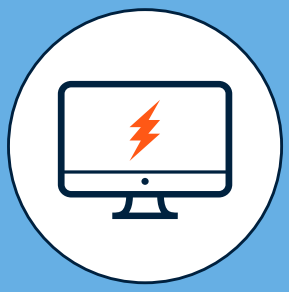
Was tun bei einer Datenpanne?

Die wichtigsten Informationen im Überblick. Von der Meldefrist über die zu informierenden Stellen bis hin zur Dokumentation.

perseus.
Cybersicherheit auf den Punkt



Bei Datenpannen ist schnelles Handeln gefragt.

Um den strengen Anforderungen der DSGVO bei Datenpannen zu genügen, muss innerhalb von 72 Stunden entschieden werden, ob eine solche der zuständigen Aufsichtsbehörde gemeldet werden muss. In diesem Zeitrahmen müssen Sie auch prüfen, ob Sie gegebenenfalls die von der Datenpanne betroffenen Personen benachrichtigen müssen. Das Zeitfenster ist eng und die Uhr tickt unerbittlich. Außerdem ist die Dokumentation des Vorfalls vorgeschrieben.

Dieses Perseus-Whitepaper soll Sie dabei unterstützen, auch unter Zeitdruck die Übersicht über Ihre Pflichten zu behalten. Damit Sie ihnen bestmöglich nachkommen können.

Inhaltsverzeichnis

01 | Was ist eine Datenpanne?

Eine Datenpanne ist eine Sicherheitsverletzung, bei der unbeabsichtigt oder unrechtmäßig personenbezogene Daten verloren gehen, vernichtet oder verändert werden oder Unbefugten offengelegt beziehungsweise zugänglich gemacht werden.
Zu einer Datenpanne kann es beispielsweise in Form eines unrechtmäßigen Hackerangriffs kommen. Aber auch durch den unbeabsichtigten Versand einer E-Mail an einen falschen Empfänger oder den Verlust eines USB-Sticks, auf dem personenbezogene Daten enthalten sind.

Gut zu wissen: Der Begriff „Datenpanne" kommt in der DSGVO nicht vor. Er hat sich aber als geläufige Bezeichnung eingebürgert und entspricht der in der DSGVO genannten „Verletzung des Schutzes personenbezogener Daten."

02 | Welche Pflichten haben Sie im Falle einer Datenpanne?

- Ggf. Meldung an die zuständige Aufsichtsbehörde
- Ggf. Benachrichtigung der Betroffenen
- Maßnahmen zur Behebung der Datenpanne und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen für die Betroffenen
- Dokumentation der Datenpanne

Im Durchschnitt verursacht eine Datenpanne in Deutschland Kosten von **4,25 Mio Euro.**

(Quelle: IBM Security 2019 Cost of a Data Breach Report)

03 | Wen müssen Sie über eine Datenpanne informieren?

Das kommt darauf an, mit welchem Risiko die Datenpanne für die Betroffenen einhergeht.

Bei einem einfachen Risiko für die Betroffen:
Meldung an die zuständige Aufsichtsbehörde.

Bei einem hohen Risiko für die Betroffenen:
Zusätzliche Benachrichtigung der Betroffenen.

Auf eine Meldung kann verzichtet werden, wenn die Datenpanne vorraussichtlich nicht zu einem Risiko für die Betroffenen führt.

03 | a) Der Aufsichtsbehörde

Müssen Sie Datenpannen immer der Aufsichtsbehörde melden?

Die DSGVO sieht in der Regel eine Meldepflicht vor. Von ihr kann nur dann abgesehen werden, wenn die Datenpanne „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt."

Bei Unsicherheiten klären Sie diesen Punkt am besten im Gespräch mit Ihren internen oder externen Datenschutz- bzw. IT-Sicherheits-Experten ab.

Wie schnell müssen Sie eine Datenpanne melden?

Sie müssen eine Datenpanne innerhalb von 72 Stunden nach Bekanntwerden melden.

