UNIVERSITÉ DE FRIBOURG
UNIVERSITÄT FREIBURG

Empfehlung der Ansprechpersonen für den Datenschutz (DPOs) Verwendung von Daten mit KI-Tools bei der Ausübung der Tätigkeit an der Universität Freiburg

Version 1 vom 21. Oktober 2026

Diese Empfehlung kann regelmässig aktualisiert werden, um der raschen Entwicklung der künstlichen Intelligenz Rechnung zu tragen.

I. Anwendungsbereich

Diese Empfehlung gilt für die Verwendung von Daten in Systemen, die auf Technologien der künstlichen Intelligenz beruhen, unabhängig von deren Form oder Zweck, insbesondere generative, analytische, dialogorientierte, entscheidungsunterstützende oder agentische KI (nachfolgend «KI-Tools»), im Rahmen der beruflichen Tätigkeit an der Universität.

1. Unter der Verwendung von Daten wird jede mit Hilfe eines KI-Tools durchgeführte Operation verstanden, die Daten betrifft, sei es deren Eingabe in das System (Prompts, Dateien, Datenbanken, automatisierte Datenflüsse), deren Bearbeitung durch das System oder die Nutzung der erzeugten Ausgaben.

2. Diese Empfehlung erfasst:
   - KI-Tools, die von Drittanbietern kostenlos oder gegen Entgelt zur Verfügung gestellt werden; sowie
   - KI-Tools, die durch Mitarbeitende der Universität entwickelt, angepasst oder eingesetzt werden.

3. Diese Empfehlung erfasst:
   - die punktuelle Nutzung von KI-Tools (z. B. das Verfassen von Texten oder E-Mails, Brainstorming zu einem Thema, Unterstützung bei der Formulierung bereits bestehender Texte, Übersetzungen usw.); sowie
   - besondere Projekte oder spezifische Anwendungen von KI-Tools, einschliesslich Pilotprojekten und Proof-of-Concepts.

Diese Empfehlung stützt sich auf das Gesetz vom 12. Oktober 2023 über den Datenschutz des Kantons Freiburg.

II. Grundsatz

Personendaten, einschliesslich besonders schützenswerter Personendaten, sowie vertrauliche oder dem Amtsgeheimnis unterliegende Informationen, und sämtliche Dokumente, die solche Daten enthalten, dürfen nicht mit KI-Tools verwendet werden, ausser im Rahmen der geregelten Nutzungen.

Für die Definitionen von Personendaten, besonders schützenswerten Personendaten sowie vertraulichen Informationen oder Informationen, die dem Amtsgeheimnis unterliegen, wird auf Anhang 1 verwiesen. Die geregelten Nutzungen werden in Abschnitt III beschrieben.

Anonymisierte Personendaten unterliegen nicht dem grundsätzlichen Verbot der Verwendung mit KI-Tools, sofern die Reidentifizierung der betroffenen Personen nicht mehr ohne unverhältnismässigen Aufwand möglich ist.
Für ausführliche Erläuterungen wird auf Anhang 1 verwiesen.

III. Geregelte Nutzungen

Geregelte Nutzung Nr. 1 – Verwendung von Microsoft Copilot Chat Basic

Microsoft Copilot Chat Basic[1] kann mit Personendaten sowie mit vertraulichen oder dem Amtsgeheimnis unterliegenden Informationen verwendet werden. **Besonders schützenswerte Personendaten dürfen hingegen nicht in Microsoft Copilot Chat Basic verwendet werden.**

> Microsoft Copilot Chat Basic ist ein institutionelles Tool, das allen Mitarbeitenden der Universität von der DIT zur Verfügung gestellt wird. Seine Nutzung wird durch einen Vertrag mit Microsoft geregelt, der Garantien hinsichtlich des Datenschutzes und der Vertraulichkeit bietet, insbesondere in Bezug auf die Nichtverwendung der Daten zur Weiterentwicklung des kommerziellen Algorithmus (Trainingsdaten).

Wichtig

- Die mit Microsoft Copilot Chat Basic verbundenen Datenschutzgarantien gelten nur dann, wenn die Nutzerin oder der Nutzer mit dem institutionellen Unifr-Konto angemeldet ist. In diesem Fall erscheint oben rechts im Fenster ein grünes Schutzschild.
- Zur weiteren Stärkung der Vertraulichkeit bei der Nutzung von Microsoft Copilot Chat Basic kann die Funktion «Web Search»[2] deaktiviert werden.

