

# Verfahren statt Bauchgefühl

## Lerngruppentreffen zur Etappe: Datenschutz-Grenzfälle

### Worum geht es?

Bei klaren Fällen reicht die KI-Ampel. Schwierig wird der **gelbe Bereich**, denn «intern» heisst nicht automatisch «harmlos». Genau hier verlässt man sich oft aufs Bauchgefühl, und genau hier passieren Fehler. Heute macht ihr daraus ein **Verfahren**: Zuerst seht ihr, dass die Varios-Warnung ein **Netz mit Löchern** ist. Darum prüft ihr Grenzfälle mit dem **Gelb-Check**, durchschaut den **Mosaik-Effekt** und macht heikle Inhalte mit **drei Werkzeugen** wieder nutzbar.

**Dauer:** ca. 45 Minuten (Tipp: Bestimmt eine Person, die auf die Zeit achtet; die Moderation rotiert von Aufgabe zu Aufgabe.)

### Nach dieser Lerneinheit könnt ihr

- Grenzfälle mit dem **Gelb-Check** (fünf Fragen) nach einem festen Verfahren einordnen, statt nach Bauchgefühl.
- den **Mosaik-Effekt** erkennen: wann einzelne harmlose Angaben zusammen eine Person verraten, und warum eine Varios-Warnung (DLP) nicht alles fängt.
- heikle Inhalte durch **Weglassen, Anonymisieren und Zusammenfassen** entschärfen, und erklären, warum «Person A» noch nicht anonym ist.

### Ablauf

| ABLAUF                                                 | ZEIT           |
|--------------------------------------------------------|----------------|
| Einstieg ins Thema (Ankommen · Rückblick · Lernimpuls) | <b>4 Min.</b>  |
| Aufgabe 1: Varios & die DLP-Grenze                     | <b>4 Min.</b>  |
| Aufgabe 2: Der Gelb-Check an Grenzfällen               | <b>13 Min.</b> |
| Aufgabe 3: Die Anonymisier-Werkstatt                   | <b>15 Min.</b> |
| Reflexion: Erlebtes einordnen                          | <b>4 Min.</b>  |
| Einzelauftrag bis zum nächsten Mal                     | <b>2 Min.</b>  |

**Zeitplan:** Eng auf 45 Minuten gerechnet, bestimmt jemanden für die Zeit. Kern sind der Gelb-Check und die Anonymisier-Werkstatt. Von den fünf Fällen sind der erste (grün) und der zweite (gelb) schnelle Anker, nehmt euch die Zeit fürs Begründen bei den drei roten Grenzfällen.

### Was ihr für heute braucht

Ihr braucht **dieses Lerndossier** und **Varios** für Aufgabe 1. Öffnet es am besten schon jetzt: **varios.uster.ch**, Anmeldung mit eurem Uster-Login. Die **Anleitungskarte «Datenschutz-Grenzfälle»** steht im Lernportal direkt unter dem Lerndossier zum Download bereit. Sie fasst KI-Ampel, Gelb-Check und die drei Werkzeuge auf einer Seite zusammen. Legt sie offen daneben, sie ist euer Spickzettel.

### Einstieg ins Thema (ca. 4 Min.)

Startet gemeinsam: Ihr kommt zuerst an, schaut kurz auf euren Einzelauftrag aus dem letzten Treffen zurück und verbindet das Erlebte mit dem Lernimpuls. Es geht nicht um richtige Antworten, sondern darum, eure Arbeitsweisen sichtbar zu machen.

**Tipp:** Tauscht euch reihum aus, offen und ohne Bewertung. In 4 Minuten schafft ihr etwa **zwei Fragen**: eine zum Rückblick auf den Einzelauftrag und eine zum heutigen Lernimpuls.

### 1 · Zum Ankommen

---

- Auf einer Skala von 0 bis 10: Wie ist meine Gefühlslage heute im Umgang mit KI ganz allgemein?
- Hatte ich seit dem letzten Treffen ein Erlebnis mit KI, das ich mit der Lerngruppe teilen möchte?

### 2 · Rückblick auf den Einzelauftrag

---

- Habe ich den Einzelauftrag ausprobiert? Wenn ja: woran? Wenn nein: was ist dazwischengekommen?
- Was hat gut funktioniert, und wo bin ich auf Schwierigkeiten gestossen?

### 3 · Zum Lernimpuls

---

- Wann ist mir schon einmal etwas «Internes» begegnet, das eigentlich heikel war?
- «Verfahren statt Bauchgefühl»: was würde sich ändern, wenn ich Grenzfälle immer mit einem festen Verfahren prüfe statt nach Gefühl?