Gut zu wissen: Bei der Meldung geht Geschwindigkeit vor Vollständigkeit. Aktuell noch nicht vorliegende Informationen zur Datenpanne können Sie schrittweise nachliefern. Zum Nachlesen: Art. 33 Abs. 4 DSGVO.

Tipp: Notieren Sie sich die Kontaktdaten der zuständigen Aufsichtsbehörde leicht auffindbar. Zum Beispiel in diesem Dokument. Dann haben Sie im Falle einer Datenpanne wenigstens eine Sorge weniger.

Über 10.000 Datenpannen wurden 2019 in Deutschland gemeldet.

(Quelle: bdsg-externer-datenschutzbeauftragter.de)

Die Meldung an die Aufsichtsbehörde: Wer und wie?

Wer: Für die Meldung ist die Geschäftsführung verantwortlich. Sie kann diese Aufgabe aber an eine im Unternehmen hierfür zuständige Person delegieren.

Wie: Per E-Mail oder Meldeformular, welches in der Regel auf der Webseite von Aufsichtsbehörden zur Verfügung gestellt wird.

Welche Aufsichtsbehörde ist die zuständige?
Für deutsche Unternehmen ist in der Regel die Aufsichtsbehörde des Bundeslandes zuständig, in dem sich der Sitz des Unternehmens befindet. Eine Liste finden Sie hier.

Zuständige Aufsichtsbehörde:

_____

Telefonnummer: _____

Die Meldung an die Aufsichtsbehörde: Was?

Die Meldung an die zuständige Aufsichtsbehörde muss mindestens die folgenden Informationen enthalten:

- Beschreibung der Art der Datenpanne (z. B. Datenverlust, unbefugte Offenlegung)
- die Kategorien der betroffenen Personen (z. B. Mitarbeitende, Kundinnen und Kunden)
- die Kategorien der betroffenen Datensätze (z. B. Passwörter, E-Mail-Adressen, Bonitätsdaten)
- die ungefähre Zahl der betroffenen Personen und Datensätze
- den Namen und die Kontaktdaten des oder der Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Einschätzung der wahrscheinlichen Folgen für die Betroffenen (z. B. Passwortmissbrauch)
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen, um die Datenpanne zu beheben oder ihre Folgen abzumildern

Zum Nachlesen: Artikel 33 DSGVO

03 | b) Den Betroffenen

Die Benachrichtigung von Betroffenen: Wann?

Wenn die Datenpanne voraussichtlich ein hohes Risiko für die von ihr betroffenen Personen zur Folge hat. Zum Beispiel: Wenn die digitalen Patientenakten eines Krankenhauses durch einen Hackerangriff in die Hände Unberechtigter gelangt sind.

Ausnahmen:
Die Betroffenen müssen u. a. dann nicht benachrichtigt werden, wenn:

- geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und auf die betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche Maßnahmen, durch welche die Daten für alle Personen, die nicht zum Zugang befugt sind, unzugänglich gemacht wurden.
- sichergestellt ist, dass die Maßnahmen nach der Datenpanne aller Wahrscheinlichkeit nach dafür sorgen, dass für die Betroffenen kein hohes Risiko mehr besteht.

Über 9 Millionen Mietverträge eines großen deutschen Autovermieters standen monatelang frei zugänglich im Internet – mit allen Daten inklusive Namen, Adresse und Führerscheinnummer. Ursache der Datenpanne: Backups der Firmendatenbank wurden auf einem ungeschützten Server gespeichert.

(Quelle: heise)

Die Benachrichtigung von Betroffenen: Wie?

Üblicherweise werden die von der Datenpanne Betroffenen **per Brief oder E-Mail** benachrichtigt. Aber was passiert, wenn die Zahl der Betroffenen sehr hoch ist? Oder wenn keine entsprechenden Kontaktdaten vorliegen?

Falls die individuelle Benachrichtigung einen unverhältnismäßigen Aufwand bedeutet, schreibt die DSGVO stattdessen eine **öffentliche Bekanntmachung** vor. In beiden Fällen – Benachrichtigung oder öffentlicher Bekanntmachung – verlangt die DSGVO, dass die Betroffenen in klarer und einfacher Sprache informiert werden.

