DSGVO-Notfallhandbuch

Datenpanne in 72 Stunden richtig melden — der Handlungsleitfaden für Geschäftsführer, Datenschutzbeauftragte und IT-Verantwortliche

Inhaltsverzeichnis

1. Was ist eine meldepflichtige Datenpanne? 2
Typische Beispiele aus dem KMU-Alltag 2
2. Die 72-Stunden-Frist (Art. 33 DSGVO) 3
Möglicher Bußgeldrahmen 3
Ablauf der Soforthilfe im Überblick 4
3. Sofortmaßnahmen — die ersten 4 Stunden 5
4. Meldung an die Aufsichtsbehörde 6
5. Benachrichtigung der Betroffenen (Art. 34 DSGVO) 6
6. Notfallplan-Vorlage zum Ausfüllen 8
6.1 Stammdaten des Vorfalls 8
6.2 Ergriffene Sofortmaßnahmen 8
6.3 Risikobewertung & Entscheidungen 9
7. Häufige Fehler — richtig statt falsch 9
8. Häufige Fragen (FAQ) 10

Wichtiger Hinweis — keine Rechtsberatung

Dieses Handbuch dient ausschließlich der allgemeinen Information und ersetzt **keine** individuelle Rechtsberatung. Die Inhalte wurden mit Sorgfalt erstellt, können den konkreten Einzelfall jedoch nicht abbilden. Im Ernstfall einer Datenpanne ziehen Sie umgehend Ihren Datenschutzbeauftragten sowie eine auf Datenschutzrecht spezialisierte Kanzlei hinzu. Eine Haftung für die Vollständigkeit, Aktualität und Richtigkeit ist ausgeschlossen.

Eine Datenpanne kommt selten zur passenden Zeit — meist freitagabends, im Urlaub oder mitten im Tagesgeschäft. Genau dann zählt jede Stunde. Dieses Handbuch führt Sie Schritt für Schritt durch die ersten, entscheidenden 72 Stunden und stellt Ihnen eine **ausfüllbare Notfallplan-Vorlage** bereit, die Sie ausdrucken und griffbereit halten sollten.

1. Was ist eine meldepflichtige Datenpanne?

Der Gesetzgeber spricht von einer **„Verletzung des Schutzes personenbezogener Daten"**. Die Legaldefinition findet sich in **Art. 4 Nr. 12 DSGVO**:

> *„Eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden."*
> — Art. 4 Nr. 12 DSGVO

Entscheidend ist: Eine Datenpanne ist **nicht nur der Hackerangriff von außen**. Auch interne Fehler, Verlust von Geräten oder eine Fehlversendung zählen dazu. Man unterscheidet drei Schutzziele, deren Verletzung eine Panne auslöst:

- **Vertraulichkeit** — unbefugter Zugriff oder Offenlegung (z. B. gehackte Datenbank, E-Mail an falschen Empfänger).
- **Integrität** — unbefugte oder unbeabsichtigte Veränderung von Daten (z. B. manipulierte Datensätze, fehlerhaftes Skript).
- **Verfügbarkeit** — Verlust oder Vernichtung von Daten (z. B. Ransomware-Verschlüsselung, gelöschtes Backup, defekte Festplatte ohne Sicherung).

Typische Beispiele aus dem KMU-Alltag

- Ransomware verschlüsselt den Fileserver mit Kunden- und Personaldaten.
- Ein Laptop oder USB-Stick mit Klartextdaten geht verloren oder wird gestohlen.
- Ein Newsletter wird mit allen Empfängern im offenen „An"-Feld statt im „BCC" versendet.
- Eine Phishing-Mail führt zum Abgriff von Zugangsdaten zum CRM-System.
- Ein Mitarbeiter sendet eine Excel-Liste mit Gehaltsdaten an den falschen internen Verteiler.

- Eine Fehlkonfiguration legt eine Cloud-Datenbank ungeschützt im Internet offen.

Risikoabwägung entscheidet über die Meldepflicht

Nicht jede Panne ist meldepflichtig. Maßstab ist das **Risiko für die Rechte und Freiheiten** der Betroffenen. Faustregel: Im Zweifel **dokumentieren und melden**. Eine versäumte Meldung wiegt deutlich schwerer als eine vorsorgliche. Jede Panne — auch eine nicht gemeldete — ist intern zu dokumentieren (**Art. 33 Abs. 5 DSGVO**).