Platz für Notizen oder Gedanken

### Aufgabe 1: Varios & die DLP-Grenze (ca. 4 Min.)

Varios hat eine eingebaute Hilfe: Vermutet das System persönliche Daten in eurer Eingabe, kann eine Warnung erscheinen (**DLP**, «Data Loss Prevention»). Ihr löst sie einmal selbst aus und schaut dann, wo dieser Schutz an seine Grenzen kommt.

#### So probiert ihr es aus (an einem Gerät genügt)

- Öffnet **Varios** und startet einen neuen Chat.
- Tippt einen Test-Prompt mit **erfundenen** Personendaten ein, zum Beispiel den unten stehenden.
- Beobachtet, **ob und wie** Varios auf die Eingabe reagiert: Erscheint eine Warnung? Welche Angaben scheint das System erkannt zu haben? Ihr müsst nichts abschicken.

#### TEST-PROMPT (ERFUNDENE ANGABEN)

«Schreibe eine kurze, freundliche Antwort an Tim Koller, Seestrasse 4, zu seiner Anfrage beim Einwohneramt.»

*Alles frei erfunden, hier stecken bewusst keine echten Personendaten drin.*

*Falls keine Warnung erscheint: Auch das ist ein Ergebnis: DLP erkennt nicht jede heikle Information.*

#### → Besprecht in der Gruppe:

- Was habt ihr gesehen: wann und wie hat Varios gewarnt?
- Würde Varios auch warnen bei «der einzigen Sachbearbeiterin im Bauamt, Aussenstelle Ost, die im Februar einen Konflikt hatte»? Da steht kein Name, also vermutlich nicht.

Was uns die Warnung zeigt, und wo sie an Grenzen kommt:

**Darum geht es weiter:** DLP ist ein Netz mit Löchern: Es erkennt typische Angaben wie Namen oder Adressen, aber nicht zuverlässig jeden Namen und nicht den ganzen Zusammenhang (etwa den Mosaik-Fall). **Keine Warnung heisst nicht «erlaubt».** Bei Grenzfällen braucht ihr darum ein Verfahren statt Bauchgefühl: den **Gelb-Check**. Den übt ihr jetzt in Aufgabe 2.

## Aufgabe 2: Der Gelb-Check an Grenzfällen (ca. 13 Min.)

«Intern» ist nicht gleich «harmlos». Mit dem Gelb-Check prüft ihr jeden Grenzfall nach einem festen Verfahren, mit denselben fünf Fragen wie im Lernimpuls. **Ein Ja bei Frage 1, 2 oder 3 macht den Fall rot.** Erst wenn diese drei klar mit Nein beantwortet sind, unnötige Angaben entfernt wurden und Varios der richtige Ort ist, bleibt der Fall **gelb** (nur Varios).

### Der Gelb-Check: fünf Fragen

- 1 **Ist eine Person direkt oder indirekt erkennbar?** Name oder über das Mosaik (Funktion, Ort, Zeitpunkt, Ereignis)? – **Rot**
- 2 **Geht es um sensible oder vertrauliche Themen?** Gesundheit, Finanzen, Sozialhilfe, Personalthemen, Konflikte, laufende Verfahren? – **Rot**
- 3 **Ist der Inhalt besonders vertraulich oder noch nicht freigegeben?** Interne Entscheide, Bewertungen, Vergaben, laufende Verfahren (oft nur für einen kleinen Kreis)? – **Rot** bzw. stoppen und die zuständige Vorgesetzte/den Vorgesetzten oder die Datenschutzstelle fragen
- 4 **Braucht die KI wirklich alle Angaben?** Wenn nein: unnötige Angaben entfernen und den Fall neu einstufen.
- 5 **Ist Varios der richtige und erlaubte Ort?** Nein oder unsicher: stoppen und nachfragen. Ja: mit der bereinigten Fassung weiterarbeiten.

Bleibt der Fall **gelb**, arbeitet ihr nur in Varios damit. Der Gelb-Check steht auch auf der **Anleitungskarte «Datenschutz-Grenzfälle»**, im Lernportal unter dem Lerndossier zum Download.

**So entscheidet ihr, erst allein, dann gemeinsam:**

● **GRÜN** = Daumen hoch    ● **GELB** = flache Hand    ● **ROT** = Faust

### So geht ihr vor

1. Eine Person liest den Fall vor. Auf «drei» zeigt jede:r zuerst **allein** die Finger-Ampel, ohne zu schielen.
2. Dann geht ihr den Fall gemeinsam durch die fünf Fragen, einigt euch auf eine Farbe und haltet fest, **welche Frage** den Ausschlag gibt.
3. Weiter mit dem nächsten Fall. Die Auflösung steht im **Lösungscheck am Ende des Dossiers**.