Die Benachrichtigung von Betroffenen: Was?

Was würden Sie wissen wollen, wenn Sie von der Datenpanne betroffen wären?

Die DSGVO schreibt mindestens die folgenden Auskünfte vor:
- die Art der Datenpanne *(Was ist passiert?)*
- den Namen und die Kontaktdaten des oder der Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen *(An wen kann ich mich wenden?)*
- eine Beschreibung der wahrscheinlichen Folgen der Datenpanne *(Was könnte mir passieren?)*
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen, um die Datenpanne zu beheben oder ihre Folgen abzumildern. Für die Betroffenen ist besonders wichtig, zu erfahren, was sie selbst tun können, z. B. ihre Passwörter ändern. *(Wie kann ich mich schützen?)*

Tipp: Einfache, verständliche, konstruktive Informationen nützen nicht nur den Betroffenen, sondern auch Ihrem Unternehmen. Denn sie wirken vertrauensbildend, was gerade angesichts einer Datenpanne sehr wichtig ist.

Eine Datenpanne in Deutschland betrifft im Durschnitt **26.610 Datensätze.**

(Quelle: IBM Security 2019 Cost of a Data Breach Report)

Die öffentliche Bekanntmachung: Wie, wo und was?

- **Wie?** Die DSGVO spricht von einer öffentlichen Bekanntmachung oder einer ähnlichen Maßnahme. Entscheidend ist, dass sie die Betroffenen „vergleichbar wirksam" zu einer individuellen Benachrichtigung über die Datenpanne informieren.

- **Wo?** Beispielsweise durch Anzeigen in Tageszeitungen oder unter bestimmten Voraussetzungen im Internet. Die Information muss möglichst viele Betroffene erreichen.

- **Was?** Die Inhalte entsprechen der Benachrichtigung von Betroffenen. Also die Art der Datenpanne, Name und Kontaktdaten einer Anlaufstelle für weitere Informationen, eine Beschreibung der wahrscheinlichen Folgen der Datenpanne sowie der bereits ergriffenen und zu empfehlenden Schutzmaßnahmen.

Zum Nachlesen: Artikel 34 DSGVO

04 | Wie muss eine Datenpanne dokumentiert werden?

Das Wichtigste vorweg: Jede Datenpanne muss dokumentiert werden. Auch solche, die nicht an die Aufsichtsbehörde gemeldet werden mussten.

- **Wer?** Für die Dokumentation ist die Geschäftsführung verantwortlich. Sie delegiert diese Aufgabe in der Regel aber an zuständige Mitarbeiterinnen oder Mitarbeiter, zum Beispiel an die Rechtsabteilung.

- **Was?** Zu dokumentieren sind:
  - alle mit der Datenpanne zusammenhängenden Fakten
  - ihre Auswirkungen
  - die ergriffenen Abhilfemaßnahmen

Zum Nachlesen: Artikel 33, Absatz 5 DSGVO.

Tipp: Falls Ihre Datenpanne durch einen Cyberangriff verursacht wurde, finden Sie in unserem Perseus Leitfaden **„Was tun im Cybernotfall?“** weitere Hinweise, um diese Situation zu bewältigen.

Disclaimer

Unsere Datenschutz-Whitepaper dienen dazu, Ihnen einen Überblick über bestimmte datenschuztrechtliche Themen zu geben und Sie hierfür zu sensibilisieren. Sie erheben keinen Anspruch auf Vollständigkeit und stellen keine Form der Rechtsberatung dar. Insbesondere können sie eine Rechtsberatung im Einzelfall nicht ersetzen.

Impressum

Perseus Technologies GmbH | Hardenbergstraße 32 | 10623 Berlin
Telefon: +49 (30) 959998080 | E-Mail: info@perseus.de
Geschäftsführer: Christoph Holle

Handelsregister: Amtsgericht Charlottenburg HRB 180356 B
USt.-Ident-Nr.: DE308271739
Verantwortlicher gem. § 55 Abs. 2 RStV: Christoph Holle