// KI-Hub VON STRUKTURAFLOW

IT-SECURITY

KI-Workflow Notfallplan bei Datenpanne: KMU-Vorlage

Vorlage für KMU: KI-Datenpanne erkennen, bewerten und DSGVO-konform melden — mit RACI-Matrix und Mustertexten für DE/AT/CH.

AUTOR
Strukturaflow-Team

VERÖFFENTLICHT
2. August 2026

ONLINE LESEN

https://wissen.strukturaflow.it.com/ki-workflow-notfallplan-datenpanne-kmu-vorlage/

Ein Make-Workflow sendet Kundendaten irrtümlich an einen externen KI-Dienst — der API-Key war falsch zugeordnet, der Fehler fällt erst zwei Stunden später auf. Was jetzt? Die DSGVO-Meldefrist beträgt 72 Stunden ab Kenntnis, und die Uhr läuft bereits. Klassische IT-Notfallpläne helfen hier kaum weiter: Sie kennen keine API-Subprozessoren, keine LLM-Trainingsdaten und keine Zapier-Datenpfade.

Dieser Artikel liefert eine strukturierte Vorlage für genau diesen Fall — aufgeteilt in vier chronologische Phasen, mit einer RACI-Matrix für KMU ohne eigene IT-Abteilung, behördenkonformen Mustertexten für DE/AT/CH und einem 90-Minuten-Aufsetzen-Guide. Alles direkt verwendbar, kein Rechtsstudium vorausgesetzt.

Was eine KI-Datenpanne von einer klassischen IT-Panne unterscheidet

Nach Art. 4 Nr. 12 DSGVO ist eine Datenschutzverletzung jede Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Weitergabe personenbezogener Daten führt — unabhängig davon, ob ein Angreifer beteiligt war oder der Fehler intern passiert ist. Art. 33 und 34 DSGVO regeln, wann und wie gemeldet werden muss.

Der Unterschied zu einer klassischen IT-Panne liegt im Datenpfad. Bei einem kompromittierten Server gibt es Logs, Firewall-Einträge und klare Systemgrenzen. Bei einem KI-Workflow verlassen Daten das eigene System über APIs, landen bei Drittanbietern in anderen Rechtsräumen und werden möglicherweise für Modell-Training verwendet — ohne dass ein einziger Firewall-Eintrag entsteht.

Zu den wachsenden Bedrohungen durch KI-gestützte Angriffsvektoren — darunter auch Ransomware — lesen Sie unseren Artikel zu KI-automatisierter Ransomware für KMU.

Die häufigsten KI-Datenpannen-Szenarien in KMU

Szenario 1: ChatGPT-Prompt enthält echte Kundendaten. Eine Mitarbeiterin kopiert eine Kundenanfrage inklusive Name, Adresse und Auftragsnummer in ChatGPT, um eine Antwort zu formulieren. Diese Daten können in OpenAIs Systemen gespeichert und für weitere Zwecke verarbeitet werden — je nach Einstellung des Unternehmenskontos.

Szenario 2: Zapier oder Make sendet Daten an einen nicht-DSGVO-konformen Dienst. Ein Automatisierungsworkflow leitet Kontaktdaten aus einem CRM an einen US-Dienst weiter, für den kein Auftragsverarbeitungsvertrag (AVV) besteht. Der Workflow läuft seit Monaten, niemand hat ihn geprüft.

Szenario 3: n8n-Workflow loggt personenbezogene Daten in unsicherer Datenbank. Debugging-Logs enthalten Klarnamen und E-Mail-Adressen. Die Datenbank ist nicht verschlüsselt und für Dritte zugänglich — oft ein Nebenbefund bei Workflow-Audits.

Szenario 4: KI-Transkriptionstool speichert Meetings mit Kundendaten. Dienste wie Otter.ai oder ähnliche Tools nehmen Kundengespräche auf und transkribieren sie auf externen Servern. Viele KMU wissen nicht, wo diese Daten gespeichert werden oder wie lange. Eine DSGVO-konforme Alternative für Meeting-Transkriptionen finden Sie im Artikel zu Fireflies-Alternativen für KMU.