*Fälle 1 und 2 sind schnelle Anker, prüft sie kurz. Bei den Fällen 3 bis 5 geht ihr den vollständigen Gelb-Check durch. Hier zählt nicht Tempo, sondern das **Begründen**; dass ihr euch nicht immer einig seid, ist normal, genau daran zeigt sich, wie der Gelb-Check hilft.*

## Fall · Verwaltungsalltag

1. Ihr lasst die KI eine **bereits auf der Website veröffentlichte Medienmitteilung** der Stadt zu fünf Stichpunkten zusammenfassen. (Schneller Anker, die Antwort ist klar.)

## Unsere Einordnung

☐ Grün

☐ Gelb

☐ Rot

## Welche Frage?

2. Ihr lasst die KI das **Protokoll der letzten Teamsitzung** zu fünf Stichpunkten zusammenfassen: Termine, Zuständigkeiten, ein neuer Ablageordner. Keine Konflikte, keine Personendaten.

☐ Grün

☐ Gelb

☐ Rot

3. Ihr entwerft eine freundliche **Antwort-E-Mail an Herrn Brunner**, der sich nach dem Stand seiner Baubewilligung erkundigt hat.

☐ Grün

☐ Gelb

☐ Rot

★ 4. Ihr fasst einen internen Vermerk zusammen: «*die einzige Sachbearbeiterin im Bauamt, Aussenstelle Ost, Mitte fünfzig, hatte im Februar einen Konflikt mit ihrer Vorgesetzten*», **kein Name** im Text.

☐ Grün

☐ Gelb

☐ Rot

5. Ihr lasst die KI die **internen Bewertungen der drei Offerten** für die Schulhaus-Sanierung vergleichen, noch **bevor** der Zuschlag entschieden ist.

☐ Grün

☐ Gelb

☐ Rot

★ Fall 4 ist der Mosaik-Fall: kein Name, und trotzdem im kleinen Umfeld sofort erkennbar.

→ **Besprecht zum Schluss:** Bei welchem Fall wart ihr euch uneinig, und welche Frage hat die Entscheidung gebracht?

### Aufgabe 3: Die Anonymisier-Werkstatt (ca. 15 Min.)

Rot heisst: den Originaltext **nicht** eingeben. Prüft zuerst, ob sich die Aufgabe durch **Weglassen**, **Anonymisieren** oder **Verallgemeinern** sicher bearbeiten lässt, von Hand, am Original, bevor die KI ihn sieht. Manche Fälle bleiben auch danach ungeeignet, dann stoppt ihr und fragt nach.

**Die Aufgabe:** Ihr wollt die KI einen **kurzen, sachlichen Text** formulieren lassen, zum Beispiel einen internen Vermerk oder eine Antwort, wie mit einer Pensumsreduktion nach einer Abwesenheit umzugehen ist. Die KI hilft beim **Formulieren** und muss dafür weder den Namen noch die Gesundheitsangabe kennen. Genau deshalb macht ihr den Fall zuerst sicher: Sie erfährt nur, **worum** es geht, nicht **um wen**. Am Schluss formuliert ihr daraus den **fertigen KI-Auftrag** — den Prompt, den ihr wirklich in Varios eingibt.

Euer Original (rot, bitte **nicht** so in die KI geben):

Tim Koller, 34, Sachbearbeiter Einwohnerdienste, war letzte Woche wegen seiner Diabetes-Erkrankung drei Tage abwesend und möchte sein Pensum neu auf 80 % reduzieren.

*Alle Namen und Angaben in diesem Übungsfall sind frei erfunden.*

Arbeitet denselben Fall mit jedem der drei Werkzeuge um. Ziel: am Schluss bleibt nur noch **eine kurze, sichere Fassung**.

| Werkzeug                                                                                                                                   | Eure Fassung |
|--------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <b>Weglassen &amp; reduzieren</b><br><i>alles streichen, was die KI nicht braucht (Name, Alter, Rolle, genaues Datum)</i>                  |              |
| <b>Anonymisieren</b><br><i>den Text so ändern, dass niemand mehr direkt oder indirekt erkennt, wer gemeint ist</i>                         |              |
| <b>Zusammenfassen / verallgemeinern</b><br><i>den Einzelfall zu einer allgemeinen Situation machen, ohne zu behaupten, sie sei typisch</i> |              |

Die drei Werkzeuge sind keine starren Alternativen, in der Praxis kombiniert ihr sie oft: zuerst Unnötiges weglassen, danach anonymisieren oder die Situation allgemeiner zusammenfassen.

