

Etappe 3

Chancen & Spielregeln

Welche Daten dürfen in die KI?

Pfad 1: Entdecken · KI-Einsteiger:innen

Agenda

Was dich in diesem Lernimpuls erwartet · ca. 20 Minuten

1

Zwei Seiten derselben Medaille

Was KI dir abnimmt — und was dabei deinen Schreibtisch verlässt

2

Die Datenreise

Wohin gehen deine Eingaben? Geschützter Raum vs. offenes Tool

3

Die KI-Ampel

Grün · Gelb · Rot — und die 2 Prüffragen vor jeder Eingabe

4

Fünf Spielregeln

Dein Reflex für den Alltag — anonymisieren statt verzichten

Zwei Seiten derselben Medaille

KI nimmt dir Arbeit ab. Und in diesem Moment verlässt deine Eingabe deinen Schreibtisch.

Die Chance

- Texte formulieren
- Lange Mails zusammenfassen
- Ideen sammeln
- Übersetzen
- In einfache Sprache umschreiben

→ **Echte Arbeit, weniger Reibung**

Das Risiko

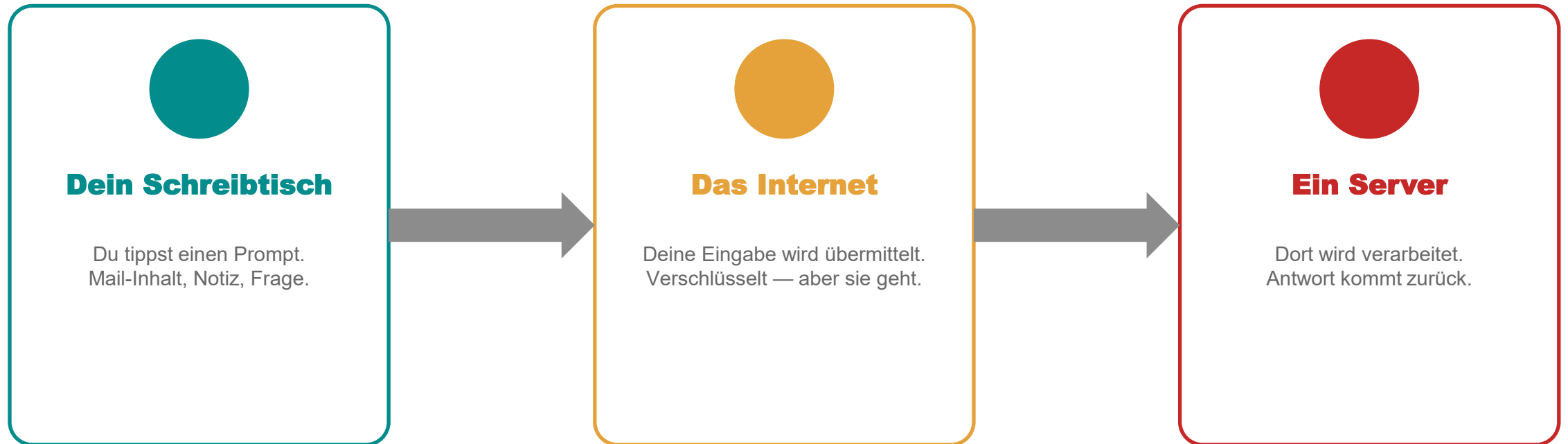
- Vollständige Namen
- Adressen, Geburtsdaten
- Hinweise auf Krankheit, Schulden
- Interne Notizen, Konflikte
- Vertrauliche Geschäftsdaten

→ **Verlässt mit einem Klick deinen Schreibtisch**

«Die meisten KI-Datenpannen passieren aus Eile — nicht aus Absicht.»

Die Datenreise

Was du in die KI eingibst, wird woanders verarbeitet.



«Deine Eingabe verlässt deinen Schreibtisch.»

Es ist nicht egal, wohin diese Reise geht.

Zwei Welten — geschützt vs. offen

Wo deine Eingabe landet, entscheidet alles.

Varios

Die freigegebene KI-Arbeitsumgebung der Stadt Uster

- freigegebene Arbeitsumgebung
- geregelter Einsatz im Arbeitskontext
- klare organisatorische Vorgaben
- erste Wahl für Arbeitsinhalte

 **«Gebäude mit Tür, Schloss und Hausordnung»**

Frei zugängliches Tool

ChatGPT privat, Gemini privat, etc.

