Infoblatt „Meldung von Datenschutzverstößen“

Datenschutzvorfälle sind häufig mit Risiken für betroffene Personen verbunden. Häufig sind eine schnelle Aufklärung und das Ergreifen von Maßnahmen notwendig, die das Risiko verringern und den betroffenen Personen helfen, sich vor möglichen Schäden zu schützen.

Aus diesem Grund sind Verantwortliche nach Art. 33 DSGVO und § 65 BDSG grundsätzlich verpflichtet eine Verletzung des Schutzes personenbezogener Daten (sog. Datenpannen oder Datenschutzvorfälle) an die zuständige Datenschutzaufsichtsbehörde zu melden und u. U. auch betroffene Personen zu benachrichtigen.

Was ist eine „Verletzung des Schutzes personenbezogener Daten“?

Eine „Verletzung des Schutzes personenbezogener Daten“ liegt in jeder Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Dies kann z. B. der Fall sein, wenn Hacker im Rahmen eines Cyber-Angriffs personenbezogene Daten abgreifen oder wenn Datenträger (z. B. USB-Sticks, Festplatten, Laptops) mit personenbezogenen Daten verloren gehen oder gestohlen werden.

Gibt es Ausnahmen zur Meldepflicht an die Datenschutzaufsichtsbehörde und zur Benachrichtigung der betroffenen Personen?

Die gesetzlichen Melde-und Benachrichtigungspflichten des Datenschutzrechts folgen dem sog. risikobasierten Ansatz:

Eine Meldung an die Datenschutzaufsichtsbehörde kann nur ausnahmsweise unterbleiben, wenn der Vorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Ansonsten ist der Vorfall zumindest der Datenschutzaufsichtsbehörde zu melden. Ist der Vorfall voraussichtlich sogar mit einem hohen Risiko für die betroffenen Personen verbunden, hat der Verantwortliche zusätzlich die betroffenen Personen zu benachrichtigen.

Welchen gesetzlichen Mindestinhalt muss eine Meldung an die Datenschutzaufsichtsbehörde haben?

Die Meldung muss mindestens die inhaltlichen Angaben nach Art. 33 Abs. 3 DSGVO bzw. § 65 Abs. 2 BDSG enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggfs. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Gibt es Fristen für die Melde-und Benachrichtigungspflichten?

Nach den gesetzlichen Bestimmungen hat der Verantwortliche einen solchen Vorfall an die Datenschutzaufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung ihm bekannt wurde, zu melden. Zudem hat der Verantwortliche auch die betroffenen Personen unverzüglich zu benachrichtigen, wenn der Vorfall voraussichtlich ein hohes Risiko für diese zur Folge hat.

Was ist wenn nach 72 Stunden noch nicht alle erforderlichen Informationen für die Meldung ermittelt werden konnten?

Insbesondere bei größeren und komplexeren Datenschutzvorfällen werden Verantwortliche u. U. länger als 72 Stunden benötigen, um alle Informationen zumutbar ermitteln zu können. Können daher noch nicht alle Informationen auf einmal bereitgestellt werden, kann der Verantwortliche die Informationen

auch schrittweise zur Verfügung stellen. Bei der schrittweisen Zurverfügungstellung darf es jedoch nicht zu einer unangemessenen weiteren Verzögerung kommen.

Wie geht das Verfahren bei dem BfDI nach der Meldung weiter?

Sofern der BfDI zuständig ist, prüft der BfDI die Meldung des Datenschutzvorfalles und die erkennbaren Risiken. Sie wird u. U. beratend auf weitere Maßnahmen zur Eindämmung der Risiken und Verbesserung der technisch-organisatorischen Maßnahmen hinweisen. Sofern erforderlich, wird der BfDI zudem von ihren datenschutzaufsichtsbehördlichen Untersuchungs-und Abhilfebefugnissen Gebrauch machen.

Ist ein Verstoß gegen die Melde- und Benachrichtigungspflichten aus Art. 33, 34 DSGVO bußgeldbewehrt?

Bei einem Verstoß gegen die Melde-und Benachrichtigungspflichten aus Art. 33, 34 DSGVO können bei Vorliegen der notwendigen Voraussetzungen gemäß Art. 83 Abs. 4 DSGVO Geldbußen von bis zu 10.000.000 Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher Betrag höher ist.