

MODUL 05

Datenschutz & sichere Nutzung von KI-Tools

Weniger teilen. Mehr schützen.
KI verantwortungsvoll nutzen.

Inhaltsverzeichnis

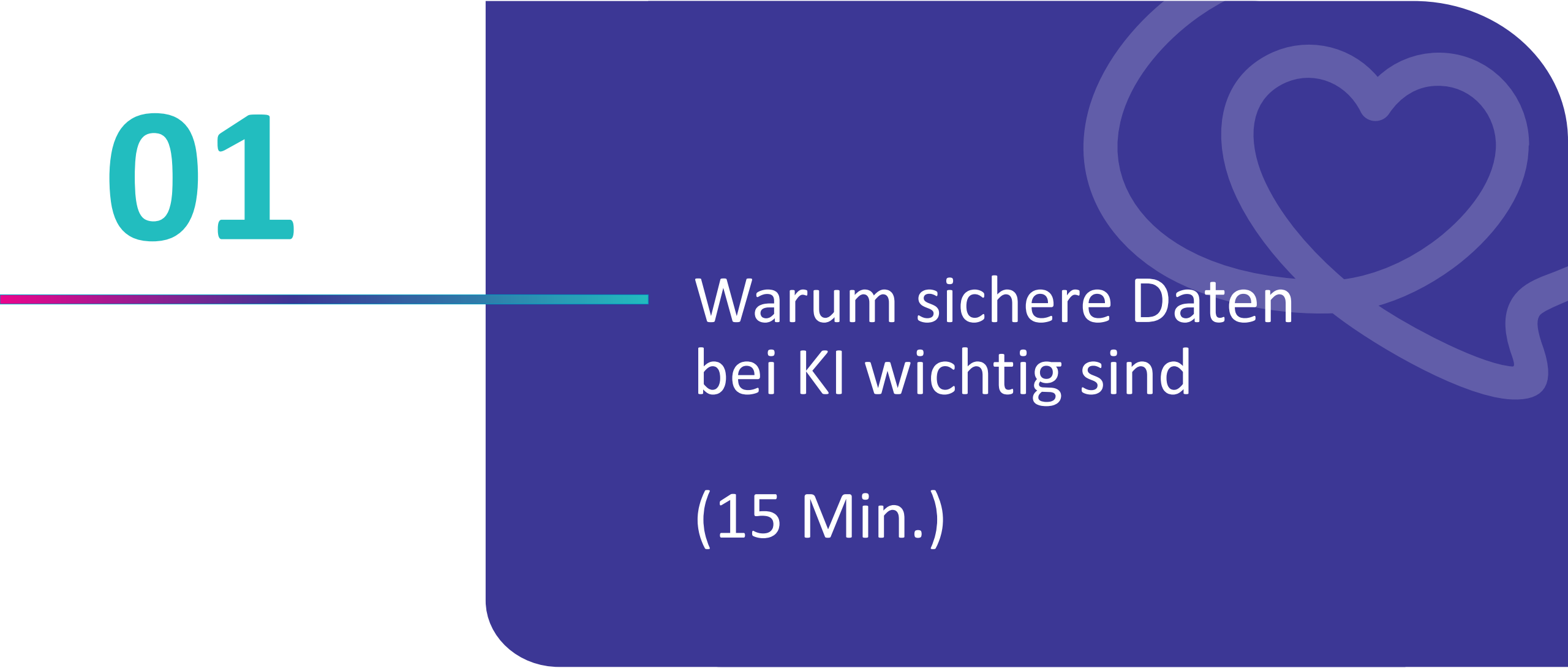
01	Warum sichere Daten bei KI wichtig sind (15 Min.)	3
02	Wie teilst du Daten sicher? (15 Min.)	10
03	Privatsphäre, Rechte und Einwilligung (15 Min.)	16
04	Sicherere KI-Workflows wählen (25 Min.)	23
05	Datenlage: Daten- und Zugangsdaten-Diebstahl (15 Min.)	33



Co-funded by
the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author or authors only and do not necessarily reflect those of the European Union or the Foundation for the Development of the Education System. Neither the European Union nor the entity providing the grant can be held responsible for them.

01

A decorative graphic on the right side of the slide. It features a large, stylized heart shape composed of concentric, slightly irregular lines in shades of blue and purple. A horizontal line, transitioning from pink to blue, extends from the left edge of the slide and ends at the heart shape.

Warum sichere Daten
bei KI wichtig sind

(15 Min.)

Daten und KI

Das Teilen von Daten mit KI-Tools ist besonders im beruflichen Kontext riskant. Wenn Eingaben gespeichert, wiederverwendet oder durch Drittanbieter-Modelle offengelegt werden, kann dies zu Datenlecks, Verstößen gegen Vorschriften sowie zu Reputations- oder Betriebsrisiken führen.

Zentrale Risiken



- **Offenlegung sensibler Daten:** Prompts oder Dateien, die an KI-Plattformen gesendet werden, können gespeichert werden oder in Ausgaben auftauchen. Dadurch können geistiges Eigentum, personenbezogene Kundendaten oder Finanzdaten offengelegt werden.
- **Schatten-KI und unkontrollierte Nutzung:** Wenn Mitarbeitende nicht freigegebene KI-Tools nutzen, entstehen blinde Flecken. Daten verlassen dann möglicherweise die Kontrolle der Organisation, und Anbieter können Eingaben speichern oder wiederverwenden.
- **Rechts- und Compliance-Verstöße:** Die Nutzung externer KI-Dienste ohne passende Verträge oder Vereinbarungen zur Datenverarbeitung kann Datenschutzgesetze verletzen und Sanktionen nach sich ziehen.
- **Mangelnde Transparenz und Nachvollziehbarkeit:** Viele KI-Anbieter legen nicht klar offen, wie Eingaben gespeichert, wo sie verarbeitet oder ob sie zum Training genutzt werden. Dadurch wird Risikobewertung schwieriger.
- **Erweiterte Angriffsfläche:** Die Integration von KI kann technische Schwachstellen vergrößern, z. B. über APIs, Plugins oder Endpunkte, die Angreifer ausnutzen können.

