

Datenschutz im ganzen Arbeitsprozess

Anleitungskarte zur Etappe · Pfad Gestalten — vom Dokument über die KI bis zum fertigen Ergebnis.

Wo arbeiten wir?

Beim Senden verlassen die Daten deinen Arbeitsbereich — entscheidend ist die **Umgebung**.



Postkarte · offene/private Tools

Für alle mitlesbar wie eine Postkarte. Städtische Inhalte hier eingeben ist verboten (= Schatten-KI).



Briefumschlag · geschäftliche KI

Zugriffsgeschützt, aber von der Stadt Uster nicht freigegeben — darum nicht für Arbeitsinhalte nutzen.



Aktenkoffer · Varios ✓

Geprüft, geschützt und freigegeben. **Alle städtischen Arbeitsinhalte gehören hierhin.**

Der sichere Datenweg

Datenschutz zählt über den **ganzen Weg** — nicht nur im einzelnen Prompt. Reihenfolge einhalten:

1

Ausserhalb der KI vorbereiten

Original bleibt im Fachsystem — nicht in die KI. Heikle Angaben im Text löschen oder durch Platzhalter wie [NAME] ersetzen.

2

In Varios bearbeiten

Nur die entschärfte Fassung in Varios eingeben. Die KI hilft beim Formulieren, kennt die echte Person aber nicht.

3

Ergebnis prüfen & lokal ergänzen

KI-Entwurf inhaltlich prüfen. Echte Namen, Adressen, Fallnummern erst danach im Fachsystem einfügen — nicht in der KI.



Nie den roten **Originaltext** zuerst in die KI kopieren, um ihn dort anonymisieren zu lassen — dann sind die Daten schon übermittelt.

Die KI-Ampel

Erste Entscheidung: Darf der Inhalt so verwendet werden?

Grün · öffentlich

Bewusst veröffentlichte, öffentliche Inhalte (Medienmitteilung, Website, Reglement). Frei nutzbar; im Job in Varios.

Gelb · intern

Interne Inhalte ohne Personendaten und ohne Vertrauliches (Vorlage, Checkliste). **Nur in Varios eingeben.**

Rot · sensibel

Persönliche, sensible oder vertrauliche Angaben — auch vertrauliche Sachthemen ohne Namen. **So nie in die KI.**

Gelb-Check · 3 Fragen

Fall wirkt harmlos? Trotzdem alle 3 Fragen prüfen. Schon **ein Ja = Rot** → erst entschärfen.

1. Ist eine Person erkennbar — durch den Namen (direkt) oder über mehrere Hinweise (indirekt)?

ja → ROT

2. Geht es um ein sensibles oder vertrauliches Thema (Gesundheit, Finanzen, Personal, laufender Fall)?

ja → ROT

3. Ist die Information nur für wenige Personen bestimmt und nicht breit bekannt?

ja → ROT



Mosaik-Prinzip: Einzelne Hinweise (Funktion, Abteilung, Zeit, Ereignis) sind harmlos — zusammen machen sie eine Person doch erkennbar.

3 Werkzeuge · bei Rot

Von Hand, **ausserhalb der KI**. Wahl je nach Aufgabe.

Anonymisieren

Alle Angaben entfernen, die zur Person führen — auch mit Zusatzwissen nicht mehr auflösbar. «Maria Müller, Bahnhofstr. 12» → «eine Bürgerin».

Pseudonymisieren

Angaben durch Platzhalter ersetzen; die Zuordnung behältst du separat. **Nicht automatisch anonym** — Mosaik prüfen. «Herr Meier» → «[NAME]».

Aggregieren

Statt einem Einzelfall nur die Menge oder das Muster nennen. «Mehrere Bürger:innen fragten zu Thema X».



Die KI muss meist nicht wissen, **um wen** — nur **worum** es geht.

4 Lecks · in Dateien

Nicht nur der Prompt — auch **Uploads** tragen Heikles.

Restname

In einer alten Vorlage steht noch der echte Name einer Person.

Metadaten

Unsichtbar in der Datei: Kommentare, frühere Änderungen, Namen der Bearbeitenden.

Veraltete Quelle

Altes Merkblatt oder alte Version → KI übernimmt falsche Fristen oder Regeln.

Prompt Injection

In der Datei versteckter Befehl an die KI (z. B. «Ignoriere alle Regeln») — v. a. bei Dateien von aussen.

Vor jedem Upload: Braucht die KI die Datei? Ist sie sauber & aktuell?

1 · Richtige Umgebung: Varios

2 · Erst prüfen (Ampel)

3 · Nur so viel wie nötig

4 · Rot ausserhalb vorbereiten

5 · Ergebnis prüfen & lokal ergänzen