Was ist eine Datenpanne?

Eine Datenpanne liegt gem. Art. 4 Nr. 12 DSGVO vor, wenn es zu einer **Verletzung der Sicherheit** kommt, die zur **Vernichtung**, zum **Verlust**, zur **Veränderung** oder zur **unbefugten Offenlegung** bzw. zum unbefugten Zugang zu personenbezogenen Daten führt - egal ob unbeabsichtigt oder unrechtmäßig.

Beispiel

- Eine Mitgliederliste wird versehentlich an den falschen E?Mail?Verteiler gesendet.
- Ein unverschlüsselter USB?Stick mit Spielergebnissen und Kontaktdaten geht verloren.



Vorfall verstehen und eindämmen

Es gibt mehrere Möglichkeiten wie es zu einer Datenpanne kommen kann. Von einem einfachen Versehen bis zu einem vorsätzlichen Cyberangriff ist vieles möglich. Zunächst solltet ihr daher **RUHE bewahren** und zugleich **schnellstmöglich handeln.** Die Ursache der Datenpanne sollte geklärt werden, Folgen eingedämmt und falls nötig, die Sicherheit eurer Systeme (wieder)hergestellt werden.

- Schritt 1: Lage verstehe und betroffene Systeme schnellstmöglich sichern - dazu solltet ihr falls nötig **Zugriffe sperren, Passwörter zurücksetzen und betroffene Konten und Ordner isolieren falls möglich.** Das kann sowohl virtuell als auch physich durch bspw. die Trennung vom Netzwerk/Internet erfolgen.
- Schritt 2: Beweise oder Nachweise sichern - Was ist passiert, wann, wo, welche Daten, wie viele Personen sind Betroffen? **Screenshots, Logfiles, E?Mails aufbewahren.**
- Schritt 3: **Interne Meldung** an den Vorstand und falls vorhanden, den Datenschutzbeauftragten absetzen.
- Schritt 4: Das vorhandensein von **Sicherungen** (Backup's) prüfen. Das regelmäßige Anfertigen muss vorab durch euch umgesetzt oder autom. eingerichetet bzw. beauftragt worden sein, sonst dürften wohl keine Sicherungen vorhanden sein. Falls ihr Cloud Services nutzt, lohnt sich eine schnellstmögliche Anfrage bei eurem Dienstleister (diese haben teilw. kurze Löschfristen) ob dieser automatische Sicherungen für euch durchgeführt hat, welche ihr nutzen könnt.
- Schritt 5: **Externe Meldung** an die Datenschutzaufsichtsbehörden und weitere zukünftige Schutzmaßnahmen (z.B. 2-Faktorauthentifizierung, sichere Passwörter etc.) prüfen (Achtung: Meldefrist von 72h beachten - dazu unten mehr!)

Beispiel

Nach der Übernahme eines Email-Vorstandaccounts durch einen Unbefugten Dritten zunächst Kontosperrung vornehmen, das Passwort ändern, durch Hacker genutzte/versendete Daten sichten und dokumentieren, auf Folgeschäden oder nötige Handlungen prüfen, Zeitraum des Vorfalls notieren und Dienstleister um Auskunft bitten, Vorstand/DSB informieren, externe Meldung an die Aufsichtsbehörden prüfen.



Zeitnah prüfen: Besteht ein Risiko?

Der Verein bewertet, ob die Panne voraussichtlich ein **Risiko für Rechte und Freiheiten Betroffener darstellt.** Solche Gefahren können bspw. folgende sein:

- Gefahr von **Identitätsdiebstahl**,
- **Rufschädigung**,
- **finanzielle Nachteile**.

Als Hilfestellung für die Risikobewertung hat die Datenschutzkonferenz der Länder ein Kurzpapier erstellt. Weitere nützliche Hinweise hat der hamburgische Beauftragte für den Datenschutz veröffentlicht. Ist ein Risiko wahrscheinlich, besteht gem. Art. 33 DSGVO eine **Meldepflicht** gegenüber der Aufsichtsbehörde. Bei hohem Risiko muss zusätzlich eine **Benachrichtigung der Betroffenen** erfolgen. In jedem Falle sollte die Entscheidung des Vereins für oder gegen eine Meldepflicht **dokumentiert** werden!

