AMS-Algorithmus**

Dies gilt nur in drei Fällen nicht

- Die Entscheidung ist für den Abschluss oder die Erfüllung eines Vertrags zwischen der Person und der:dem Verantwortlichen unbedingt erforderlich
- Es gibt eine gesetzliche Grundlage und diese enthält angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten und der berechtigten Interessen der betroffenen Person oder
- Die Person hat ihre ausdrückliche Einwilligung erteilt

- Auch in diesen Fällen muss die betroffene Person darüber informiert werden, dass eine automatisierte Entscheidung über sie getroffen wird, inklusive der zugrundeliegenden Logik und der angestrebten Auswirkungen der Entscheidung.

  Die betroffene Person hat – außer es liegt eine gesetzliche Grundlage vor – zudem das Recht, die Entscheidung anzufechten und ihren Standpunkt darzulegen sowie eine menschliche Intervention zur Überprüfung der Entscheidung zu verlangen.

  Soweit automatisierte Entscheidungen auf **sensiblen Daten** gemäß Art. 9 Abs. 1 DSGVO beruhen, sind darüber hinaus die besonderen Vorgaben von Art. 22 Abs. 4 DSGVO zu beachten.

Muss ich die DSGVO einhalten, auch wenn ich die KI NICHT entwickelt habe?

kabelplus
alles im plus

• Ja

- Jeder, der festlegt, wie und warum Daten verarbeitet werden, ist datenschutzrechtlich verantwortlich und muss die DSGVO einhalten.
- Auch wenn ein Anbieter oder Betreiber die technischen Vorgaben macht, bleibt die Person oder Stelle, die ein KI-System nutzt, in der Regel datenschutzrechtlich verantwortlich.

Gibt es Tools mit deren Hilfe ich die DSGVO-Konformität von KI-Systemen überprüfen kann?

Der Europäische Datenschutzausschuss hat auf seiner Website Dokumente zur Durchführung von „AI Audits“ veröffentlicht:

- Checklist for AI auditing
- Proposal for AI leaflets
- Proposal for Algo-scores

Diese stehen zur freien Verfügung und können bei der Prüfung der DSGVO-Konformität eines KI-Systems von Nutzen sein.

- Weitere Informationen »

Bewusste Wahl von datenschutzfreundlichen Diensten und Anwendungen

Bedeutung des Datenschutzes

Der Schutz persönlicher Daten ist unerlässlich in der heutigen digitalen Welt, um Privatsphäre und Sicherheit zu gewährleisten.

Best Practices

Es gibt bewährte Praktiken, die Nutzer*innen befolgen können, um datenschutzfreundliche Dienste zu wählen und ihre Daten zu schützen.

Empfehlungen für Nutzer*innen

Nutzer sollten sich über datenschutzfreundliche Optionen informieren und ihre Einstellungen optimieren, um ihre Privatsphäre zu schützen.

Datenschutz-Tipps

- Datenschutzeinstellungen prüfen & aktualisieren
- Zwei-Faktor-Authentifizierung aktivieren
- KI-generierte Inhalte erkennen lernen

Wo gibt es weiterführende Informationen?

- Die KI-Servicestelle, welche in der **RTR GmbH** eingerichtet ist, dient als Ansprechpartnerin und Informationshub zum Thema KI. KI-Servicestelle »
  Der Europäische Datenschutzausschuss arbeitet zudem derzeit an Leitlinien in Bezug auf KI und Datenschutz. Diese werden nach Veröffentlichung hier ergänzt.
  Darüber hinaus hat die **Datenschutzbehörde** bereits die folgenden Informationen zum Verhältnis zwischen DSGVO und KI-VO bereitgestellt:
  Informationen der Datenschutzbehörde zum Verhältnis zwischen der DSGVO und der Verordnung (EU) über künstliche Intelligenz (KI-VO) für **Verantwortliche des privaten Bereichs**
  Zum Dokument »
  Informationen der Datenschutzbehörde zum Verhältnis zwischen der DSGVO und der Verordnung (EU) über künstliche Intelligenz (KI-VO) für **Verantwortliche des öffentlichen Bereichs**
  Zum Dokument »

Quellen & Links

- Datenschutzbehörde Österreich (DSB): https://www.dsb.gv.at/kuenstlichebrintelligenz/kuenstliche-intelligenz-datenschutz
- DSGVO (EU): https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679
- KI-Verordnung (AI Act): https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R1689
- Österreichisches DSG: https://www.ris.bka.gv.at
- FAQ der DSB zu KI & Datenschutz: https://www.dsb.gv.at/faq-zur-ki-verordnung

Hintergrund & Orientierung

FAQ der DSB zu KI & Datenschutz
https://www.dsb.gv.at/faq-zur-ki-verordnung

KI & DSGVO – Orientierungshilfe für Verantwortliche (DSB)
PDF-Download: https://www.dsb.gv.at/download-links

Europäische Datenschutzaufsichtsbehörde (EDSA/EDPB)
https://edpb.europa.eu

Regeln umso wichtiger

- Transparenz:
  - KI-generierte Inhalte müssen klar gekennzeichnet werden.
  - Darf nicht der Eindruck entstehen, dass sich zum Beispiel bei Bildern um die Abbildung von Realität handelt.
- Ethische Verantwortung:
  - Die Einhaltung von ethischen Standards wird durch die „menschliche Letztentscheidung" sichergestellt.
- Verantwortung der Anbieter:
  - Anbieter von KI-Tools sollen die Funktionsweise ihrer Systeme transparent machen.
- Regelmäßige Anpassung:
  - Um mit den Entwicklungen im KI-Bereich Schritt halten zu können, wird die Richtlinie kontinuierlich überprüft und aktualisiert.

Es braucht den Menschen als Kontrolle.

kabelplus
alles im plus

Es liegt an uns.

BILDUNGSWERK

BhW Bildung hat Wert.
Kultur.Region.Niederösterreich