Drei negative Effekte: Datenschutz, Unfairness und falsche Sicherheit

01

Datenschutzrisiko (Offenlegung):

Zu viele Details können persönliche, sensible oder fremde Informationen sichtbar machen.

02

Fairness-Risiko (Schaden):

Verzernte oder unvollständige Daten können Stereotype verstärken oder Gruppen benachteiligen.

03

Zuverlässigkeitsrisiko (falsche Sicherheit):

KI kann überzeugend klingen, auch wenn Eingaben schwach, unvollständig oder irreführend sind.



TUN



Frage: Was fehlt? Wer ist nicht vertreten?
Könnte diese Ausgabe jemandem schaden?



Nutze Checks:
Einwilligungs-Gate +
Fair-Data-Check + SAFE-
Workflow-Stufen



NICHT TUN



KI-Ausgaben als neutrale
Wahrheit behandeln



KI-Ergebnisse nutzen, um
Menschen zu beurteilen
oder Entscheidungen
ohne Kontext zu treffen

Werte-Linse

Sichere Daten = kluge Entscheidungen, die sich an Werten orientieren.

Nutze vier Wertefragen, wenn du KI mit Daten verwendest:

1. **Selbstbestimmung:** Entscheide ich bewusst oder klicke ich nur automatisch?
2. **Datenschutz:** Teile ich mehr Daten als nötig – über mich oder andere?
3. **Fairness:** Könnte meine Datennutzung jemandem schaden oder jemanden benachteiligen?
4. **Transparenz:** Kann ich erklären, welche Daten ich genutzt habe und warum?

Daten, bei denen besondere Vorsicht gilt

Beim Teilen dieser Daten mit KI-Systemen ist besondere Vorsicht erforderlich.

1. Personenbezogene Daten
2. Sensible Daten
3. Gesundheitsdaten
4. Finanzdaten
5. Login-Daten und Zugangsdaten
6. Kundendaten
7. Interne Organisationsdokumente
8. Unveröffentlichte Forschungsergebnisse
9. Daten, die durch Geschäftsgeheimnisse geschützt sind

02



Wie teilst du
Daten sicher?

(15 Min.)

Bevor du KI nutzt: Deine Eingabe wird zu Daten

Viele Menschen konzentrieren sich darauf, was KI antwortet.

Sichere Datennutzung beginnt früher:
bei dem, was du tippst, einfügst oder hochlädst.



In der Praxis können KI-Tools arbeiten mit:

- deinem Text: Prompts, Nachrichten, kopierte Inhalte
- deinen Dateien: Dokumente, Tabellen, PDFs
- deinen Bildern: Fotos, Screenshots
- deinem Kontext: Details, aus denen Rückschlüsse gezogen werden können

Bevor du KI nutzt: Deine Eingabe wird zu Daten

Wenn du zu viel teilst, können Risiken entstehen, die du nicht vollständig rückgängig machen kannst: Datenschutzrisiken, Schaden für andere und unfaire oder irreführende Ergebnisse.

Sichere KI-Nutzung beginnt mit einer einfachen Gewohnheit: Teile nur das notwendige Minimum; oder teile gar nichts.



TUN



TUN: Denke daran: Alles, was du tippst, einfügst oder hochlädst, sind Daten, die du teilst.



NICHT TUN



NICHT TUN: Gehe nicht davon aus: „Es ist nur Text“ oder „Es ist nur ein schneller Upload“.

„Sieht harmlos aus“
ist es aber nicht
immer (Mythos vs.
Realität)



Mythos

„Es ist sicher, wenn ich den Namen entferne.“

Realität

Menschen können indirekt identifiziert werden durch Kombinationen wie:

- Alter + Stadt + Schule/Praktikum
- einmalige Ereignisdetails
- Screenshots mit kleinen sichtbaren Hinweisen
- Standort- und Zeitmuster

Mythos

„Es ist sicher, wenn es nur ein Screenshot ist.“

Realität

Screenshots enthalten oft Namen, Gesichter, Kontaktdaten oder Kontext, den du übersiehst.



● Mikroaufgabe: Rote Flaggen erkennen

Aufgabe (60–90 Sekunden):

Ordne jedes Beispiel zu: Nie teilen / Vermeiden / Meist okay:

- Ein Passwort-Zurücksetzcode
- Ein Lebenslauf mit vollständiger Adresse und Telefonnummer
- Ein Chat-Screenshot mit sichtbaren Namen
- Eine allgemeine Frage: „Wie strukturiere ich einen Lebenslauf?“
- Eine Schulliste mit Namen und E-Mail-Adressen
- Eine Umfragezusammenfassung mit Gesamtzahlen, ohne Namen

Du weißt nie alles

- Es ist nicht immer klar, wo Daten verarbeitet werden.
- Daten können im Gesprächsverlauf gespeichert werden.
- Je nach Einstellungen und Nutzungsbedingungen können Daten zur Verbesserung von Diensten genutzt werden.
- Nutzer*innen können versehentlich vertrauliche Informationen offenlegen.

Merke: Wenn du nicht weißt, wie ein Tool Daten verarbeitet, teile weniger.

03

Privatsphäre, Rechte und Einwilligung

(15 Min.)