- Eingaben können gespeichert werden
- Teils zum Training des Modells genutzt
- Standort des Servers oft unklar
- Du hast weniger Kontrolle darüber, was mit der Eingabe passiert

 **«Öffentlicher Platz — was du sagst, ist gesagt»**

Was die Schweiz dazu sagt

Du musst keine Juristin und kein Jurist sein. Aber drei einfache Grundsätze gelten immer.

Nur wofür du zuständig bist

(Zweckbindung) Nur Daten bearbeiten, wozu du als Verwaltungs-Mitarbeitende:r berechtigt bist.

Beispiel

Einen Antrag prüfen ≠ die Antragstellerin googeln.

Nur was wirklich nötig ist

(Verhältnismässigkeit) Nur so viele Daten wie nötig — und nicht länger als nötig.

Beispiel

Personendaten aus alten Akten gehören nicht ins KI-Tool.

Nicht nach aussen tragen, was vertraulich ist

(Berufsgeheimnis) Verwaltungs-Mitarbeitende sind zur Verschwiegenheit verpflichtet.

Beispiel

Was du extern nicht erzählst, gehört auch nicht in ein offenes Tool.

«Diese Pflichten gelten unabhängig vom Werkzeug — ob Word, Excel oder KI.»

Grundlage: IDG des Kantons Zürich (Datenschutz öffentlicher Organe) · Pflichtbereich Stadt Uster

Die KI-Ampel

Drei Farben. Drei klare Antworten. Das einzige Werkzeug, das du brauchst.

GRÜN

Unbedenklich

Öffentliche Informationen
Keine Person erkennbar
Kein interner Bezug
Beispiel: öffentlicher Text von der Website

→ Grundsätzlich unproblematisch — im
Arbeitskontext trotzdem zuerst Varios

GELB

Intern

Interne, nicht öffentliche Info
Ohne besonderen Schutzbedarf
Beispiel: interne Traktandenliste ohne
Personendaten

→ Nur über Varios

ROT

Personendaten & Vertrauliches

Namen, Adressen, Schulden
Krankheit, Konflikte, Geheimes
Verhandlungen
Beispiel: Mail mit Name, Adresse oder Konflikt

→ Nicht eingeben oder zuerst
anonymisieren

Die zwei Prüffragen

Vor jeder Eingabe. Zwei Fragen — die Farbe steht fest.

Frage 1

Sind Personendaten, Sensibles oder Geheimnisse drin?

Vollständige Namen · Adressen · Krankheit · Konflikt · Vertrauliches

ja → ROT
nein → Frage 2

Frage 2

Ist es eine interne, nicht-öffentliche Information?