★ **Stolperfalle Pseudonymisieren:** Nur den Namen durch «Person A» zu ersetzen, macht den Fall **nicht** sicher. Solange man über den Rest (Rolle, Ort, Zeit, Ereignis) auf die Person schliessen kann, bleibt er **rot**. Darum ist Pseudonymisieren **kein** vollwertiges Schutzwerkzeug, es steht bewusst nicht in der Liste oben.

→ **Entscheidet gemeinsam:** Welche eurer drei Fassungen ist wirklich sicher genug für Varios? Prüft besonders: Verrät der Rest-Kontext die Person immer noch?

*Unsere sichere Fassung (nur worum es geht, nicht um wen):*

### Euer KI-Auftrag: so gebt ihr ihn in Varios ein

Das ist der eigentliche Schritt: Ihr lasst die KI den Text jetzt wirklich schreiben. Dafür formuliert ihr **einen Prompt**, der die Aufgabe löst **und** den Datenschutz einhält — eine klare Anweisung (*was die KI tun soll*) **plus eure sichere Fassung** als Grundlage. Keine echten Namen, keine Gesundheitsangaben.

#### SO KÖNNTE EUER PROMPT BEGINNEN

«Du bist Sachbearbeiter/in der Einwohnerdienste. Formuliere eine kurze, freundliche und sachliche Antwort auf die folgende Anfrage. Erfinde keine Angaben. — Anfrage: [hier eure sichere Fassung einsetzen]»

*Unser vollständiger Prompt für Varios:*

**Und danach?** Die KI liefert einen Entwurf. Die echten Angaben (Name, genaue Umstände) ergänzt ihr **erst danach von Hand** — ausserhalb der KI. So löst ihr die Aufgabe, ohne je einen roten Originalfall einzugeben.

**Merksatz:** Ein anderer Name macht einen roten Fall nicht automatisch gelb. Solange der Restkontext (hier Gesundheit, Rolle, Alter, Abwesenheit, Pensum) die Person erkennen lässt, bleibt der Fall **rot**. Im Zweifel das stärkere Werkzeug wählen oder nachfragen.

### Reflexion: Erlebtes einordnen (ca. 4 Min.)

Nehmt euch zum Abschluss bewusst Zeit, das Erlebte einzuordnen. Sprecht in der Gruppe über die folgenden Fragen. Es geht nicht darum, fertige Antworten zu haben, sondern darum, einen ehrlichen Blick auf eure eigene Erfahrung zu werfen.

**Tipp:** Wählt zwei bis drei Fragen aus, die euch besonders ansprechen.

### Zum Erlebten

---

- Was habe ich in dieser Phase über den Umgang mit Daten und KI gelernt?
- Was ist mir leichtgefallen, was war schwierig?
- Wo war ich überrascht – positiv oder negativ?
- Welche Erkenntnis nehme ich für den nächsten Versuch mit?

### Zum Umgang mit heiklen Daten in der KI

---

Schaut nun nochmal auf den Gelb-Check und den Umgang mit Grenzfällen zurück.

- Welcher Fall war am schwierigsten einzuordnen, und warum?
- Wo hätte mich mein Bauchgefühl getäuscht, das Verfahren aber nicht?
- Was war neu für mich am Mosaik-Effekt oder an den drei Werkzeugen (Weglassen · Anonymisieren · Zusammenfassen)?

### Zur eigenen Gefühlslage

---

- Wie geht es mir jetzt, nach dem ersten eigenen Ausprobieren? Hat sich etwas verändert im Vergleich zum Anfang?
- Fühle ich mich sicherer, neugieriger – oder vielleicht auch verunsicherter?
- Gibt es etwas, das mich beschäftigt oder ins Nachdenken bringt?
- Was würde mir helfen, mich beim Arbeiten mit KI wohler zu fühlen?

Mein wichtigster Schritt – und meine nächste Aufgabe mit KI:

## Einzelauftrag bis zum nächsten Mal: Mein Verfahren im Alltag

Damit das Verfahren sitzt, nimmst du einen kleinen Auftrag mit. Wähle eine Stufe, die zu dir passt, es gibt kein «richtiges» Level.

**Wichtig:** Gib niemals einen roten Originalfall in ein KI-Tool ein. Beschreibe deine Beispiele allgemein und ohne echte Personendaten.