Entscheide, bevor du Daten über andere teilst

Nutze diesen Check immer dann, wenn deine Eingabe Informationen über andere Menschen enthält, z. B. Nachrichten, Fotos, Listen, Geschichten oder Dokumente.

3 Fragen stellen:

- Recht / Erlaubnis: Habe ich die Erlaubnis oder eine klare Grundlage, diese Daten mit KI zu verwenden?
- Risiko: Könnte dies jemanden jetzt oder später identifizieren, bloßstellen, verletzen oder schädigen?
- Sicherere Alternative: Kann ich das Ziel mit weniger Daten oder ganz ohne personenbezogene Daten erreichen?

Regel

Wenn du eine Frage mit „Nein“ oder „Nicht sicher“ beantwortest, lade die Daten nicht hoch. Wähle einen sichereren Workflow, z. B. eine allgemeine Frage ohne private Details. „Nicht sicher“ ist ein Warnsignal.

Einwilligung und Daten anderer Menschen: Was verantwortungsvolle Nutzung bedeutet

Privatsphäre und Rechte sind nicht nur technische Fragen. Es geht um Respekt und darum, Schaden zu verhindern.



TUN – sicherere Alternativen:

- Frage nach Einwilligung und respektiere ein „Nein“.
- Ersetze Namen durch Rollen: Person A, Freund*in, Lehrkraft, Kolleg*in.
- Entferne eindeutige Details wie genaue Orte, Daten oder Identifikatoren.
- Stelle eine allgemeine Frage ohne persönliche Geschichte.

TUN



NICHT TUN – hohes Risiko:

- Private Nachrichten anderer Menschen „für Rat“ in KI einfügen
- Gruppenlisten mit Namen oder E-Mails hochladen, um sie „zu organisieren“
- Persönliche Geschichten anderer Menschen ohne Nachfrage teilen

NICHT TUN



● Kurze Übung: Besteht das Einwilligungs-Gate?

Anleitung
Entscheide für jedes Szenario: Besteht oder besteht nicht. Schreibe anschließend einen kurzen Grund.

- „Fasse den Feedbackbrief meiner Lehrkraft zusammen. Er enthält den Namen der Lehrkraft und die Schule.“
- „Hilf mir, eine Entschuldigungsnachricht zu schreiben. Ich beschreibe die Situation, ohne den vollständigen Chat einzufügen.“
- „Analysiere eine Freiwilligenliste mit Namen und Telefonnummern, um ‚unzuverlässige‘ Personen zu finden.“

Habe ich das Recht, diese Daten zu verwenden?

Sichere KI-Nutzung betrifft nicht nur deine eigene Privatsphäre. Es geht auch um Rechte: Darf ich Daten verwenden, teilen oder verarbeiten – besonders, wenn sie jemand anderem oder einer Organisation gehören?

Diese Daten darfst du in der Regel nicht ohne Weiteres mit KI teilen:

- private Nachrichten anderer Menschen, auch wenn du Teil des Chats bist
- Listen von Personen: Klassen-, Freiwilligen- oder Kund*innenlisten
- Dokumente, die nicht dir gehören: Verträge, HR-Notizen, interne E-Mails
- persönliche Geschichten, die dir vertraulich erzählt wurden

Diese Daten kannst du in der Regel eher verwenden:

- eigener Text ohne sensible Details
- allgemeine Fragen ohne personenbezogene Daten
- anonymisierte Beispiele, die du selbst erstellt hast

Einwilligung: Was „echte Einwilligung“ bedeutet – und was nicht



Einwilligung bedeutet nicht nur: „Jemand hat einmal Ja gesagt.“

Für KI-Nutzung sollte Einwilligung sein:

- **informiert:** Die Person versteht, was geteilt wird und warum.
- **spezifisch:** Die Einwilligung gilt für diesen Zweck, nicht für „alles Mögliche“.
- **freiwillig:** Kein Druck, keine Angst vor Nachteilen.
- **widerrufbar:** Die Person kann ihre Meinung ändern.

Wichtig: Einwilligung hängt von Zielgruppe und Tool ab. Eine Person kann dir etwas erzählen, aber nicht wollen, dass es mit einem KI-Tool geteilt wird.

Indirekte Identifizierung: Wenn „Namen entfernen“ nicht reicht

Menschen können auch ohne Namen identifiziert werden, wenn Details Rückschlüsse ermöglichen.

Häufige indirekte Identifikatoren:

- genaues Alter, genauer Ort, Schule/Arbeitgeber oder besondere Rolle
- genaue Daten und Ereignisse: „die einzige Person, die ...“
- Kombinationen: Alter + Stadt + Hobby + Situation
- Screenshots mit kleinen sichtbaren Hinweisen

Sicherere Alternativen:

- Abstrahieren: Situation ohne einmalige Details beschreiben
- Verallgemeinern: Altersgruppe statt genaues Alter, Region statt Adresse
- Rollen verwenden: Person A / Person B
 - Nicht hochladen, wenn Kontext identifizierend bleibt

04

Sicherere KI-Workflows wählen

(25 Min.)

Sicherere KI-Workflows wählen – gleiches Ziel, weniger Daten

Viele Risiken entstehen nicht nur durch das KI-Tool selbst, sondern dadurch, wie wir es nutzen. Oft teilen wir zu viele Daten, weil es schneller oder einfacher wirkt.

