

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 physisch 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. eingerichtet 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

4.2 Verfall verstehen und erklären

Ein Individuum, ein Unternehmen oder eine Organisation verfallen, wenn:

- seine/ihre Identität verloren geht
- seine/ihre Werte verloren gehen
- seine/ihre Mission verloren geht
- seine/ihre Vision verloren geht
- seine/ihre Kultur verloren geht
- seine/ihre Strategie verloren geht
- seine/ihre Organisation verloren geht
- seine/ihre Ressourcen verloren gehen
- seine/ihre Leistung verloren geht
- seine/ihre Reputation verloren geht
- seine/ihre Zukunft verloren geht
- seine/ihre Existenz verloren geht

(Quelle: eigene Zusammenfassung)

<https://lsb-niedersachsen.vibss.de/vereinsmanagement/recht/datenschutz-internet/datenschutz/ersthilfe-bei-datenpannen> – 20.09.2026

zuletzt aktualisiert:

Februar 2026

Quelle:

Art. 33/34 DSGVO

[Art. 33 DSGVO](#)

[Art. 4 Nr. 12 DSGVO](#)