Reaktionsplan bei Datenschutzpannen

Damit der Verantwortliche die Meldepflichten entsprechend der gesetzlichen Vorgaben zügig umsetzen kann, wurde er auf den Eintritt von Datenpannen und die anschließende Reaktion vorbereitet. Die nachfolgende Dokumentation zeigt die einzelnen Schritte auf, dazu gehören auch klare Zuständigkeitsregelungen.

Der Reaktionsplan des Unternehmens enthält folgende Schritte:

1. Schnelle Kenntniserlangung von Datenpannen
2. Bewertung
3. Maßnahmen zur Abwendung/Eindämmung
4. Entscheidung ob eine Meldung erfolgen soll
5. Meldung an die Aufsichtsbehörde und/oder den Betroffenen

1) Schnelle Kenntniserlangung

Der erste Schritt, die zügige Kenntniserlangung von Datenpannen und deren anschließende Weiterleitung an den Datenschutzbeauftragten erfolgt unverzüglich. **Das Zeitfenster bis zur Meldung an die Aufsichtsbehörde beträgt 72 Sunden, unabhängig von Wochenenden oder Feiertagen.**

2) Bewertung von Datenpannen

Nach Meldung an den Datenschutzbeauftragten wird dieser anschließend gemeinsam mit dem Verantwortlichen eine Bewertung der Datenpanne durchführen. Mögliche Kriterien zur Ermittlung des Risikos einer Datenschutzpanne sind u.a. die Kategorien der betroffenen Daten oder die Art der Verletzung.

3) Durchführung von Gegenmaßnahmen

Gemeinsam mit dem Verantwortlichen entwickelt der Datenschutzbeauftragte unverzüglich einen Plan mit effektiven Gegenmaßnahmen, diese werden dann sofort umgesetzt. Diese Maßnahmen reduzieren möglichst den möglichen Schaden, verhindern auf alle Fälle eine Ausweitung des Schadens.

4) Entscheidung über die Meldung des Vorfalls

An die Bewertung der Datenpanne schließt sich die Entscheidung an, ob eine Meldung an die Aufsichtsbehörde und/oder an den Betroffenen erfolgen soll. Bei der Entscheidung ist in Unternehmen die Geschäftsführung einbezogen. Bei positiver Entscheidung erfolgt dann die Meldung an die Aufsichtsbehörde und/oder den Betroffenen

5) Meldung an die Aufsichtsbehörde und/oder den Betroffenen

Auf den Seiten der Landes-Aufsichtsbehörden wird Verantwortlichen die Möglichkeit gegeben, die Meldung einer Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO, umgangssprachlich „Datenpanne“ genannt, online vorzunehmen.

Die Meldung muss vom Verantwortlichen gemacht, es empfiehlt sich aber immer vorher Ihren Datenschutzbeauftragten zu kontaktieren.

FAQ’s - Fragen bei einer Datenpanne

Beispielhaft sind nachfolgend die Fragen aufgelistet, die in der Regel bei Meldung einer Datenpanne zu beantworten sind:

Wo ist die Datenpanne passiert?

Name der betroffenen Stelle (z.B. Unternehmen, Verein, Praxis)
Name des Verantwortlichen
Straße und Hausnummer
PLZ und Ort

Name der meldenden Person
Funktion der meldenden Person beim Verantwortlichen
E-Mail-Adresse der meldenden Person
Telefon-Nr. der meldenden Person

Was ist passiert?

An dieser Stelle genügt eine kurze Zusammenfassung des Vorfalls. Mögliche 'Datenpannen' sind z.B.:Fehlversendung/Sendung an falschen Adressaten, Unberechtigte Weitergabe/unberechtigter Zugriff Dritter, Datenverlust durch verloren gegangenes Medium, Datenverlust durch Hacking, Datenverlust durch Ausspähen (z. B. Skimming) , Datenverlust durch Diebstahl, Datenverlust durch sonstige Umstände (bitte erläutern).

Beschreibung der Datenpanne

Zeitpunkt des Vorfalls
Zeitpunkt der Kenntnisnahme des Vorfalls

Welche Datenarten sind betroffen?

Nennung der Datenkategorien wie z.B. Beschäftigtendaten, Kundendaten, Bankverbindungsdaten, Gesundheitsdaten etc.

Die Daten wie vieler Personen sind betroffen?

Falls die Zahl der Betroffenen nicht genau ermittelt werden kann oder konnte, geben Sie bitte eine geschätzte Obergrenze an.

Risikoeinschätzung

Welche Folgen der Verletzung des Schutzes personenbezogener Daten halten Sie für wahrscheinlich?
Die wahrscheinlichen oder bereits eingetretenen nachteiligen Folgen für die Betroffenen (z.B. unberechtigte Kontoabbuchungen, Identitätsdiebstahl, Ruf-/Imageschädigung, Existenzgefährdung, Lebensgefährdung, Bloßstellung, Identitätsdiebstahl, Geheimnisoffenbarung) sind aufzuführen.

- Welche Gegenmaßnahmen wurden vom Verantwortlichen ergriffen oder werden vorgeschlagen?
- Welche Gegenmaßnahmen haben Sie bereits eingeleitet, welche weiteren Gegenmaßnahmen sind geplant?
- Besteht nach Ihrer Einschätzung für Sie die Pflicht, die Betroffenen zu benachrichtigen (Art. 34 DS-GVO)?

Falls nein: Bitte begründen Sie Ihre Entscheidung.

Geben Sie bitte hier an: Wann wurden oder werden die Betroffenen über den Vorfall informiert? Auf welche Weise wurden oder werden die Betroffenen informiert? Welche konkreten Gegenmaßnahmen haben Sie den Betroffenen empfohlen?
Falls ja: Wie und wann wurden (werden) die Betroffenen benachrichtigt und welche Gegenmaßnahmen haben Sie ihnen empfohlen?

Sonstige Mitteilungen

Wurde Strafanzeige erstattet? Falls ja, teilen Sie uns bitte die betreffende Dienststelle und das Aktenzeichen mit.
Sonstige Mitteilung an die Datenschutzaufsichtsbehörde.