Sicherere KI-Workflows wählen – gleiches Ziel, weniger Daten

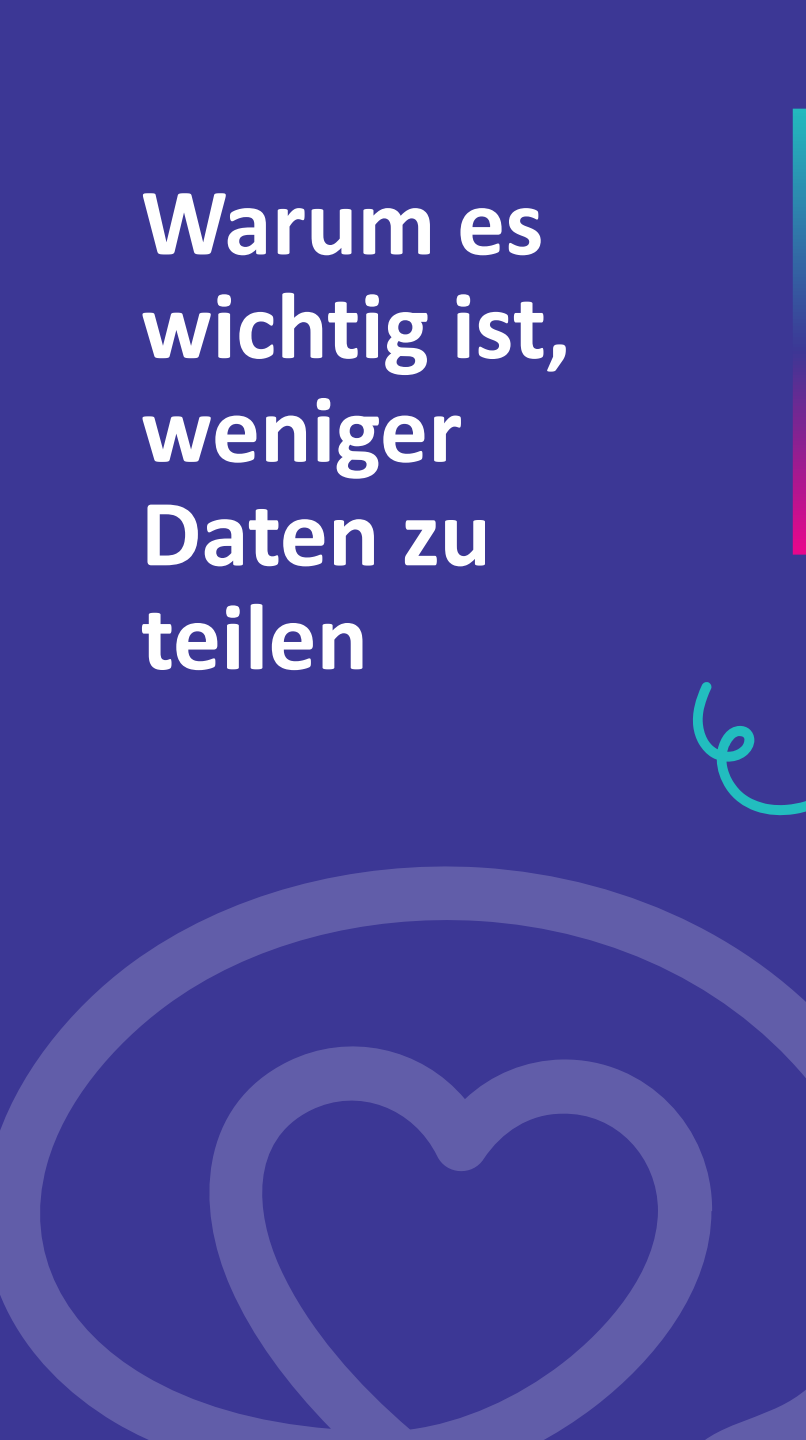
Wenn du Daten mit KI teilst,
können sie verarbeitet,
gespeichert und
wiedergegeben werden



Wenn du Daten in ein KI-Tool tippst, einfügst oder hochlädst, muss das System sie verarbeiten, um eine Antwort zu erzeugen. Je nach Dienst und Einstellungen können deine Daten auch:

- gespeichert oder protokolliert werden
- in bestimmten Fällen überprüft werden
- zur Personalisierung deiner Nutzung verwendet werden
- in Ausgaben wieder auftauchen
- indirekt weitergegeben werden, wenn du Ausgaben kopierst oder Screenshots versendest

Warum es wichtig ist, weniger Daten zu teilen



- Du verringerst die Wahrscheinlichkeit von Datenschutzlecks: Was du nicht teilst, kann nicht aus diesem Tool heraus offengelegt werden.
- Du reduzierst Schaden für andere: weniger fremde Daten, weniger Identifikatoren.
- Du verringerst das Risiko unfairer oder irreführender Schlussfolgerungen: weniger „Rauschen“, mehr zweckbezogene Eingabe.
- Du behältst mehr Kontrolle über deine Informationen.

Merke: Wenn ein Detail für die Aufgabe nicht notwendig ist, entferne es.

SAFE- Workflow- Stufen

Stopp-Regel:

Wenn du sensible
oder vertrauliche
Elemente nicht
entfernen kannst:
nicht hochladen!



Wenn du KI-Hilfe möchtest, beginne nicht damit, alles hochzuladen.
Wähle die sicherste Stufe, die noch funktioniert.

- **Stufe 1 – am sichersten: Stelle eine allgemeine Frage ohne personenbezogene Daten.**
Beispiel: „Wie strukturiere ich einen Lebenslauf?“
- **Stufe 2: Nutze eine anonymisierte Zusammenfassung mit Rollen und ohne Identifikatoren.**
Beispiel: „Person A und Person B hatten einen Konflikt über Fristen. Wie kann Person A reagieren?“
- **Stufe 3: Nutze begrenzte, de-identifizierte Daten nur dann, wenn es notwendig ist.**

Eine riskante Anfrage sicherer machen: vorher → nachher

Regel
Teile Zweck und Muster
– nicht persönliche
Identifikatoren.