Die 72-Stunden-Uhr – DSGVO-Meldepflichten im Überblick

Art. 33 DSGVO verpflichtet Verantwortliche, eine Datenschutzverletzung der zuständigen Aufsichtsbehörde „unverzüglich und möglichst binnen 72 Stunden" zu melden. Die Frist startet mit der „Kenntnis" — dazu gleich mehr. Wenn die Meldung nicht innerhalb von 72 Stunden erfolgt, muss die Verzögerung begründet werden.

Art. 34 DSGVO ergänzt: Wenn die Verletzung voraussichtlich ein „hohes Risiko" für die Rechte und Freiheiten natürlicher Personen mit sich bringt, müssen auch die betroffenen Personen direkt benachrichtigt werden — ohne unangemessene Verzögerung. Was „hohes Risiko" bedeutet, hängt von Datenmenge, Datenkategorie und Missbrauchspotenzial ab.

Behördliche Anlaufstellen nach Land

Deutschland: Die Zuständigkeit liegt bei den Datenschutzbehörden der Bundesländer — je nach Unternehmensstandort. Eine vollständige Übersicht findet sich auf der Website der Datenschutzkonferenz (DSK). Für Unternehmen mit Sitz in Bayern ist das BayLDA, in Baden-Württemberg der LfDI, in NRW die LDI NRW — und so weiter.

Österreich: Zuständig ist die Datenschutzbehörde (DSB) mit Sitz in Wien. Die Meldung erfolgt über das Online-Formular auf dsb.gv.at. Besonderheit: Die 72-Stunden-Frist läuft auch an Wochenenden und Feiertagen durch — es gibt keine gesetzliche Fristunterbrechung. Wer freitags von einer Panne erfährt, muss spätestens am Montag früh gemeldet haben.

Schweiz: Seit dem neuen Datenschutzgesetz (nDSG, in Kraft seit September 2023) besteht eine Meldepflicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) — ebenfalls binnen 72 Stunden ab Kenntnis, wenn voraussichtlich ein hohes Risiko für die betroffenen Personen besteht.

Was passiert bei gerissener Frist? Der Bußgeldrahmen nach DSGVO liegt bei bis zu 10 Mio. Euro oder 2 % des weltweiten Jahresumsatzes — je nachdem, was höher ist. In der Praxis fallen Bußgelder für KMU bei erstmaligem Verstoß und nachweislicher Kooperationsbereitschaft deutlich niedriger aus. Trotzdem: Verspätete Meldungen mit plausibler Begründung werden besser bewertet als keine Meldung.

Die Notfallplan-Vorlage – Schritt für Schritt

Die folgende Vorlage ist in vier Phasen aufgeteilt, die chronologisch abgearbeitet werden. Jede Phase enthält Checklisten und Vorlagetexte, die Sie direkt auf Ihr Unternehmen anpassen können.

Phase 1 – Erkennung & erste 2 Stunden (0-120 Min.)

Das Wichtigste in dieser Phase: Ruhe bewahren, dokumentieren und den betroffenen Workflow sofort stoppen.

Sofortmaßnahmen:

- Make: Scenario öffnen → „Deactivate scenario“ klicken
- Zapier: Zap öffnen → Toggle oben rechts auf „Off“ schalten
- n8n: Workflow öffnen → „Deactivate“ im oberen Menü wählen

Interne Erste-Meldung (Vorlage):

FELD	EINTRAG
Datum / Uhrzeit der Entdeckung	
Entdeckt durch (Name, Funktion)	
Betroffener Workflow / Dienst	
Art der betroffenen Daten	
Geschätzte Anzahl betroffener Datensätze	
Empfänger der Daten (Dienst/Person)	
Sofortmaßnahmen bereits getroffen	
Koordination übernommen durch	

Diese Tabelle ist der Startpunkt Ihres Dokumentationsprozesses. Behörden erwarten bei einer Meldung nach Art. 33 DSGVO genau diese Informationen — je früher Sie sie zusammenführen, desto einfacher wird Phase 3.

Phase 2 – Bewertung & Entscheidung (2-8 Stunden)

In dieser Phase entscheiden Sie: Meldepflichtig oder nicht? Dafür brauchen Sie eine Risikoklassifizierung.

