Datenpannen-Meldeverfahren

Internes Prozessdokument gemäß Art. 33 & 34 DSGVO

Verantwortlich: Bastian Barkowski · Flowmatix · privacy@flowmatix.io
Version: 1.0 · **Stand:** April 2026

> **72-Stunden-Frist:** Eine Datenpanne muss innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde gemeldet werden (Art. 33 Abs. 1 DSGVO). **Die Uhr läuft ab dem Moment, in dem Flowmatix oder einer seiner Unterauftragsverarbeiter (z. B. Hetzner, 360dialog, Anthropic) von der Panne Kenntnis erlangt** — nicht erst ab dem Zeitpunkt, zu dem Flowmatix selbst informiert wird. Die Kenntnis eines Sub-Processors gilt als Kenntnis von Flowmatix. Unterauftragsverarbeiter sind vertraglich verpflichtet, Flowmatix unverzüglich (max. 24h nach deren eigener Kenntnis) zu informieren (siehe AVV § 8).

1. Was ist eine meldepflichtige Datenpanne?

Eine Verletzung des Schutzes personenbezogener Daten liegt vor, wenn es zu einer unbeabsichtigten oder unrechtmäßigen:

- Vernichtung, Verlust oder Veränderung personenbezogener Daten kommt
- Unbefugten Offenbarung oder unbefugtem Zugang zu personenbezogenen Daten kommt

Beispiele für meldepflichtige Ereignisse bei Flowmatix:

- Unbefugter Zugriff auf die PostgreSQL-Datenbank (Patient oder Klinik-Daten)
- Datenbankdump oder Backup-Datei gelangt an Unbefugte
- Cross-Tenant-Bug: Klinik A sieht Daten von Klinik B
- Kompromittierter Admin-Account mit Zugriff auf Patientendaten
- WhatsApp-Nachrichten an falsche Empfänger gesendet
- Ransomware-Angriff mit Datenzugriff
- Versehentliche Veröffentlichung von Patientendaten (z.B. in Logs)

> **Nicht meldepflichtig** (aber intern zu dokumentieren): Fehlgeschlagene Login-Versuche, DDoS ohne Datenzugriff, verschlüsselte Daten ohne Schlüssel-Kompromittierung.

2. Sofortmaßnahmen (erste 4 Stunden)

1. **[0 Min]** Panne entdeckt → sofort an **privacy@flowmatix.io** melden

2. **[15 Min]** Betroffene Systeme isolieren (Container stoppen, Ports sperren falls nötig)
3. **[30 Min]** Initialbewertung: Welche Daten? Wie viele Personen? Wie lange?
4. **[1 Std]** Eintrag im Datenpannen-Register (Datei: Datenpannen-Register.xlsx)
5. **[2 Std]** Entscheiden: Meldepflicht an Aufsichtsbehörde? → Wenn unklar: JA
6. **[4 Std]** Betroffene Klinik(en) informieren (per E-Mail + Telefon)

3. Meldung an Aufsichtsbehörde (72h-Frist)

Zuständige Behörde (Deutschland):

Landesbeauftragter für Datenschutz Niedersachsen (Sitz: Hude, Niedersachsen)
Online-Meldung: lfd.niedersachsen.de
E-Mail: poststelle@lfd.niedersachsen.de
Tel.: +49 511 120-4500

Inhalt der Meldung (Art. 33 Abs. 3 DSGVO):

Pflichtangabe	Details
Art der Verletzung	Unbefugter Zugriff / Verlust / Veränderung / Offenbarung
Betroffene Kategorien	z.B. Patientendaten, Gesundheitsdaten, Kontaktdaten
Ungefähre Anzahl Personen	Anzahl betroffener Patienten/Nutzer
Ungefähre Anzahl Datensätze	Anzahl betroffener Einträge
Wahrscheinliche Folgen	Identitätsdiebstahl, Diskriminierung, finanzieller Schaden etc.
Ergriffene/geplante Maßnahmen	Isolierung, Patch, Benachrichtigungen etc.
Kontakt Datenschutzbeauftragter	privacy@flowmatix.io

> Wenn zum Zeitpunkt der Meldung nicht alle Infos vorliegen: trotzdem melden und nachliefern. Besser unvollständige Meldung in Zeit als vollständige Meldung zu spät.

4. Benachrichtigung betroffener Personen (Art. 34 DSGVO)

Betroffene Patienten/Personen müssen **unverzüglich** benachrichtigt werden, wenn die Panne *voraussichtlich ein hohes Risiko* für ihre Rechte und Freiheiten zur Folge hat.

Hohes Risiko liegt vor bei:

- Offenbarung von Gesundheitsdaten (Art. 9) an Unbefugte
- Zugriff auf Nachrichten-Inhalte (WhatsApp-Verläufe)
- Kompromittierung von Passwörtern oder Authentifizierungsdaten
- Daten von mehr als ~1.000 Personen betroffen

Benachrichtigung enthält (Art. 34 Abs. 2 DSGVO):

- Art der Verletzung in klarer Sprache
- Name und Kontaktdaten des Datenschutzbeauftragten
- Wahrscheinliche Folgen
- Ergriffene oder geplante Maßnahmen
- Empfehlungen für Betroffene (z.B. Passwort ändern)

5. Nachbearbeitung

1. Root-Cause-Analyse dokumentieren
2. Technische Maßnahmen zur Verhinderung umsetzen
3. Eintrag im Datenpannen-Register abschließen
4. DPIA bei Bedarf aktualisieren
5. Klinik-Kunden über abgeschlossene Maßnahmen informieren
6. Folgemeldung an Aufsichtsbehörde wenn nötig

6. Datenpannen-Register

Alle Pannen — auch nicht-meldepflichtige — müssen intern dokumentiert werden (Art. 33 Abs. 5 DSGVO):

Feld	Beispiel
Datum/Uhrzeit Entdeckung	2026-04-17 14:32 UTC
Art der Panne	Unbefugter Datenbankzugriff
Betroffene Systeme	fm-postgres, patients-Tabelle
Datenkategorien	Gesundheitsdaten, Kontaktdaten
Anzahl Personen (geschätzt)	120
Meldepflichtig?	Ja / Nein
Gemeldet am	2026-04-17 22:00 UTC

Maßnahmen	Passwort-Reset, Patch deployed
Abgeschlossen am	2026-04-18
Verantwortlich	Bastian Barkowski