Vorher – riskant:

„Hier ist mein vollständiger Lebenslauf. Verbessere ihn.“
(Du lädst ein Dokument mit Adresse, Telefonnummer, Referenzkontakten usw. hoch.)

Was ist riskant? Unnötige Identifikatoren, Kontaktdaten anderer Personen und Daten, die kopiert oder offengelegt werden könnten.

Nachher – sicherer:

„Bitte verbessere Sprache und Struktur dieses Lebenslaufs. Ich habe persönliche Daten entfernt. Konzentriere dich auf Klarheit, Leistungen und prägnante Formulierungen.“

Ausgabesicherheit: Auch KI-Ergebnisse können Informationen preisgeben

Selbst wenn du vorsichtig teilst, kann die Ausgabe sensible Details enthalten, wenn:

- deine Eingabe private Informationen enthielt, oder
- die KI diese Informationen in einer Zusammenfassung, Checkliste oder Nachricht wiederholt.

Sicherere Gewohnheiten:

- Handle Ausgaben wie Dokumente: nicht einfach in öffentliche Chats oder Gruppen kopieren.
- Entferne Namen, Identifikatoren und einmalige Details vor dem Teilen.
- Wenn die Ausgabe eine Person betrifft, halte sie privat oder formuliere sie allgemeiner.
- Speichere sensible Ausgaben sicher oder lösche sie, wenn du sie nicht mehr brauchst.



● Hauptaktivität: Unsichere KI-Nutzung sicherer machen (10 Minuten)

Du übst die gesamte Fähigkeit anhand fiktiver Beispiele. Ziel ist es, sicherere Anfragen zu formulieren, die das Problem trotzdem lösen.

Für jede Anfrage:

- **Identifiziere unsichere Teile: Never Share / Einwilligungs-Gate / Fairness-Risiko.**
- **Formuliere sicherer um: minimieren, anonymisieren, abstrahieren.**
- **Ergänze eine FDC-Zeile: „Was könnte fehlen oder verzerrt sein?“**
- **Wähle den Workflow: Stufe 1 / Stufe 2 / Stufe 3 / Stopp.**

Ergebnis:

Ein kurzes Safe-Data-Playbook für deine tägliche KI-Nutzung.



● Hauptaktivität: Unsichere KI-Nutzung sicherer machen (10 Minuten)

Übung 1:

Chat-Screenshot (Privatsphäre + Einwilligung)

„Hier ist ein Screenshot eines Chats mit meinem Freund / meiner Freundin [Namen sichtbar]. Sag mir, wer recht hat und was ich antworten soll.“

Schritt-für-Schritt-Aufgaben:

- NSL / Nie teilen: Was sollte hier niemals hochgeladen werden?
- Einwilligungs-Gate: Hast du die Erlaubnis, diese Daten zu teilen?
- Sichere Umformulierung (Stufe 1 oder 2): Bitte um Rat, ohne den Screenshot hochzuladen.
- Fairness-Zeile: Was könnte in der Geschichte fehlen?

Unsichere Teile: _____ FDC-Zeile: _____



● Hauptaktivität: Unsichere KI-Nutzung sicherer machen (10 Minuten)

Übung 2:

Personenliste (Vertraulichkeit + Fairness)

„Bitte analysiere diese Freiwilligenliste [mit Namen, Telefonnummern und Anwesenheitsproblemen]. Erstelle eine Rangliste, wer zuverlässig ist.“

Warum das riskant ist:

- personenbezogene Identifikatoren + Daten anderer Menschen
- schädliches Ergebnis: Menschen werden bewertet oder gerankt
- hohes Fairness- und Wirkungsrisiko

Sichereres Ziel: Formuliere die Frage so, dass es um die Verbesserung des Systems geht – nicht um die Bewertung einzelner Personen.

05

Datenlage (15 Min.)

Daten- und Zugangsdaten-Diebstahl – Der illegale Missbrauch von Daten nimmt zu



„7 % Zunahme bei Ransomware oder anderen destruktiven Angriffen. 23 % Zunahme bei Versuchen zum Diebstahl von Zugangsdaten.“

Microsoft Threat Intelligence, „Microsoft Digital Defense Report 2025: Lighting the Path to a Secure Future“ (Microsoft, 2025); <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025>

„Das Volumen der Datenexfiltration bei 10 großen Ransomware-Familien stieg um 92,7 %.“

Zscaler ThreatLabz, „Zscaler ThreatLabz 2025 Ransomware Report“ (Zscaler, 2025); <https://threatlabz.zscaler.com/>

Daten- und Zugangsdaten-Diebstahl – Der illegale Missbrauch von Daten nimmt zu

„Ransomware-Angriffe auf Industrieunternehmen nahmen gegenüber 2024 um 87 % zu.“

*Dragos, „Dragos’s 8th Annual OT Cybersecurity Year in Review Is Now Available“ (2025);
<https://www.dragos.com/blog/dragos-8th-annual-ot-cybersecurity-year-in-review-is-now-available>*

Daten- und Zugangsdaten-Diebstahl – Es gibt Hinweise, dass KI-Systeme Angreifer erheblich unterstützen können



„Der Akteur [...] stützte sich stark auf Claude bei der Implementierung von [Malware].“

A. Moix, K. Lebedev, J. Klein, „Threat Intelligence Report: August 2025“ (Anthropic, 2025).

Hinweis: Der Link im Ausgangsmodul scheint unvollständig zu sein und endet mit „.pd“. Bitte den vollständigen PDF-Link prüfen und ersetzen.