Risikobeurteilungsbogen:

FRAGE	JA	NEIN
Betreffen die Daten besondere Kategorien (Gesundheit, Religion, politische Meinung, biometrische Daten)?	Hoch	—
Sind mehr als 50 Personen betroffen?	Mittel+	Niedrig
Ist der Empfänger unbekannt oder unkontrolliert?	Hoch	—
Besteht ein realistisches Missbrauchspotenzial (Identitätsdiebstahl, Betrug)?	Hoch	—
Sind die Daten ohne Schlüssel nutzlos (verschlüsselt, pseudonymisiert)?	—	Niedrig

Ergebnis-Logik:

- **Niedrig:** Interne Dokumentation, keine Meldepflicht — aber dokumentieren, warum nicht
- **Mittel:** Meldung an Aufsichtsbehörde prüfen, rechtlichen Rat einholen
- **Hoch:** Meldung nach Art. 33 DSGVO verpflichtend, Art. 34 prüfen

Bei Unsicherheit gilt: Im Zweifel melden. Eine unnötige Meldung hat keine negativen Konsequenzen; eine versäumte schon.

Phase 3 – Meldung & Kommunikation (8-72 Stunden)

Mustertext Behördenmeldung (Art. 33 DSGVO) — anpassbar für DE/AT/CH:

> Betreff: Meldung einer Datenschutzverletzung gemäß Art. 33 DSGVO
>
> Verantwortlicher: [Firmenname], [Adresse], [Kontaktperson mit Funktion]
>
> Beschreibung der Verletzung: Am [Datum] um [Uhrzeit] wurde festgestellt, dass [kurze Beschreibung des Vorfalls]. Betroffen sind voraussichtlich [Anzahl] Personen. Bei den betroffenen Daten handelt es sich um [Datenkategorien].
>
> Ursache: [Technische/organisatorische Ursache, soweit bekannt]
>
> Bereits getroffene Maßnahmen: [z. B. Workflow deaktiviert, betroffene API-Verbindung getrennt, Passwörter zurückgesetzt]
>
> Geplante Maßnahmen: [z. B. Sicherheitsüberprüfung aller Workflows, Schulung der Mitarbeiter]
>
> Einschätzung des Risikos für betroffene Personen: [Niedrig / Mittel / Hoch — mit kurzer Begründung]
>
> [Datum, Unterschrift]

Mustertext Betroffenenbenachrichtigung (Art. 34 DSGVO) — nur bei hohem Risiko:

> Betreff: Information zu einem Datenschutzvorfall
>
> Sehr geehrte/r [Name],
>
> wir möchten Sie darüber informieren, dass es bei [Firmenname] am [Datum] zu einem Datenschutzvorfall gekommen ist. Dabei wurden möglicherweise folgende Daten betroffen: [Datenkategorien].
>
> Was ist passiert: [Kurze, verständliche Erklärung ohne technisches Fachwissen]
>
> Was wir unternommen haben: [Sofortmaßnahmen]
>
> Was Sie tun können: [z. B. auf verdächtige E-Mails achten, Passwort ändern, wenn betroffen]
>
> Bei Fragen stehen wir Ihnen unter [Kontakt] zur Verfügung.
>
> [Firmenname]

Interne Kommunikation: Mitarbeiter sollten eine klare Anweisung erhalten, was sie Kunden bei Nachfragen sagen dürfen: „Wir sind uns eines technischen Vorfalls bewusst und arbeiten an der Klärung. Für weitere Informationen wenden Sie sich bitte an [Name].“ Keine Spekulationen, keine Details — bis die Meldung abgeschlossen ist.

Externe Kommunikation: Für die meisten KMU unter 50 Mitarbeitern ist eine Presseanfrage nach einer Datenpanne unwahrscheinlich. Sollte es trotzdem eine geben: Keine Statements ohne Rücksprache mit einem Rechtsanwalt.

Phase 4 – Nachbereitung & Verbesserung (nach 72 Stunden)

Die Panne ist gemeldet — jetzt geht es darum, sie nicht zu wiederholen.