Geregelte Nutzung Nr. 2 – Verwendung mit hohem Risiko

Bei Projekten mit hohem Risiko ist die Bearbeitung von Personendaten sowie von vertraulichen oder dem Amtsgeheimnis unterliegenden Informationen, mit einem KI-Tool nur zulässig, wenn:

- die Bearbeitung Gegenstand einer Datenschutz-Folgenabschätzung (DSFA) war; und
- **das in der DSFA festgestellte Risikoniveau** von der zuständigen Stelle gemäss dem anwendbaren DSFA-Verfahren **akzeptiert wurde**[3].

Als Behandlungen mit einem hohen Risiko gelten insbesondere Bearbeitungen mit einem KI-Tool, die Folgendes umfassen:

- die Verwendung von besonders schützenswerten Personendaten;
- die Verwendung von hochvertraulichen Informationen;
- die Bewertung, Klassifizierung, Benotung, Vorhersage oder das Profiling von Personen hinsichtlich persönlicher Merkmale oder ihres Verhaltens;
- die systematische Überwachung oder Nachverfolgung des Verhaltens von Personen;

[1] Diese geregelte Nutzung erstreckt sich nicht auf Microsoft 365 Copilot, da es sich um einen separaten Dienst handelt, dessen Nutzung ein zusätzliches Abonnement voraussetzt.
[2] Bei der Standardnutzung von Copilot Chat Basic analysiert Microsoft die Eingabeaufforderung (Prompt) und identifiziert jene Begriffe, für die Informationen aus dem Internet die Qualität der Antwort verbessern könnten. Auf Grundlage dieser Begriffe erstellt Copilot eine Suchanfrage, die an den Suchdienst Bing übermittelt wird, um zusätzliche Informationen abzurufen.
Zum Deaktivieren der Funktion „Web Search“ öffnen Sie das Menü Chat Settings>Personalisation >Advanced.
[3] Das DSFA-Verfahren befindet sich derzeit in Ausarbeitung. Für Fragen stehen Ihnen die DPOs unter folgender Adresse zur Verfügung: dpo@unifr.ch.

- eine grossflächige Datenbearbeitung, insbesondere unter Berücksichtigung der Anzahl der betroffenen Personen, des Umfangs der bearbeiteten Daten, der Dauer der Bearbeitung oder ihrer geografischen Reichweite;
- eine automatisierte oder teilautomatisierte Einzelentscheidung, die für die betroffenen Personen rechtliche Wirkungen oder andere erhebliche Auswirkungen hat;
- eine Bearbeitung, die geeignet ist, einer Person den Zugang zu einer Dienstleistung zu verwehren, sie am Abschluss eines Vertrags zu hindern oder die Ausübung oder Erlangung eines Rechts einzuschränken.

Wichtig: Die Verwendung von Microsoft Copilot Chat Basic ist für Projekte mit hohem Risiko ohne eine genehmigte DSFA nicht zulässig.

Eine DSFA ist eine vertiefte und strukturierte Analyse der geplanten Datenbearbeitung, der damit verbundenen Risiken sowie der zu treffenden Schutzmassnahmen.

Sie ist ein im Datenschutzrecht vorgesehenes Standardinstrument für Bearbeitungen von Personendaten, die mit hohen Risiken für die betroffenen Personen verbunden sind.

Die Durchführung einer DSFA stellt einen erheblichen Aufwand dar. Diese Investition ist jedoch unerlässlich, um sicherzustellen, dass die Risiken vor der Umsetzung des Projekts angemessen identifiziert, bewertet und beherrscht werden.

Die DPOs stellen Ihnen einen Leitfaden zur Durchführung einer DSFA zur Verfügung und unterstützen Sie bei diesem Vorgehen in Zusammenarbeit mit weiteren Dienststellen, insbesondere mit der DIT sowie der oder dem Verantwortlichen für Informatiksicherheit.

Geregelte Nutzung Nr. 3 – Nutzung nach Durchführung einer Risikoanalyse

Bei Projekten, die **kein hohes Risiko** aufweisen, ist die Bearbeitung von Personendaten sowie von vertraulichen oder dem Amtsgeheimnis unterliegenden Informationen, mit einem KI-Tool zulässig, wenn:

- **vorgängig eine Risikoanalyse durchgeführt wurde; und**
- das in dieser Analyse festgestellte Risikoniveau von der Mitarbeiterin oder dem Mitarbeiter akzeptiert wurde, die oder der für diese Bearbeitung verantwortlich ist.