„Ransomware-Betreiber APT INC setzten ein vermutlich von einem LLM verfasstes Skript zur Datenzerstörung ein.“

CrowdStrike, „CrowdStrike 2025 Global Threat Report“ (CrowdStrike, 2025);

<https://www.crowdstrike.com/en-gb/global-threat-report/>

Daten- und Zugangsdaten-Diebstahl – Es gibt Hinweise, dass KI-Systeme Angreifer erheblich unterstützen können



„[Die Google Threat Intelligence Group] entdeckte eine Code-Familie, die KI-Fähigkeiten während der Ausführung einsetzte, um das Verhalten der Malware dynamisch zu verändern. [...] Angreifer gehen über die Nutzung von KI-Tools für technische Unterstützung hinaus.“

*Google Threat Intelligence Group, „GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools“ (Google Threat Intelligence, 2025);
<https://services.google.com/fh/files/misc/advances-in-threat-actor-usage-of-ai-tools-en.pdf>*

Daten- und Zugangsdaten-Diebstahl



Der Beitrag von KI-Systemen zu diesem Trend scheint begrenzt zu sein und ist wahrscheinlich anderen Faktoren nachgeordnet. Dennoch würden einige böswillige Akteure ihre Angriffe ohne KI-Systeme vermutlich nicht starten.

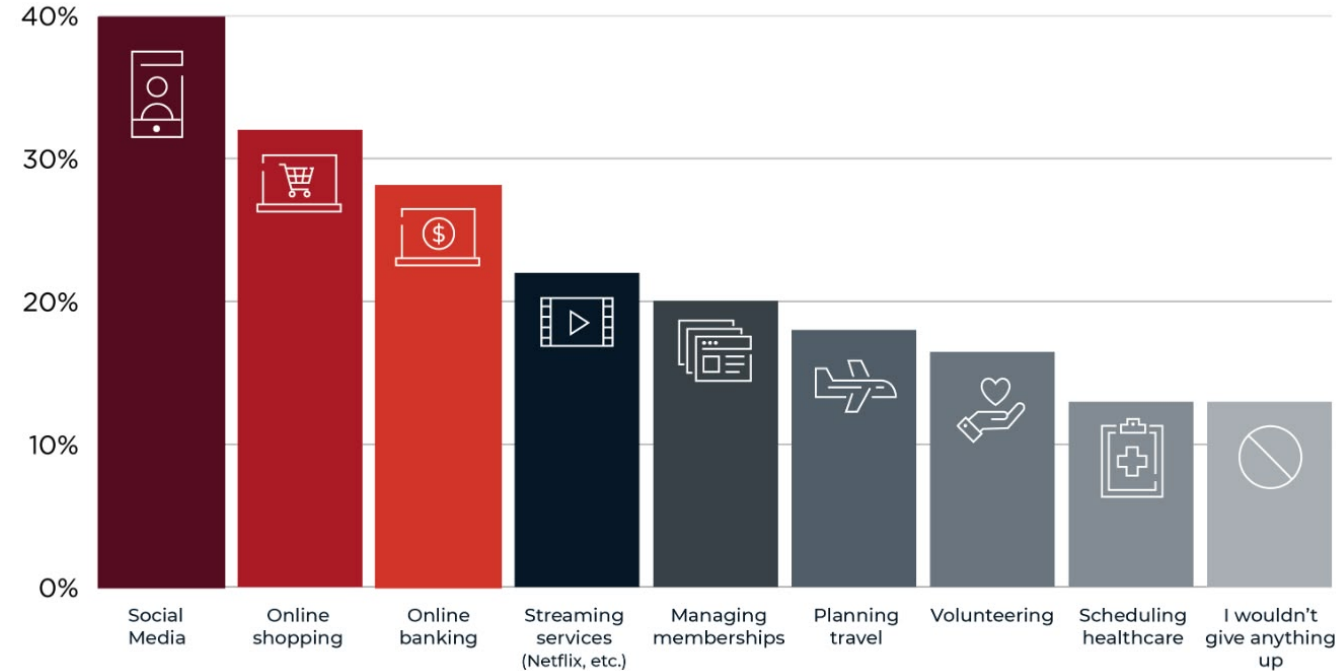
*International AI Safety Report 2026 (DSIT 2026/001, 2026);
<https://internationalaisafetyreport.org>*

Daten- und Zugangsdaten-Diebstahl

Ping Identity. (2024). Bridging the trust gap in the age of AI: 2025 consumer survey. Ping Identity.
<https://www.pingidentity.com/en/lp/2025-consumer-survey.html>

Welchen Arten von Online-Diensten vertraust du deine Identitätsdaten am wenigsten an?

Denke daran: KI wird inzwischen breit genutzt und vermittelt häufig Dienste und Transaktionen.



Daten- und Zugangsdaten-Diebstahl

Ping Identity. (2024). Bridging the trust gap in the age of AI: 2025 consumer survey. Ping Identity.
<https://www.pingidentity.com/en/lp/2025-consumer-survey.html>