Root-Cause-Analyse:

- An welchem Punkt im Workflow sind die Daten unkontrolliert weitergegeben worden?
- War es ein Konfigurationsfehler, ein fehlendes AVV, ein fehlerhafter API-Key oder mangelnde Mitarbeiterschulung?
- Wurde der betroffene Dienst im Verarbeitungsverzeichnis (Art. 30 DSGVO) aufgeführt?

Maßnahmenplan:

- Technisch: Datenmaskierung vor API-Übergabe einrichten, Logging auf personenbezogene Daten reduzieren, API-Zugriffsrechte überprüfen
- Organisatorisch: Mitarbeiter zum Thema „Was gehört nicht in den KI-Prompt?“ schulen, Workflow-Freigabeprozess einführen
- Dokumentation: Verarbeitungsverzeichnis aktualisieren, Vorfall im internen Register festhalten

Verarbeitungsverzeichnis und Ablage: Für die strukturierte Ablage Ihres Notfallplans und des Verarbeitungsverzeichnisses eignen sich DSGVO-konforme Wikis — einen Vergleich relevanter Tools finden Sie im Artikel zu Notion-Alternativen für Notizen und Wissensmanagement.

RACI-Matrix für den KI-Notfallfall – wer macht was?

RACI steht für Responsible (führt aus), Accountable (trägt Verantwortung), Consulted (wird einbezogen) und Informed (wird informiert). In einem KMU übernimmt oft eine Person mehrere Rollen — das ist datenschutzrechtlich zulässig, muss aber vorab schriftlich festgehalten sein.

AUFGABE	GF	OFFICE-/PROJEKTLEITUNG	EXTERNER IT-DL	DSB (INT./EXT.)	KI-TOOL-ADMIN	RA (OPTIONAL)
Entdeckung intern melden	I	R	—	—	R	—
Koordination übernehmen	A	R	—	—	—	—
Workflow stoppen	I	—	C	—	R	—
Risikoklassifizierung	A	R	C	C	C	C
Behördenmeldung Art. 33	A	R	—	C	—	C
Betroffenenbenachrichtigung	A	R	—	C	—	C
Root-Cause-Analyse	I	R	R	C	R	—
Verarbeitungsverzeichnis aktualisieren	A	R	—	C	—	—

Vorlage zum Befüllen:

AUFGABE	NAME PERSON 1	NAME PERSON 2	NAME EXTERNER IT	NAME DSB	NAME KI-ADMIN
Entdeckung intern melden					
Koordination					
Workflow stoppen					
Risikoklassifizierung					
Behördenmeldung					
Betroffenenbenachrichtigung					
Root-Cause-Analyse					
Verzeichnis aktualisieren					

Bei KMU unter 20 Mitarbeitern trägt die Geschäftsführung oft die Accountability für alle Punkte, während die operative Verantwortung (Responsible) auf eine Person — häufig die Projektleitung oder einen Allrounder — gebündelt wird. Wichtig: Diese Zuweisung schriftlich festhalten und der zuständigen Datenschutzbehörde auf Nachfrage vorlegen können.

KI-spezifische Präventivmaßnahmen – damit der Notfallplan nicht gebraucht wird

Der beste Notfallplan ist der, den Sie nie aktivieren müssen. Die folgenden Maßnahmen adressieren die häufigsten Ursachen von KI-Datenpannen in KMU.

Datenmaskierung vor KI-Übergabe (PII-Scrubbing): Personenbezogene Daten sollten vor der Übergabe an ein KI-System anonymisiert oder pseudonymisiert werden. In n8n lässt sich das mit einem vorgeschalteten Code-Node umsetzen, der Namen, E-Mail-Adressen und Kundennummern durch Platzhalter ersetzt. Das gleiche Prinzip gilt für Make und Zapier.

API-Berechtigungen auf Minimum setzen: Jeder KI-Dienst sollte nur die Zugriffsrechte erhalten, die er für seine konkrete Aufgabe benötigt — nicht mehr. Wie Sie den Datenzugriff von KI-Agenten generell absichern, erklären wir ausführlich im Guide zu KI-Agenten und Berechtigungsmodellen. Ergänzend lohnt ein Blick auf den Artikel zu KI-Workflows mit Unternehmensdaten absichern.