2. Die 72-Stunden-Frist (Art. 33 DSGVO)

Sobald Ihnen eine meldepflichtige Datenpanne **bekannt wird**, beginnt die Uhr zu laufen. Nach **Art. 33 Abs. 1 DSGVO** muss die Meldung an die zuständige Aufsichtsbehörde **„unverzüglich und möglichst binnen 72 Stunden"** erfolgen. Die Frist beginnt mit der Kenntnisnahme — nicht mit dem Vorfall selbst.

Fristbeginn	**Mit Kenntnisnahme der Verletzung (nicht mit dem Vorfall)**
Frist	**Unverzüglich, möglichst innerhalb von 72 Stunden**
Adressat	**Zuständige Landes-Datenschutzaufsichtsbehörde**
Verspätung	**Möglich, aber mit Begründung der Verzögerung**
Auftragsverarbeiter	**Meldet unverzüglich an den Verantwortlichen (Art. 33 Abs. 2)**

Die 72 Stunden laufen kalendarisch — nicht in Werktagen

Die Frist umfasst auch Wochenenden und Feiertage. Eine am Freitag um 16 Uhr entdeckte Panne ist im Zweifel bis Montag um 16 Uhr zu melden. Halten Sie deshalb Notfallkontakte und Zugänge erreichbar — auch außerhalb der Geschäftszeiten.

Möglicher Bußgeldrahmen

72 h
Maximale Meldefrist ab Kenntnis

20 Mio €
Bußgeld-Obergrenze (absolut)

4 %
des weltweiten Jahresumsatzes (je nachdem, was höher ist)

10 Mio €
oder 2 % bei reinen Melde-/Dokumentationsverstößen

Verstöße gegen die Meldepflicht aus Art. 33 fallen in den Rahmen von **bis zu 10 Mio € oder 2 % des Jahresumsatzes** (Art. 83 Abs. 4 DSGVO). Schwere Verstöße gegen Verarbeitungsgrundsätze können **bis zu 20 Mio € oder 4 %** erreichen (Art. 83 Abs. 5 DSGVO) — maßgeblich ist jeweils der höhere Betrag.

Ablauf der Soforthilfe im Überblick

1. **Erkennen & Stoppen**
   Vorfall bestätigen, Datenabfluss stoppen, betroffene Systeme isolieren.
2. **Bewerten**
   Art, Umfang und Risiko der Panne einschätzen. Welche Daten, wie viele Betroffene?
3. **Dokumentieren**
   Zeitleiste, Maßnahmen und Entscheidungen lückenlos festhalten (Notfallplan-Vorlage nutzen).
4. **Melden**
   Bei Risiko: Meldung an die Aufsichtsbehörde innerhalb von **72 Stunden** (**Art. 33 DSGVO**).
5. **Benachrichtigen**
   Bei hohem Risiko zusätzlich die Betroffenen informieren (**Art. 34 DSGVO**).

3. Sofortmaßnahmen — die ersten 4 Stunden

In der akuten Phase gilt: **Ruhe bewahren, Schaden begrenzen, alles dokumentieren.** Arbeiten Sie diese Liste der Reihe nach ab — parallelisieren Sie, wo möglich, im Notfallteam.

1. **Vorfall verifizieren** — Handelt es sich tatsächlich um eine Datenpanne? Fehlalarm ausschließen, aber nicht verharmlosen.
2. **Notfallteam alarmieren** — Geschäftsführung, Datenschutzbeauftragter und IT-Verantwortlicher sofort informieren.
3. **Schaden eindämmen** — Betroffene Systeme vom Netz nehmen, kompromittierte Zugänge sperren, Passwörter zurücksetzen.
4. **Beweise sichern** — Logfiles, Screenshots und Systemzustände sichern, bevor Spuren überschrieben werden. Nichts vorschnell löschen.
5. **Zeitstempel setzen** — Exakten Zeitpunkt der Kenntnisnahme dokumentieren — hier beginnt die 72-Stunden-Frist.
6. **Umfang einschätzen** — Welche Datenkategorien, welche und wie viele Betroffene sind erfasst?
7. **Risiko bewerten** — Drohen den Betroffenen finanzielle Schäden, Identitätsdiebstahl oder Diskriminierung?
8. **Externe Hilfe prüfen** — IT-Forensik, Fachanwalt und ggf. Versicherung (Cyber-Police) frühzeitig einbinden.

