

Datenschutz-Grenzfälle sicher meistern

Anleitungskarte zur Etappe · für KI-Praktiker:innen — ergänzt die Pfad-1-Karte, ersetzt sie nicht.

Die KI-Ampel · Auffrischung Pfad 1



Grün — öffentlich, kein Personenbezug → nutzbar (zuerst Varios)

Gelb — intern, ohne Schutzbedarf → nur in Varios

Rot — Personendaten / Sensibles → erst anonymisieren

Sicher arbeiten – drei Sicherheitschecks



① Vor der Eingabe

Schwerpunkt

Was gebe ich ein? → Ampel · bei Gelb: Gelb-Check + Mosaik · bei Rot: zuerst anonymisieren.



② Bei Grenzfällen

Gelb-Check

Wirkt «intern/harmlos»? Genauer hinschauen: Könnte eine Person übers **Mosaik** erkennbar sein?



③ Vor der Verwendung

Was übernehme ich aus der KI? Stimmt es? Ist es fair? Darf ich es so verwenden?

Gelb-Check · 5 Fragen

«Intern» ≠ «harmlos». **Nicht sicher?** → alle fünf Fragen der Reihe nach prüfen.

1. Person direkt oder indirekt (Mosaik) erkennbar?

ja → ROT

2. Sensibel/vertraulich — Gesundheit, Finanzen, Sozialhilfe, Konflikt, Personal?

ja → ROT

3. Nur für wenige Personen bestimmt? Kleiner Kreis = eher vertraulich.

eher ROT

4. Braucht die KI wirklich alle Angaben?

nein → kürzen

5. Ist Varios der richtige, erlaubte Ort?

Arbeit → VARIOS

Der Mosaik-Effekt

Kein Name heisst nicht anonym — mehrere harmlose Hinweise ergeben zusammen eine eindeutig erkennbare Person.

Beispiel: «Sachbearbeiterin im Bauamt, Aussenstelle Ost, Mitte fünfzig, im Februar Konflikt mit der Vorgesetzten.» Kein Name — und doch wissen im Team alle, wer gemeint ist.

Faustregel: Je kleiner der Kreis möglicher Personen — weniger als eine Handvoll — desto eher wie **Rot** behandeln.



NOTBREMSE

Unsicher? **Nicht eingeben** — zuerst klären.

3 Wege · bei Rot

Rot trotzdem nutzbar machen — **von Hand, am Original**, bevor die KI etwas sieht.

Weglassen

Alles streichen, was die Aufgabe nicht braucht — Namen, Adressen, genaue Orte, Daten.

Anonymisieren

So ändern, dass niemand mehr direkt oder indirekt erkennt, wer gemeint ist. **Name ersetzen reicht nicht.**

Zusammenfassen

Einzelfall → allgemeine Aussage. «Drei Mitarbeitende meldeten hohe Belastung.»



Zuerst bearbeiten, dann eingeben — nie das Original hineinkopieren und die KI anonymisieren lassen.

Pseudonym ≠ anonym

Ein anderer Name macht einen **roten Fall nicht automatisch gelb**.

Pseudonymisieren

Name → Platzhalter. «Maria Müller» → «Person A». Solange eine Zuordnung existiert oder der Kontext verrät, wer gemeint ist, bleiben es **Personendaten**.

Erst wirklich anonym ...

... wenn niemand mehr herausfindet, wer gemeint ist. «Eine Person aus der Verwaltung» ist sicherer als «Person A».



DLP in Varios warnt bei Namen, Adressen, Nummern — ein Sicherheitsnetz, keine Freigabe. Keine Warnung heisst nicht «erlaubt». **Die Entscheidung bleibt bei dir.**