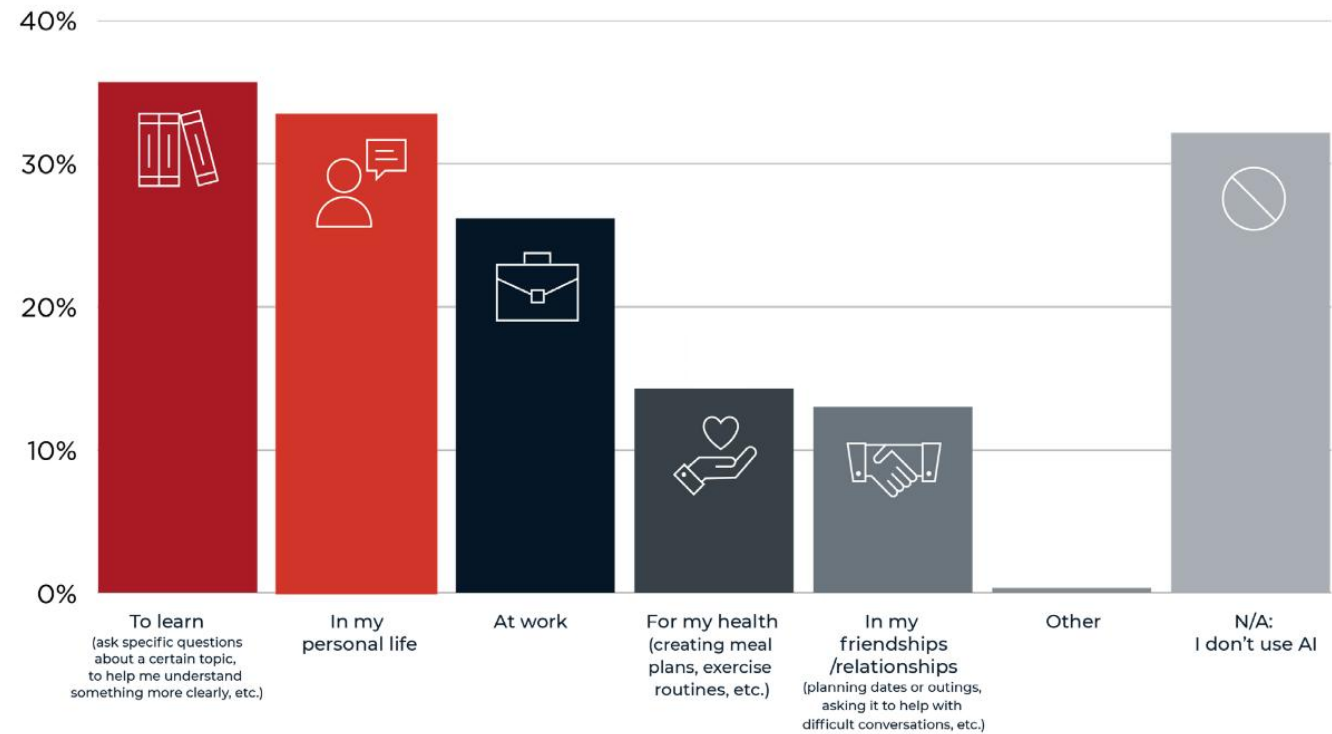
Wie nutzt du künstliche Intelligenz (KI) derzeit?

*„Auch wenn Wissen Macht ist, hat die zunehmende Nutzung von KI im Alltag vielen Verbraucher*innen erst bewusst gemacht, was KI leisten kann. Sie erleben direkt, wie leistungsfähig diese Technologie in eigenen Anwendungsfällen sein kann. Gleichzeitig sehen sie mehr Nachrichten und Datenpunkte zu zunehmenden Sicherheitsbedrohungen und Cyberangriffen. Zusammengenommen ist es verständlich, dass dies zu einer Vertrauenskrise gegenüber der Fähigkeit von Marken beiträgt, Identitätsdaten von Verbraucher*innen sicher zu schützen.“*

Daten- und Zugangsdaten-Diebstahl

Ping Identity. (2024). Bridging the trust gap in the age of AI: 2025 consumer survey. Ping Identity.
<https://www.pingidentity.com/en/lp/2025-consumer-survey.html>

Wie nutzt du künstliche
Intelligenz (KI) derzeit?



Daten- und Zugangsdaten-Diebstahl – Welche Bedenken hast du ggf. im Hinblick auf KI und Identitätssicherheit?

Eingriff von KI-Programmen in meine Privatsphäre	27 %
KI-generiertes Phishing	27 %
Nutzung von KI, um mich oder eine Marke/Person, mit der ich interagiere, fälschlich nachzuahmen	26 %
Mangelnde Transparenz darüber, wie KI-Systeme meine personenbezogenen Daten nutzen und speichern	25 %
Erhöhte Cybersicherheitsrisiken, die die Sicherheit meiner personenbezogenen Daten gefährden	25 %
KI-generiertes Stimmklonen	24 %

Fortsetzung auf der nächsten Folie



Ping Identity. (2024). Bridging the trust gap in the age of AI: 2025 consumer survey. Ping Identity. <https://www.pingidentity.com/en/lp/2025-consumer-survey.html>

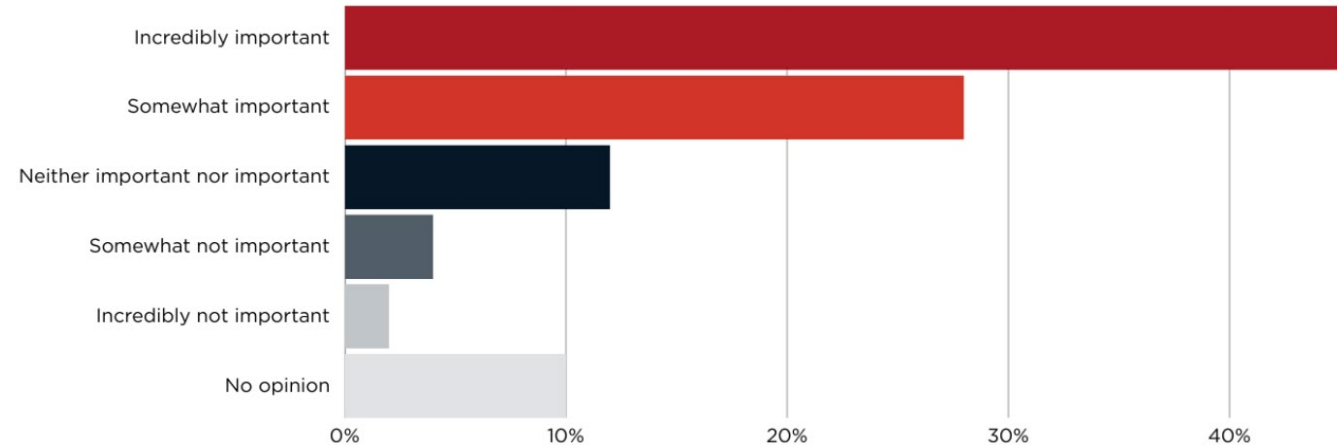
Daten- und Zugangsdaten-Diebstahl – Welche Bedenken hast du ggf. im Hinblick auf KI und Identitätssicherheit?