Subprozessor-Verzeichnis pflegen: Jeder KI-Dienst, der personenbezogene Daten verarbeitet, ist ein Auftragsverarbeiter und muss im Verarbeitungsverzeichnis nach Art. 30 DSGVO aufgeführt sein — mit Angabe des Dienstleisters, des Datentyps und des Verarbeitungszwecks. Viele KMU führen diese Liste nicht aktuell, was im Ernstfall teuer werden kann.

Regelmäßige Workflow-Audits: Einmal pro Quartal sollten alle aktiven Automationen auf ihre Datenpfade geprüft werden. Welche Dienste werden angesprochen? Welche Daten fließen wohin? Gibt es aktuelle AVVs? Ein strukturiertes Vorgehen dabei erklärt der Artikel zum KI-Audit für KMU.

Mitarbeitersensibilisierung: Was gehört nicht in einen KI-Prompt? Kundennamen, Adressen, Auftragsnummern, Kontonummern, Gesundheitsdaten, Personalakten — die Liste ist länger als die meisten Mitarbeiter vermuten. Eine einseitige interne Richtlinie, die konkrete Beispiele nennt, ist wirkungsvoller als ein zweistündiges Compliance-Seminar.

Vorlage herunterladen oder direkt verwenden

Die Vorlage steht in zwei Varianten zur Verfügung:

Option A — Direkt im Browser: Das eingebettete Google Sheet enthält alle vier Phasen, die RACI-Matrix und die Mustertexte als ausfüllbare Felder. Öffnen Sie das Dokument, erstellen Sie eine eigene Kopie („Datei → Kopie erstellen“) und befüllen Sie es direkt in Ihrem Google-Konto. Die Daten verbleiben bei Ihnen.

Option B — Word/PDF-Download: Unter strukturaflow.com steht die Vorlage als .docx-Datei zum Download bereit — ohne Anmeldung. Das Format eignet sich für Unternehmen, die Dokumente lokal speichern möchten.

Wichtiger Hinweis: Die Vorlage ist ein strukturierter Startpunkt, keine rechtliche Beratung. Für komplexe Fälle — insbesondere bei sensiblen Datenkategorien, größeren Betroffenenzahlen oder unklarer behördlicher Zuständigkeit — ist anwaltliche Unterstützung sinnvoll. Der Übergang vom Ausfüllen der Vorlage zur Fachberatung ist oft ein einziges Telefonat.

Praxis-Tipp: Notfallplan in 90 Minuten aufsetzen

Kein Vorwissen, keine vorhandenen Strukturen — so gehen Sie vor:

30 Minuten: Vorlage öffnen, RACI-Matrix befüllen. Tragen Sie echte Namen ein. Wer ist bei Ihnen die Person, die einen Workflow-Fehler zuerst bemerken würde? Wer entscheidet über externe Kommunikation? Wer hat die Zugangsdaten zu Make/Zapier/n8n? Diese Fragen klären sich beim Befüllen von selbst.

20 Minuten: Behörden-Kontaktdaten eintragen. AT: dsb.gv.at, Meldeformular direkt auf der Startseite. DE: Behörde Ihres Bundeslandes recherchieren und URL + Telefonnummer eintragen. CH: edoeb.admin.ch. Speichern Sie die Links als Lesezeichen — im Ernstfall zählt jede Minute.

20 Minuten: Bestehende KI-Workflows auflisten. Öffnen Sie Make, Zapier, n8n — und schreiben Sie auf, welche Automationen aktiv sind. Ordnen Sie jeder eine Risikostufe zu (Niedrig/Mittel/Hoch) basierend auf den Datentypen, die sie verarbeiten. Das ist der Kern Ihres Subprozessor-Verzeichnisses.

20 Minuten: Mustertexte anpassen. Ersetzen Sie [Firmenname], [Kontaktperson] und [Adresse] in den Behörden- und Betroffenenmustertexten. Speichern Sie die Texte als Vorlage in Ihrem E-Mail-Client oder Dokumentensystem — damit Sie im Notfall nicht von Null beginnen.

Ehrliche Einschätzung: Diese 90 Minuten schützen Sie nicht vor allen möglichen Szenarien. Aber sie stellen sicher, dass Sie in den ersten zwei Stunden einer echten Datenpanne handlungsfähig bleiben — anstatt gelähmt vor einem leeren Dokument zu sitzen.