Die DPOs stellen Ihnen einen Leitfaden für die Durchführung der Risikoanalyse zur Verfügung und unterstützen Sie bei diesem Vorgehen in Zusammenarbeit mit weiteren Dienststellen, insbesondere mit der DIT sowie der oder dem Verantwortlichen für die Informatiksicherheit.
Sind die DPOs der Auffassung, dass das akzeptierte Risikoniveau angesichts der festgestellten Risiken nicht angemessen ist, können sie die Angelegenheit der oder dem administrativen Vorgesetzten der für die Bearbeitung verantwortlichen Person unterbreiten.

Geregelte Nutzung Nr. 4 – Nutzung auf lokaler Infrastruktur

Die Verwendung von Personendaten, einschliesslich besonders schützenswerter Personendaten, sowie von vertraulichen oder dem Amtsgeheimnis unterliegenden Informationen, mittels KI-Tools, die ausschliesslich auf Infrastrukturen oder Servern der Universität betrieben werden, ist zulässig, sofern diese Tools keinen Datenaustausch mit Systemen ausserhalb der universitären Infrastruktur ermöglichen.

> Der geschlossene Charakter des KI-Tools ist vorgängig durch die oder den Verantwortlichen für die Informatiksicherheit zu validieren.

Anhang 1 – Begriffsbestimmungen

1. Personendaten

Definition**:** Informationen, die sich direkt oder indirekt auf eine Person beziehen, unabhängig von ihrer Form, ihrem Inhalt oder ihrem Datenträger.

Einige Daten ermöglichen die direkte Identifizierung einer Person (Name, Vorname, E-Mail-Adresse, AHV-Nummer usw.). Andere Daten sind indirekt identifizierend (Geburtsdatum, genauer Wohnort usw.).

Auch Daten, die je nach Kontext oder in Verbindung mit anderen Informationen die Identifizierung von Personen ermöglichen können, gelten als Personendaten.

Form: Personendaten können jede Form annehmen, beispielsweise Textdaten, Audiodaten, Bilder, Videoaufzeichnungen usw. Die Stimme und das Bild einer Person stellen Personendaten dar.

2. Besonders schützenswerte Personendaten

Besonders schützenswerte Personendaten bilden eine Unterkategorie der Personendaten. Als besonders schützenswerte Personendaten gelten:

- Daten zu den religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten;
- Daten zur Gesundheit, zur Intimsphäre oder zur Zugehörigkeit zu einer Rasse oder Ethnie;
- genetische Daten;
- biometrische Daten, mit denen eine natürliche Person eindeutig identifiziert wird;
- Daten zu Massnahmen der Sozialhilfe;
- Daten zu Betreibungen oder zu strafrechtlichen und administrativen Sanktionen.

3. Anonymisierte Daten

Anonymisierte Daten gelten nicht mehr als Personendaten.

L'anonymisation est un procédé technique qui consiste à **modifier de façon irréversible** les données personnelles afin qu'elles **ne puissent plus être liées à une personne spécifique**, sans efforts disproportionnés.

Die Anonymisierung ist ein technisches Verfahren, bei dem Personendaten irreversibel verändert werden, sodass sie ohne unverhältnismässigen Aufwand keiner bestimmten Person mehr zugeordnet werden können.

Zur Beurteilung, ob eine Reidentifizierung ohne unverhältnismässigen Aufwand möglich ist, sind sämtliche Mittel zu berücksichtigen, die vernünftigerweise eingesetzt werden könnten, sowie alle relevanten Umstände. Das Risiko einer Reidentifizierung sowie die Mittel, die vernünftigerweise zur Reidentifizierung einer Person eingesetzt werden könnten, sind konkret zu bewerten. Dabei sind insbesondere die für eine Reidentifizierung erforderlichen Kosten und der erforderliche Zeitaufwand sowie die verfügbaren Technologien und deren voraussichtliche Entwicklung zu berücksichtigen.

Aufgrund der besonders leistungsfähigen Fähigkeiten von KI-Tools in den Bereichen Analyse, Korrelation und Inferenz darf das Risiko einer Reidentifizierung nicht unterschätzt werden. Bei der Bewertung dieses Risikos ist zu berücksichtigen, dass scheinbar anonymisierte Daten mit anderen

Informationen verknüpft werden können und dadurch eine direkte oder indirekte Identifizierung von Personen möglich wird.

Die blosse Ersetzung direkt identifizierender Daten durch einen Code (**kodierte oder pseudonymisierte Daten**) gilt nicht als Anonymisierung der Daten. Dabei handelt es sich häufig lediglich um einen Schritt des Anonymisierungsverfahrens, der nicht zwangsläufig ausreicht, um davon auszugehen, dass die Personendaten ohne unverhältnismässigen Aufwand keiner bestimmten Person mehr zugeordnet werden können.

