



Hinweise zur Meldepflicht bei „Datenpannen“ nach Art. 33 und 34 EU-DSGVO

Sofern eine Verletzung des Schutzes personenbezogener Daten geschehen ist, besteht für die verantwortliche Stelle eine Meldepflicht gegenüber der Aufsichtsbehörde und eine Benachrichtigungspflicht gegenüber der betroffenen Person.

Eine solche Verletzung kann beispielsweise durch fehlerhafte Übermittlung, durch Gehackt-Werden, durch Datendiebstahl oder durch Verlieren eines Datenträgers geschehen.

1. Meldung an die Aufsichtsbehörde

Eine Meldung muss erfolgen, sofern eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat und diese voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies ist meist der Fall, denn es ist bei den meisten Vorfällen nicht auszuschließen, dass ein solches Risiko besteht. Anderenfalls ist der Ausschluss des Risikos nachzuweisen („Rechenschaftspflicht“).

Inhalt der Meldung:

1. Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien der Daten und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien der Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze,
2. Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
3. Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
4. Beschreibung der von der verantwortlichen Stelle ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die Aufsichtsbehörde ist der „Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg“ (LfDI)

Hausanschrift: Lautenschlagerstr. 20, 70173
Stuttgart

Postanschrift: Postfach 10 29 32, 70025 Stuttgart
Fax: 0711-671181341-15

Zeitpunkt der Meldung

Eine Meldung der Datenpanne muss innerhalb von **72 Stunden** erfolgen. Das Überschreiten der Frist ist nur in begründeten Fällen möglich. Die Begründung ist der verzögerten Meldung beizufügen.

Liegen die für die Meldung erforderlichen Informationen im Meldezeitraum noch nicht vollständig vor, sind diese unverzüglich schrittweise zur Verfügung zu stellen.

2. Benachrichtigung der betroffenen Person

Eine Benachrichtigung muss erfolgen, sofern eine Verletzung des Schutzes personenbezogener Daten stattgefunden hat und diese voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies ist u. a. dann der Fall, wenn sog. besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 EU-DSGVO oder Daten über schulische Leistungen (Noten, Kompetenzen, Beurteilungen) einer Schülerin bzw. eines Schülers betroffen sind.

Keine Benachrichtigung ist erforderlich, wenn

- die verantwortliche Stelle geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat, die den Unbefugten Zugang auf die personenbezogenen Daten praktisch nicht ermöglichen, etwa durch Verschlüsselung der Daten,
- die verantwortliche Stelle durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko, das zum Zeitpunkt der Datenpanne bestand, beseitigt wurde,
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. Stattdessen muss eine öffentliche Bekanntmachung oder ähnliche Maßnahme erfolgen, durch die die betroffene Person vergleichbar wirksam informiert wird.

Inhalt der Benachrichtigung:

1. Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache,
2. Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

3. Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,
4. Beschreibung der von der verantwortlichen Stelle ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Verstöße gegen diese Melde- und Benachrichtigungspflicht sind mit hohem Bußgeld belegt.

Die **Meldung** an die Aufsichtsbehörde bei Datenpannen hat immer zu erfolgen, es sei denn, dass die Datenpanne „voraussichtlich nicht zu einem Risiko“ für die betroffene Person führt.

Die **Benachrichtigung** der betroffenen Person muss jedoch nur dann erfolgen, wenn ein **hohes** Risiko für deren Rechte und Freiheiten besteht.

Der LfDI hat auf seiner Homepage ein **elektronisches Formular** zur Meldung bereitgestellt.