

Sofort-Checkliste: KI-Datenschutzvorfall

Was in den ersten 72 Stunden zu tun ist — ruhig, priorisiert, ohne Panik.

DIE 72-STUNDEN-UHR



STUNDE 0

Entdeckung

Die Frist beginnt, sobald das Unternehmen Kenntnis erlangt.



STUNDE 0–24

Sichern & Einordnen

Zugriff stoppen, dokumentieren, Risiko bewerten.



BIS STUNDE 72

Melden — falls nötig

Meldung an die Datenschutzbehörde (DSGVO Art. 33).

• DIE 5 SCHRITTE — IN DER RICHTIGEN REIHENFOLGE

1 Stoppen & Sichern



Weitere Verbreitung sofort stoppen: geteilten Chat-Link deaktivieren, betroffenen API-Key widerrufen oder rotieren. Nichts löschen, was als Beweis dient.

2 Dokumentieren & Einordnen



Was wurde wann von wem in welches Tool eingegeben? Screenshots, Zeitstempel, Beteiligte festhalten. Dann klären: Personenbezug, Geschäftsgeheimnis oder beides? Sensible Daten? — Daraus folgt, ob die 72-Stunden-Uhr tickt.

3 Anbieter kontaktieren



Löschung der Eingaben und Logs schriftlich anfordern und bestätigen lassen. Prüfen, ob die Trainings-Nutzung deaktiviert werden kann (Opt-out). Bei US-Anbietern zusätzlich Rechtsgrundlage & AV-Vertrag prüfen.

4 Melden — wenn nötig (72-Stunden-Frist)



Bei Risiko für betroffene Personen: Meldung an die Datenschutzbehörde nach Art. 33 vorbereiten. Bei hohem Risiko zusätzlich die Betroffenen informieren (Art. 34). Auch eine begründete Nicht-Meldung dokumentieren.

5 Vorbeugen



Damit derselbe Vorfall nicht in zwei Wochen wieder passiert: eine schlanke KI-Nutzungsregel und ein freigegebenes, sicheres Tool bereitstellen, bei dem Eingaben nicht ins Training wandern.

Die Entscheidungslogik

1 • Personenbezogene Daten betroffen?

Nein → DSGVO-Meldung meist nicht einschlägig

NICHT EINSCHLÄGIG. Relevant bleiben
Geschäftsgeheimnis-Schutz & Verträge.

2 • Risiko für die betroffenen Personen?

Ja → Meldung an die Datenschutzbehörde, Art. 33,
binnen 72 h **ART. 33**.

3 • Hohes Risiko (sensibel/identifizierbar)?

Ja → zusätzlich die Betroffenen informieren, Art. 34
ART. 34.

Do & Nicht

- ✓ Alles dokumentieren — auch die Risikoabwägung.
- ✓ Löschung & Training-Opt-out schriftlich anfordern.
- ✓ Im Zweifel Frist als laufend behandeln.
- ✗ Den Vorfall vertuschen oder aussitzen.
- ✗ Ohne Dokumentation „aus dem Bauch“ entscheiden.
- ✗ Betroffene bei hohem Risiko im Unklaren lassen.

● IHRE NOTFALL-KONTAKTE – JETZT AUSFÜLLEN, BEVOR ES BRENNT

INTERNE:R VERANTWORTLICHE:R /
DSB

ANBIETER-SUPPORT / LÖSCHUNG

ZUSTÄNDIGE DATENSCHUTZBEHÖRDE **Österreich:** Datenschutzbehörde (DSB) · dsb.gv.at | **DE:** Landesbehörde

EXTERNE SOFORTHILFE **Thomas Stermole** — thomas@stermole.at · stermole.at

Tipp: Diese Zeilen einmal ausfüllen, ausdrucken und griffbereit ablegen. Im Ernstfall zählt jede Minute.

● NÄCHSTER SCHRITT

Unsicher, ob Ihr Fall meldepflichtig ist?

Der interaktive Vorfall-Wizard ordnet Ihre Situation in 5 Fragen ein —
inklusive Einschätzung zur 72-Stunden-Frist.

**STERMOLE.AT/
LEISTUNGEN/
KI-VORFALL-SOFORTHILFE**

Hinweis: Diese Checkliste ist eine allgemeine Orientierungshilfe und ersetzt keine individuelle Rechts- oder Datenschutzberatung. Für verbindliche Bewertungen — insbesondere zu Meldepflichten nach DSGVO Art. 33 und 34 sowie den Vorgaben des EU AI Act — binden Sie bitte Ihre:n Datenschutzbeauftragte:n oder eine:n Jurist:in ein. © 2026 Thomas Stermole · Souveräne KI für KMU.