4. Vertrauliche oder dem Amtsgeheimnis unterliegende Informationen

Vertrauliche oder dem Amtsgeheimnis unterliegende Informationen sind Informationen, von denen Sie im Rahmen Ihrer Tätigkeit Kenntnis erlangen und die nicht öffentlich sind.

Beispiele: Protokolle von Kommissionen oder nicht öffentlichen Sitzungen, Dossiers von Studierenden, Bewerbungsunterlagen, Prüfungen von Studierenden, interne Korrespondenz sowie Daten, die einer vertraglichen Geheimhaltungspflicht unterliegen.

Hierunter fallen sämtliche Informationen, deren Bekanntgabe an unbefugte Dritte geeignet wäre, die Interessen, Tätigkeiten, Vermögenswerte, die Sicherheit, die Reputation oder das ordnungsgemässe Funktionieren der Universität oder ihrer Partner zu beeinträchtigen.

Hochvertrauliche Informationen sind Informationen, deren Bekanntgabe gegenüber unbefugten Dritten geeignet wäre, die Interessen, Tätigkeiten, Vermögenswerte, Sicherheit, Reputation oder das ordnungsgemässe Funktionieren der Universität oder ihrer Partner **schwerwiegend zu beeinträchtigen**.

Im Forschungsbereich wird empfohlen, folgende Daten als vertraulich einzustufen:

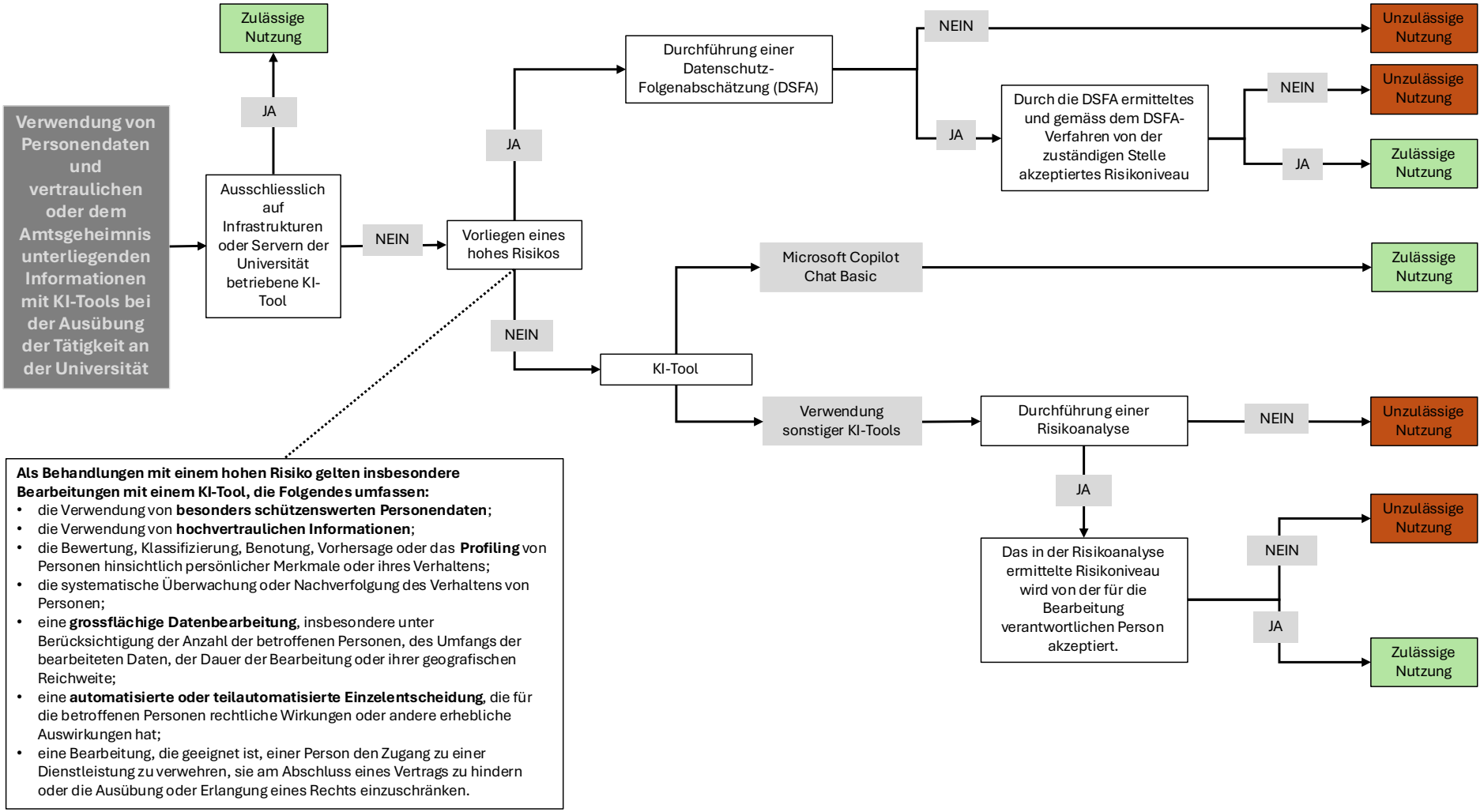
- Forschungsdaten und Forschungsergebnisse, die noch nicht Gegenstand einer wissenschaftlichen Publikation waren;
- Daten und Ergebnisse, die einen kommerziellen Wert haben könnten und/oder zu einer Patentanmeldung führen könnten;
- Daten, für die die Universität oder Sie nicht Inhaberinnen der Immaterialgüterrechte sind;
- alle anderen Daten oder Ergebnisse, die Sie im Rahmen Ihrer Forschung als vertraulich betrachten (beispielsweise im Zusammenhang mit Dual-Use-Forschung).