Bei Strukturaflow sehen wir regelmäßig, dass KMU KI-Workflows einführen und dabei die Datenpfade unterschätzen. Die eigentliche Frage ist nicht „Was machen wir, wenn etwas passiert?" — sondern „Welche unserer Workflows wären überhaupt betroffen?"

FAQ

Muss ich als KMU mit weniger als 10 Mitarbeitern auch einen Notfallplan haben?

Ja. Die DSGVO macht keine Ausnahme für Unternehmensgröße. Wer personenbezogene Daten verarbeitet — und das tun praktisch alle KMU — ist zur Einhaltung von Art. 33 und 34 verpflichtet. Der Aufwand für einen Basisplan ist überschaubar; die Konsequenzen einer fehlenden Dokumentation im Ernstfall nicht.

Was gilt als „Kenntnis" der Datenpanne — wann startet die 72-Stunden-Frist?

Die Frist startet, sobald die verantwortliche Stelle von der Panne weiß. Das ist nicht zwingend die Geschäftsführung: Ein Mitarbeiter, der einen Fehler im KI-Workflow entdeckt, startet die Uhr — auch wenn die Führungsebene noch nicht informiert ist. Deshalb ist es wichtig, interne Meldewege klar zu definieren und zu dokumentieren, wann welche Person informiert wurde.

Brauche ich für jedes KI-Tool einen eigenen Notfallplan?

Nein. Ein zentraler Notfallplan mit einer Übersicht aller eingesetzten KI-Dienste und deren Datenpfade reicht aus. Die Vorlage in diesem Artikel ist so aufgebaut, dass Sie in Phase 1 den betroffenen Workflow eintragen — und der Rest des Plans bleibt gleich. Was Sie tatsächlich für jedes Tool benötigen, ist ein Eintrag im Verarbeitungsverzeichnis und ein aktueller Auftragsverarbeitungsvertrag (AVV).

Gilt die Meldepflicht auch, wenn kein Schaden entstanden ist?

Ja — die Meldepflicht knüpft nicht am tatsächlichen Schaden an, sondern am Risiko für die betroffenen Personen. Auch wenn eine Datenpanne folgenlos geblieben ist, kann eine Meldepflicht bestehen. Entscheidend ist die Risikoklassifizierung aus Phase 2.

Nächste Schritte

Die drei wichtigsten Punkte zum Mitnehmen:

- Die 72-Stunden-Frist läuft ab dem Moment, in dem irgendeine Person in Ihrem Unternehmen von der Panne weiß — nicht ab Ihrer Kenntnis.
- Klassische IT-Notfallpläne decken KI-Workflows nicht ab: andere Datenpfade, andere Subprozessoren, andere Risikoprofile.
- In 90 Minuten lässt sich ein belastbarer Basisplan aufsetzen — die Vorlage aus diesem Artikel enthält alle notwendigen Bausteine.

Was dieser Artikel nicht leisten kann: einen Blick in Ihre konkrete Systemlandschaft. Welche Ihrer bestehenden KI-Workflows verarbeiten tatsächlich personenbezogene Daten? Welche Dienste fehlen in Ihrem Verarbeitungsverzeichnis? Welche API-Verbindungen haben zu weit gefasste Berechtigungen?

Das sind Fragen, die sich oft in einem kurzen strukturierten Gespräch klären lassen — ohne dass vorher alles perfekt dokumentiert sein muss. Im Rahmen unseres unverbindlichen 30-Minuten-Beratungsgesprächs schildern Sie Ihre Situation, und wir geben eine ehrliche Einschätzung: Was ist dringend, was kann warten, wo liegen die realistischen Risiken in Ihrem konkreten Kontext. Kein Verkaufsgespräch, kein Vortrag.

NÄCHSTER SCHRITT

Mehr praktische KI-Anleitungen für KMU

Dieser Artikel ist Teil des KI-Hubs von Strukturaflow — einer deutschsprachigen Plattform für den praktischen KI-Einsatz in kleinen und mittleren Unternehmen.

https://wissen.strukturaflow.it.com