> **Niemals den Vorfall vertuschen**
>
> Das Verschweigen einer Datenpanne ist kein gangbarer Weg. Es erhöht den Schaden, gefährdet Betroffene zusätzlich und führt im Entdeckungsfall zu erheblich höheren Bußgeldern. Transparenz und schnelles Handeln werden von Aufsichtsbehörden hingegen positiv bewertet.

4. Meldung an die Aufsichtsbehörde

Die Meldung erfolgt in der Regel über das **Online-Meldeformular** der zuständigen Landes-Aufsichtsbehörde. **Art. 33 Abs. 3 DSGVO** schreibt die Pflichtangaben verbindlich vor. Liegen noch nicht alle Informationen vor, ist eine **schrittweise Meldung** zulässig — melden Sie zunächst, was Sie wissen, und reichen Sie Details nach.

Pflichtangabe (Art. 33 Abs. 3)	Was muss hinein?
Art der Verletzung	Beschreibung des Vorfalls — Vertraulichkeit, Integrität oder Verfügbarkeit betroffen?
Kategorien Betroffener	Kunden, Beschäftigte, Bewerber, Patienten etc. — und ungefähre Anzahl.
Kategorien von Daten	Z. B. Kontakt-, Bank-, Gesundheits- oder Bewerbungsdaten — und ungefähre Zahl der Datensätze.
Kontaktstelle	Name und Kontaktdaten des Datenschutzbeauftragten oder einer anderen Auskunftsstelle.
Wahrscheinliche Folgen	Voraussichtliche Konsequenzen der Verletzung für die Betroffenen.
Ergriffene Maßnahmen	Maßnahmen zur Behebung und zur Abmilderung möglicher nachteiliger Auswirkungen.

Zuständige Behörde finden

Zuständig ist grundsätzlich die Datenschutz-Aufsichtsbehörde des Bundeslandes, in dem Ihr Unternehmen seinen Sitz hat. Bei grenzüberschreitenden Verarbeitungen kann das „One-Stop-Shop"-Prinzip mit einer federführenden Behörde greifen. Halten Sie den Link zum Online-Meldeformular Ihrer Behörde bereits **vor** dem Ernstfall griffbereit.

5. Benachrichtigung der Betroffenen (Art. 34 DSGVO)

Besteht **voraussichtlich ein hohes Risiko** für die persönlichen Rechte und Freiheiten der Betroffenen, müssen diese nach **Art. 34 DSGVO** zusätzlich **unverzüglich und in klarer, einfacher Sprache** informiert werden — über die Behördenmeldung hinaus.

Wann ist eine Betroffenen-Benachrichtigung Pflicht?

- ☐ **Hohes Risiko liegt vor**
  z. B. drohender Identitätsdiebstahl, finanzieller Schaden, Rufschädigung oder Offenlegung sensibler Daten.
- ☐ **Sensible Datenkategorien betroffen**
  Gesundheits-, Finanz-, Login- oder besondere Kategorien personenbezogener Daten (Art. 9).

- [ ] **Daten waren unverschlüsselt**
  Bei starker Verschlüsselung/Anonymisierung kann die Benachrichtigung entfallen (Art. 34 Abs. 3).
- [ ] **Klare Sprache verwendet**
  Verständliche Beschreibung der Panne, der Folgen und der empfohlenen Schutzmaßnahmen.
- [ ] **Pflichtangaben enthalten**
  Mindestens: Art der Panne, Kontaktstelle, wahrscheinliche Folgen, ergriffene Maßnahmen.
- [ ] **Handlungsempfehlung gegeben**
  z. B. Passwörter ändern, Kontobewegungen prüfen, auf Phishing achten.

Ausnahme: öffentliche Bekanntmachung

Wäre die Einzelbenachrichtigung mit unverhältnismäßigem Aufwand verbunden, genügt eine öffentliche Bekanntmachung oder eine vergleichbar wirksame Maßnahme, durch die die Betroffenen vergleichbar effektiv informiert werden (Art. 34 Abs. 3 lit. c).

6. Notfallplan-Vorlage zum Ausfüllen

Dies ist das **Herzstück** dieses Handbuchs. Drucken Sie diese Seiten aus und füllen Sie sie im Ernstfall sofort aus — oder nutzen Sie die interaktiven Formularfelder direkt im PDF. Eine lückenlose Dokumentation ist nicht nur Pflicht (Art. 33 Abs. 5), sondern Ihr bester Schutz gegenüber der Aufsichtsbehörde.