### BASIS: Zehn Eingaben sortieren (ca. 15 Min., über 2 Wochen)

**Ziel:** Die Ampel-Einstufung im Alltag automatisieren.

Sammele nach und nach zehn Eingaben, die du einer KI gegeben hast oder geben würdest. Ordne jede mit dem Gelb-Check ein und halte bei jeder roten Eingabe fest, **welche** der fünf Fragen den Ausschlag gibt.

**Datenschutz:** Notiere nur die **Art** der Eingabe, nicht den ursprünglichen Text. Falls du nicht zehn echte Eingaben hast: Nimm geplante Aufgaben und ordne ein, welche Ampelfarbe sie hätten.

| Eingabe / Aufgabe (allgemein beschrieben) | Ampel             | Welche Frage gab den Ausschlag? |
|-------------------------------------------|-------------------|---------------------------------|
|                                           | Grün / Gelb / Rot |                                 |
|                                           | Grün / Gelb / Rot |                                 |
|                                           | Grün / Gelb / Rot |                                 |
|                                           | Grün / Gelb / Rot |                                 |
|                                           | Grün / Gelb / Rot |                                 |
|                                           | Grün / Gelb / Rot |                                 |
|                                           | Grün / Gelb / Rot |                                 |
|                                           | Grün / Gelb / Rot |                                 |

**VERTIEFT: Drei Grenzfälle einordnen und einen entschärfen** (ca. 25 Min.)

**Ziel:** Vom Einordnen zum sicheren Umarbeiten kommen.

Nimm drei echte Grenzfälle aus deinem Bereich (allgemein beschrieben), ordne sie mit dem Gelb-Check ein und **anonymisiere einen davon** zu einer kurzen, sicheren Fassung. Achte auf den Mosaik-Effekt: Reicht das Streichen des Namens, oder verraten Funktion, Ort und Zeit die Person trotzdem? Arbeite am Original, von Hand, nur die bereinigte Fassung kommt in die KI.

| Grenzfall (allgemein beschrieben) | Ampel             | Welche Frage? |
|-----------------------------------|-------------------|---------------|
|                                   | Grün / Gelb / Rot |               |
|                                   | Grün / Gelb / Rot |               |
|                                   | Grün / Gelb / Rot |               |

Mein anonymisierter Fall (kurze, sichere Fassung für die KI):

## CHALLENGE: Fünf Gelb-Regeln für eure Abteilung (ca. 40 Min.)

**Ziel:** Aus dem Verfahren konkrete Regeln für euer Team machen.

Formuliere fünf konkrete Gelb-Regeln für deine Abteilung: typische Grenzfälle, die bei euch immer wieder vorkommen, und die sichere Handlung dazu (keine allgemeinen Floskeln). Die Regeln sind ein **Entwurf**: Stimme sie vor einer offiziellen Verwendung mit der zuständigen Anlaufstelle (Datenschutz, Vorgesetzte) ab und bring sie zum nächsten Treffen mit.

| Typischer Grenzfall bei uns | Sichere Handlung (unsere Gelb-Regel) |
|-----------------------------|--------------------------------------|
|                             |                                      |
|                             |                                      |
|                             |                                      |
|                             |                                      |
|                             |                                      |

### Brücke zur nächsten Etappe

Denke bei deinen Grenzfällen zusätzlich kurz darüber nach:

«Welche wiederkehrende Aufgabe würde ich am liebsten einmal sauber einrichten, statt sie jedes Mal neu zu prompten?»

Diese Frage nehmt ihr in die nächste Etappe mit. Dort baut ihr euch **persönliche KI-Assistenten** für wiederkehrende Aufgaben.

**Lösungsscheck zum Gelb-Check** erst nach eurer eigenen Einordnung in Aufgabe 2 lesen.

**Fall 1 – Grün:** bereits öffentlich, keine der fünf Fragen greift. · **Fall 2 – Gelb:** intern, aber keine Person und nichts Vertrauliches (Fragen 1 bis 3 = Nein), nur in Varios. · **Fall 3 – Rot** (Frage 1): Person direkt erkennbar (Name). · **Fall 4 – Rot** (Frage 1 + 2): über das Mosaik indirekt erkennbar, dazu ein Konflikt. · **Fall 5 – Rot** (Frage 2 + 3): vertrauliche interne Bewertung, laufendes Vergabeverfahren.

**Merksatz:** Verfahren statt Bauchgefühl: bei Grenzfällen entscheidet nicht das Gefühl, sondern der Gelb-Check. Übt heute und im Einzelauftrag nur mit Texten ohne echte Personendaten.