Vertrauliche oder dem Amtsgeheimnis unterliegende Informationen *enthalten häufig Personendaten. Aus diesem Grund ist es sachgerecht, sie in derselben Empfehlung zu behandeln.*

Unterstützung bei Fragen

*Falls Sie unsicher sind, ob eine bestimmte Angabe, Information oder ein konkretes Dokument als **Personendaten**, **besonders schützenswerte Personendaten**, **vertrauliche oder dem Amtsgeheimnis unterliegende Informationen**, einzustufen ist oder ob Daten als **anonymisiert** betrachtet werden können, können Sie sich an die DPOs wenden: dpo@unifr.ch.*

Anhang 2 – Schematische Darstellung der zulässigen und unzulässigen Nutzungen



Diese Darstellung dient lediglich der Veranschaulichung und soll das Verständnis der Empfehlung der DPOs vom 21. Oktober 2026 erleichtern. Es ersetzt nicht den Text der Empfehlung, der allein verbindlich ist.

Anhang 3 - Warum die Nutzung von Daten mit KI-Tools geregelt werden muss

Trotz der Bemühungen der Anbieter von KI-Tools, Datenschutzoptionen bereitzustellen, kann kein online verfügbares KI-Tool die Vertraulichkeit der eingegebenen Daten zu 100% garantieren. Auch wenn die Algorithmen von KI-Tools leistungsfähige Analyse- und Synthesemöglichkeiten bieten, muss ihre Nutzung stets rechtskonform erfolgen. Der Schutz von Personendaten und die Wahrung der Vertraulichkeit von Informationen sind nicht nur ethische Anforderungen, sondern auch gesetzliche Pflichten.

Die wichtigsten rechtlichen Risiken bei der Verwendung von Personendaten oder vertraulichen oder dem Amtsgeheimnis unterliegenden Informationen in KI-Tools sind:

- die Offenlegung von Daten, die zu einer Verletzung der Vertraulichkeitspflicht, des Amtsgeheimnisses oder des Berufsgeheimnisses führt;
- die Offenlegung strategischer Daten, die die Interessen, Tätigkeiten, Vermögenswerte, Sicherheit, Reputation oder das ordnungsgemässe Funktionieren der Universität Freiburg oder ihrer Partner beeinträchtigen kann;
- die unzulässige Wiederverwendung von Personendaten zum Training von KI-Lösungen;
- das Risiko des Profilings;
- eine unzulässige grenzüberschreitende Bekanntgabe von Personendaten;
- die rechtswidrige Auslagerung einer Bearbeitung von Personendaten.

Hinzu kommen die allgemeinen Risiken der Nutzung von KI, deren Folgen bei der Verarbeitung von Personendaten oder vertraulichen oder dem Amtsgeheimnis unterliegenden Informationen noch schwerwiegender sein können:

- Mangelnde Transparenz der Systeme: Schwierigkeiten zu verstehen, wie die KI-Lösung funktioniert, und nachzuvollziehen, weshalb sie ein bestimmtes Ergebnis geliefert hat (Black-Box-Effekt);
- Halluzinationen oder frei erfundene Inhalte;
- fehlerhafte oder ungenaue Informationen;
- fehlende Überprüfung der von der KI verwendeten Quellen;
- Verzerrungen (Bias) und Diskriminierungen in den erzeugten Ergebnissen;
- übermässige Abhängigkeit von KI, die zu einem Verlust von internem Wissen und kritischem Denken führen kann.