6.1 Stammdaten des Vorfalls

Datum & Uhrzeit der Entdeckung (Fristbeginn!)

Wer hat die Panne entdeckt / gemeldet?

Beteiligte / betroffene Systeme

Betroffene Datenkategorien (z. B. Kontakt-, Bank-, Gesundheitsdaten)

Geschätzte Anzahl betroffener Personen

Verantwortlicher für die Bearbeitung des Vorfalls

6.2 Ergriffene Sofortmaßnahmen

Welche Sofortmaßnahmen wurden ergriffen?

Detaillierte Zeitleiste der Maßnahmen (Uhrzeit + Aktion + Verantwortlicher)

6.3 Risikobewertung & Entscheidungen

Liegt ein Risiko für die Betroffenen vor? (ja / nein + Begründung)

Meldung an die Aufsichtsbehörde erforderlich?

Benachrichtigung der Betroffenen erforderlich (hohes Risiko)?

Begründung der Entscheidung / weitere Notizen

7. Häufige Fehler — richtig statt falsch

Richtig	Falsch
+ Notfallteam vorab definieren und Kontakte griffbereit halten.	x Erst recherchieren, wer überhaupt zuständig ist — und so Stunden verlieren.
+ Frist ab Kenntnisnahme dokumentieren und ernst nehmen.	x Frist erst ab „abschließender Klärung" rechnen.
+ Im Zweifel dokumentieren und melden.	x Panne als „wohl nicht so schlimm" abtun und nichts festhalten.
+ Beweise (Logs, Screenshots) vor jeder Bereinigung sichern.	x Systeme sofort plattmachen und damit Spuren vernichten.
+ Schrittweise melden, wenn noch nicht alle Fakten vorliegen.	x Mit der Meldung warten, bis alle Details vollständig sind.
+ Betroffene bei hohem Risiko in klarer Sprache informieren.	x Betroffene gar nicht oder erst nach Wochen informieren.

8. Häufige Fragen (FAQ)

Muss ich wirklich jede kleine Panne melden?

Nein. Meldepflichtig ist nur, was voraussichtlich ein Risiko für die Rechte und Freiheiten der Betroffenen birgt. Jede Panne — auch eine nicht gemeldete — ist jedoch intern zu dokumentieren (Art. 33 Abs. 5 DSGVO).

Was passiert, wenn ich die 72 Stunden überschreite?

Eine verspätete Meldung ist möglich, muss aber begründet werden. Wichtiger als perfekte Pünktlichkeit ist, dass überhaupt und nachvollziehbar gemeldet wird. Eine gänzlich unterlassene Meldung wiegt deutlich schwerer.

Ab wann läuft die Frist genau?

Ab dem Zeitpunkt, zu dem Ihnen die Verletzung bekannt wird — also mit hinreichender Sicherheit über das Vorliegen einer Panne. Nicht ab dem Vorfall selbst und nicht ab einem ersten vagen Verdacht.

Mein Dienstleister (Auftragsverarbeiter) ist betroffen — wer meldet?

Der Auftragsverarbeiter muss Sie als Verantwortlichen unverzüglich informieren (Art. 33 Abs. 2). Die Meldung an die Aufsichtsbehörde gibt jedoch der Verantwortliche ab — also Ihr Unternehmen.

Müssen verschlüsselte Daten gemeldet werden?

Waren die Daten mit dem Stand der Technik entsprechend stark verschlüsselt und ist der Schlüssel nicht kompromittiert, kann das Risiko und damit die Pflicht zur Betroffenen-Benachrichtigung entfallen. Eine interne Dokumentation bleibt dennoch erforderlich.

Vorbereitung schlägt Improvisation. Wer Notfallteam, Kontakte und diese Vorlage griffbereit hat, gewinnt im Ernstfall die wertvollste Ressource: **Zeit.** Prüfen Sie jetzt, wie gut Ihr Unternehmen wirklich aufgestellt ist.

Machen Sie den kostenlosen DSGVO-Compliance-Check und finden Sie Ihre Lücken, bevor es ein Ernstfall tut.

https://www.sw-business-solutions.de/leadmagnete