Sitzungsprotokolle · interne Vorlagen · Arbeitsstände

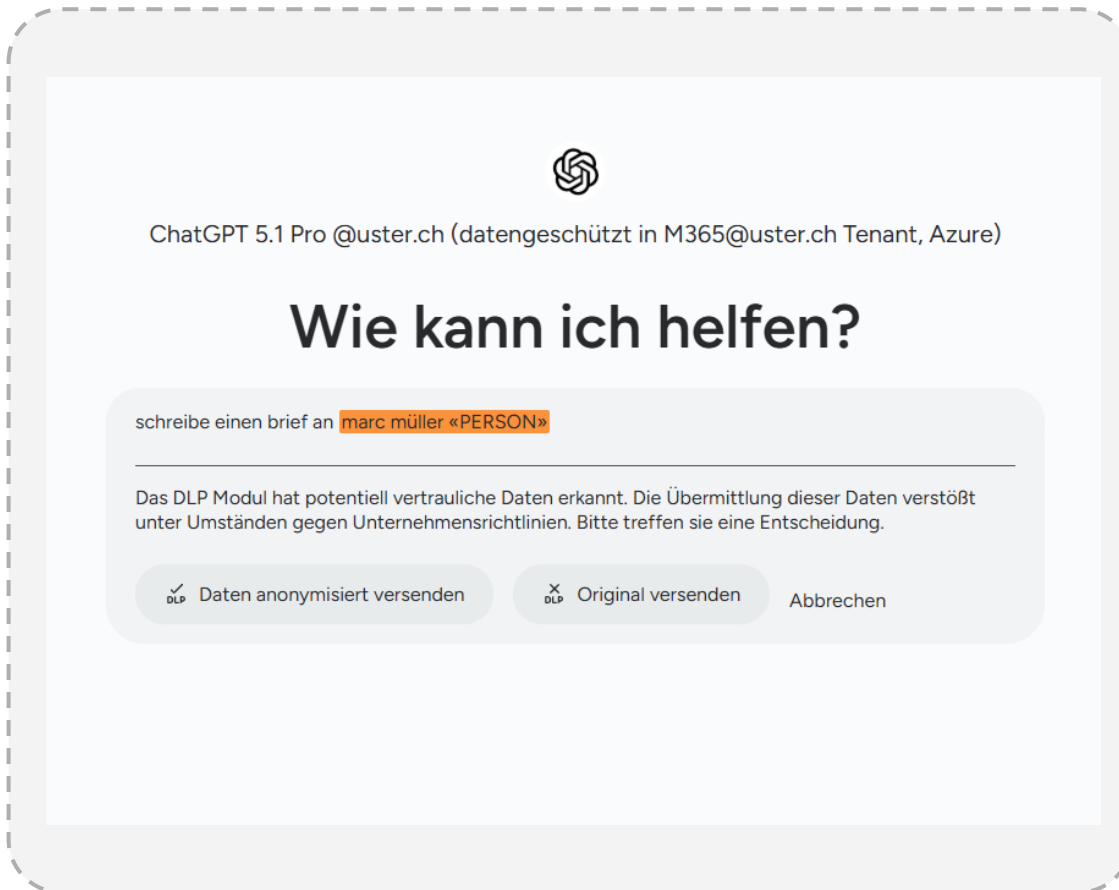
ja → GELB
nein → GRÜN

«Identifizierbar» heisst nicht «benannt».

Auch ohne Namen kann durch Kombinationen klar werden, wer gemeint ist — dann gilt Rot.

Varios warnt dich bei sensiblen Daten

Das DLP-Modul erkennt mögliche vertrauliche oder personenbezogene Daten — und stoppt die Eingabe, bevor sie versendet wird.



The screenshot shows the ChatGPT 5.1 Pro interface. At the top, it says "ChatGPT 5.1 Pro @uster.ch (datengeschützt in M365@uster.ch Tenant, Azure)". Below this is the question "Wie kann ich helfen?". The user's input is "schreibe einen brief an marc müller «PERSON»". A warning message from the DLP module is displayed: "Das DLP Modul hat potentiell vertrauliche Daten erkannt. Die Übermittlung dieser Daten verstößt unter Umständen gegen Unternehmensrichtlinien. Bitte treffen sie eine Entscheidung." At the bottom, there are three buttons: "Daten anonymisiert versenden" (with a checkmark icon), "Original versenden" (with an 'X' icon), and "Abbrechen".

Du hast drei Möglichkeiten

Im Beispiel: «Marc Müller» wird als Person erkannt.

- 1 · Daten anonymisiert versenden
- 2 · Original versenden
- 3 · Abbrechen

Wichtig: Nur weil «Original versenden» möglich ist, heisst das nicht, dass du es auch darfst.

«DLP hilft dir beim Erkennen — entscheiden musst du trotzdem.»

Fünf Spielregeln

Dein Reflex vor jeder Eingabe. Nicht zum Auswendiglernen — zum Beigewohnen.

1

Erst prüfen, dann eingeben

Schau vor jeder Eingabe kurz hin: Sind die Informationen grün, gelb oder rot?

Fünf Spielregeln

Dein Reflex vor jeder Eingabe. Nicht zum Auswendiglernen — zum Beigewohnen.

1

Varios nutzen

Der geschützte Raum der Stadt Uster. Erste Wahl im Arbeitskontext.

2

Arbeitsinhalte nur in Varios

Wenn du KI für deine Arbeit bei der Stadt Uster nutzt, arbeitest du in Varios.

Fünf Spielregeln

Dein Reflex vor jeder Eingabe. Nicht zum Auswendiglernen — zum Beigewohnen.

1

Varios nutzen

Der geschützte Raum der Stadt Uster. Erste Wahl im Arbeitskontext.

2

Ampel zuerst

Vor jeder Eingabe die zwei Prüffragen. Ergebnis: Grün, Gelb oder Rot.

