Datenschutz & Informationssicherheit bei der KIPITZ-Nutzung

Kompakt-Merkblatt für Beschäftigte der Bundesverwaltung • 6 goldene Regeln für den Arbeitsalltag

Grundsatz: KIPITZ ist eine sichere KI-Plattform des ITZBund – die datenschutz- und geheimschutzkonforme Nutzung hängt jedoch entscheidend von den eingegebenen Inhalten (Prompts) und der Prüfung der Ergebnisse ab.

1 Keine hochsensiblen Daten (Art. 9 DSGVO) ungeschwärzt eingeben

STOLPERSTEIN

Ungeschwärztes Einkopieren von Gesundheitsdaten, religiöser Überzeugung, ethnischer Herkunft oder politischen Meinungen (z. B. aus Protokollen oder Attesten) in allgemeine Chats.

SO GEHT ES RICHTIG

Personenbezogene und besonders schützenswerte Angaben vorab konsequent **anonymisieren oder pseudonymisieren** (z. B. `[Person A]`), sofern kein speziell freigegebenes Fachmodul genutzt wird.

2 Freigabestufe prüfen: Offen vs. VS-NfD

STOLPERSTEIN

Eingabe eingestufter Verschlusssachen (**VS-NfD**) in Standard-Chat-Instanzen oder externe Modelle, die nur für offene Informationen zugelassen sind.

SO GEHT ES RICHTIG

Vor jedem Prompt die Sicherheitszone der gewählten Anwendung prüfen und **VS-NfD-Daten ausschließlich** in der ausdrücklich dafür freigegebenen On-Premise-Instanz verarbeiten.

3 Datenminimierung statt kompletter Akten-Uploads

STOLPERSTEIN

Hochladen ganzer PDF-Akten inklusive unbeteiligter Dritter (Zeugen, Angehörige, Beschäftigte), obwohl nur ein einzelner Absatz bearbeitet werden soll.

SO GEHT ES RICHTIG

Grundsatz der **Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)** beachten: Nur die Textpassagen übergeben, die für die konkrete Aufgabe zwingend erforderlich sind.

4 Ergebnisse immer gegenprüfen (Human-in-the-Loop)

STOLPERSTEIN

Blindes Übernehmen von KI-Zusammenfassungen mit erfundenen Aktenzeichen, verdrehten Daten oder Fehlinterpretationen (Verstoß gegen Datenrichtigkeit, Art. 5 Abs. 1 lit. d DSGVO).

SO GEHT ES RICHTIG

Jede KI-Ausgabe anhand der Originalakte prüfen. Die KI erstellt nur einen **unverbindlichen Rohentwurf** – die fachliche und rechtliche Verantwortung bleibt immer beim Menschen.

5 Keine Bewertung von Personen im allgemeinen Chat

STOLPERSTEIN

Nutzung allgemeiner KIPITZ-Chats für Prognosen zu Antragserfolgen, Glaubhaftigkeitsbewertungen oder zur Vorselektion von Bewerbungen und Anträgen.

SO GEHT ES RICHTIG

Allgemeine Sprachmodelle ausschließlich zur **Text-, Strukturierungs- und Recherchehilfe** einsetzen – niemals für Profilbildung (Profiling) oder eigenständige Personenbewertungen.

6 Chatverläufe regelmäßig bereinigen

STOLPERSTEIN

Dauerhaftes Speichern alter Prompts und Fallkonstellationen im persönlichen Chatverlauf, nachdem der Vorgang längst abgeschlossen wurde.

SO GEHT ES RICHTIG

Arbeitsergebnisse nach Prüfung in die **führende E-Akte** übernehmen, Chatverläufe regelmäßig löschen und keine dauerhafte Schattenaktenhaltung im KI-Portal aufbauen.

Merksatz & Meldepflicht: Bei Unsicherheiten zur Einstufung oder bei versehentlicher Eingabe unzulässiger personenbezogener bzw. eingestufter Daten umgehend den Chatverlauf löschen und den **behördlichen Datenschutzbeauftragten** bzw. den **Geheimschutzbeauftragten** informieren.