Deepfake-Imitationen von Menschen, die ich kenne und denen ich vertraue	22 %
KI-Imitation durch Chatbots	20 %
Mangelnde Genauigkeit / Bias in KI-Systemen	18 %
Ich verstehe nicht, welchen rechtlichen Schutz ich in Bezug darauf habe, wie KI meine Daten nutzt	18 %
KI autorisieren, in meinem Namen zu handeln	17 %
Ich habe keine Bedenken in Bezug auf KI und Identitätssicherheit	9 %
Weiß nicht	13 %

Daten- und Zugangsdaten-Diebstahl

Ping Identity. (2024). Bridging the trust gap in the age of AI: 2025 consumer survey. Ping Identity.
<https://www.pingidentity.com/en/lp/2025-consumer-survey.html>

Wie nutzt du künstliche
Intelligenz (KI) derzeit?

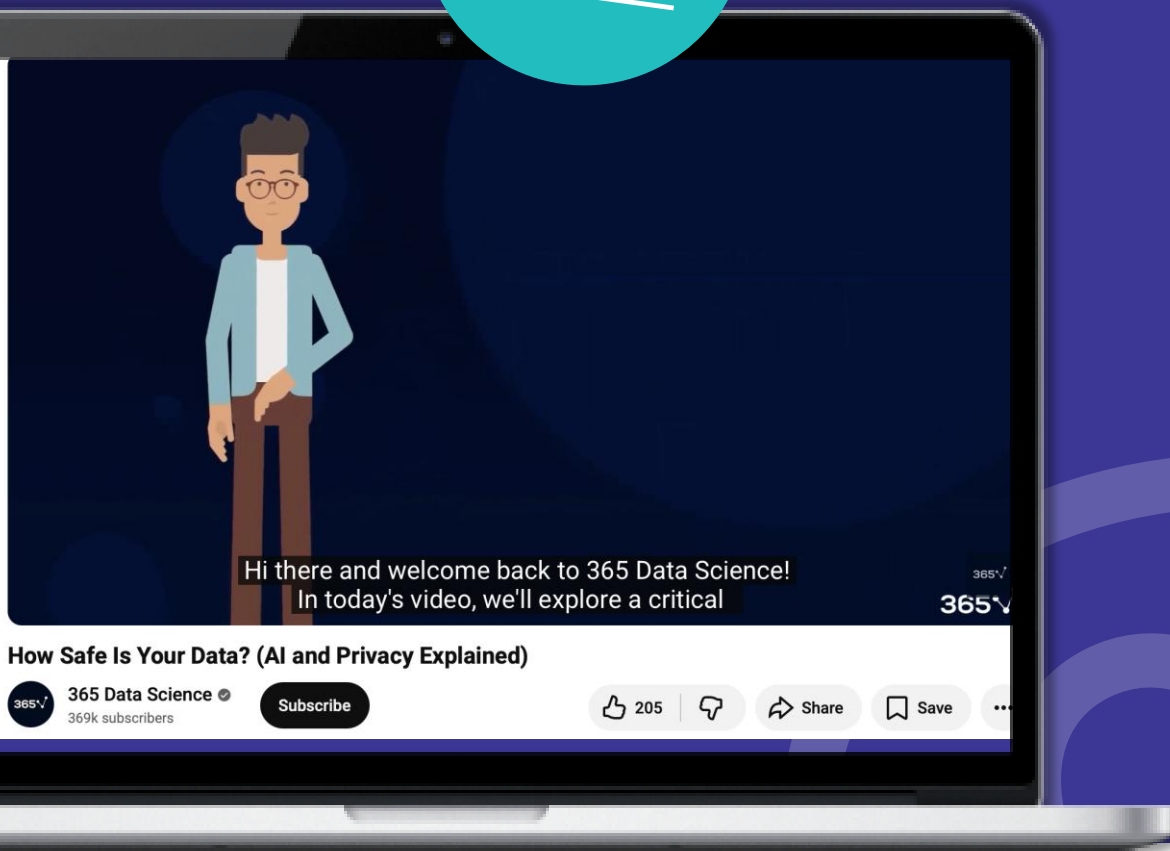


73%

of respondents reported feeling that government regulation of AI to protect their identity data is important.

Video: Daten sicher schützen

ZUM
VIDEO



In der heutigen digitalen Welt war der Schutz deiner Daten noch nie so wichtig wie jetzt.

Dieses Video erklärt die komplexen Wechselwirkungen zwischen künstlicher Intelligenz und den Daten, die wir jeden Tag online teilen – von Social-Media-Beiträgen bis hin zu Online-Shopping-Gewohnheiten.



www.valuesai.eu

Folge unserer Reise



Co-funded by
the European Union

Mitfinanziert von der Europäischen Union. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die der Autor*innen und spiegeln nicht unbedingt die Ansichten der Europäischen Union oder der Stiftung für die Entwicklung des Bildungssystems wider. Weder die Europäische Union noch die fördernde Einrichtung können dafür verantwortlich gemacht werden.