3

Nur so viel wie nötig

Die KI braucht oft weniger Informationen, als du denkst.

Fünf Spielregeln

Dein Reflex vor jeder Eingabe. Nicht zum Auswendiglernen — zum Beigewöhnen.

1

Varios nutzen

Der geschützte Raum der Stadt Uster. Erste Wahl im Arbeitskontext.

2

Ampel zuerst

Vor jeder Eingabe die zwei Prüffragen. Ergebnis: Grün, Gelb oder Rot.

3

Anonymisieren statt verzichten

Rot heisst: so nicht eingeben — erst anonymisieren, abstrahieren oder klären.

4

Rot nie im Original eingeben

Wenn ein Text persönliche, sensible oder vertrauliche Informationen enthält, ist er rot.

Fünf Spielregeln

Dein Reflex vor jeder Eingabe. Nicht zum Auswendiglernen — zum Beigewöhnen.

1

Varios nutzen

Der geschützte Raum der Stadt Uster. Erste Wahl im Arbeitskontext.

2

Ampel zuerst

Vor jeder Eingabe die zwei Prüffragen. Ergebnis: Grün, Gelb oder Rot.

3

Anonymisieren statt verzichten

Rot heisst: so nicht eingeben — erst anonymisieren, abstrahieren oder klären.

4

Im Zweifel fragen

Eine kurze Frage ist immer billiger als eine Panne.

5

Im Zweifel stoppen und nachfragen

Gib die Information noch nicht ein und frage zuerst bei der zuständigen Anlaufstelle, deiner KI-Koordinatorin oder deinem KI-Koordinator nach.

Rot heisst: so nicht eingeben

Erst anonymisieren, abstrahieren oder klären.

✗ Mit Personendaten

Roter Fall — nicht eingeben

«Maria Müller, geb. 14.03.1968, Bahnhofstr. 12, hat sich am 18.05. über die Bauarbeiten an der Kreuzung Birmensdorfer-/Sihltalstrasse beschwert und droht mit Anwaltsbrief, falls die Baulärm-Beschränkungen nicht eingehalten werden.»

✓ Anonymisiert

Sicher für Varios

«Eine Bürgerin hat sich über Baulärm an einer Strassenkreuzung beschwert und droht mit rechtlichen Schritten, falls die Beschränkungen nicht eingehalten werden. Bitte einen sachlichen Antwortentwurf formulieren.»
→ Achte auch auf indirekte Hinweise: Ort, Zeitpunkt, Funktion, seltene Ereignisse.

«Die KI muss nie erfahren, um wen es geht — nur worum.»

Das nimmst du mit

Datenschutz im Blick — die ganze Etappe in vier Sätzen.



Deine Eingabe verlässt deinen Schreibtisch

Was du eintippst, wird woanders verarbeitet.

Das nimmst du mit

Datenschutz im Blick — die ganze Etappe in vier Sätzen.

1

Deine Eingabe verlässt deinen Schreibtisch

Was du eintippst, wird woanders verarbeitet.

2

Zwei Welten — geschützt vs. offen

Für die Arbeit zählt nur der geschützte Raum Varios.

Das nimmst du mit

Datenschutz im Blick — die ganze Etappe in vier Sätzen.

1

Deine Eingabe verlässt deinen Schreibtisch

Was du eintippst, wird woanders verarbeitet.

2

Zwei Welten — geschützt vs. offen

Für die Arbeit zählt nur der geschützte Raum Varios.

3

Identifizierbar heisst nicht benannt

Auch ohne Namen können Kombinationen klar machen, wer gemeint ist — Rot.

Das nimmst du mit

Datenschutz im Blick — die ganze Etappe in vier Sätzen.

1

Deine Eingabe verlässt deinen Schreibtisch

Was du eintippst, wird woanders verarbeitet.

2

Zwei Welten — geschützt vs. offen

Für die Arbeit zählt nur der geschützte Raum Varios.

3

Identifizierbar heisst nicht benannt

Auch ohne Namen können Kombinationen klar machen, wer gemeint ist — Rot.

4

Die KI-Ampel zeigt dir, was zu tun ist

Grün: unproblematisch. Gelb: nur in Varios. Rot: so nicht eingeben.

Ausblick

Nächste Etappe: Assistenten anwenden