Behaltet die Fristen im Blick: **72 Stunden zählen!**

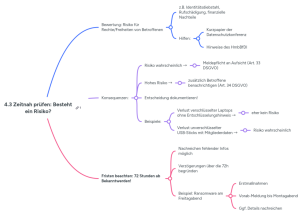
- Meldung an die zuständige Aufsichtsbehörde unverzüglich, möglichst innerhalb von 72 Stunden nach Bekanntwerden, es sei denn, es besteht voraussichtlich kein Risiko.
- Fehlen Informationen, dürfen sie schrittweise nachgereicht werden. Verzögerungen sind im Formular zu begründen.

Beispiel

- Verlust eines **verschlüsselten Laptops** ohne Hinweise auf Entschlüsselung -> eher kein Risiko.
- Verlust eines **unverschlüsselten USB?Sticks** mit Mitgliederdaten -> Risiko wahrscheinlich.

- Ein Ransomware-Befall (Verschlüsselungstrojaner zur Erpressung von "Lösegeld") wird am Freitagabend entdeckt: Erstmaßnahmen einleiten, vorläufige Meldung spätestens bis Montagabend absetzen und Details nachreichen.

  Zur Checkliste



Benachrichtigung betroffener Personen

Bei voraussichtlich **hohem Risiko** sind Betroffene unverzüglich in klarer, einfacher Sprache zu informieren. Der Inhalt lehnt sich an die Angaben der Behördenmeldung an.

WICHTIG: Keine Benachrichtigung ist nötig, wenn z. B. **starke Verschlüsselung** wirksam war, die Daten bereits öffentlich bekannt waren, das hohe Risiko durch andere Maßnahmen entfallen ist oder eine **öffentliche Bekanntmachung ausreicht**.

Beispiel

- Ein Newsletter-Verteiler wird versehentlich offen sichtbar mit E?Mail-Adressen externer Personen versendet, da der Versender davon ausgeht im Feld "Empfänger" müsse immer eine Mail-Adresse stehen. Je nach Umfang und Sensibilität (z.B. Reha-/Herzsportteilnehmer) **kann** ein hohes Risiko vorliegen, der Verein wird durch einen Betroffenen auf den Fehler hingewiesen. Nach einer Prüfung sollten die Betroffenen direkt informiert werden und künftige „BCC“-Nutzung (Blindverteiler, bei dem die Empfänger keine anderen Empfänger sehen können) zugesichert werden.
- Versehentliche Veröffentlichung von Mitarbeiterdaten auf der Webseite inkl. Gehaltsabrechnungen. Ein hohes Risiko ist hier wahrscheinlich (Identitätsdiebstahl, Datenmissbrauch). Die Veröffentlichung sollte möglichst rückgängig gemacht werden, ggf. wird eine Anweisung der Mitarbeiter zur Datenlöschung benötigt, die Mitarbeiter sind zu informieren und die Maßnahmen mitzuteilen.



Besonderheiten bei Auftragsverarbeitern

Auftragsverarbeiter müssen eine Panne unverzüglich an den Verein melden und den Vorgang dokumentieren, damit der Verein seinen Meldepflichten aus Art. 33/34 DSGVO nachkommen kann.

Beispiel: Ein Cloud-Dienstleister meldet einen verdächtigen Zugriff auf einen Backup-Ordner des Vereins. Der Verein prüft den Zugriff, bewertet das Risiko (insb. ob eine Verschlüsselung vorlag), dokumentiert den gesamten Vorgang, meldet ggf. an die Aufsicht und informiert ggf. Betroffene.

Details

Autor:
Sandro Geil

zuletzt aktualisiert:
Februar 2026

Quelle:
Art. 33/34 DSGVO

Art. 33 DSGVO

Art. 4 Nr. 12 DSGVO