Information zur „Meldung einer Datenschutzverletzung“

Zweck des Datenschutzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten (oder Informationen über ihn) in seinem Persönlichkeitsrecht beeinträchtigt wird. Wie personenbezogenen Daten dabei verarbeitet werden (analog oder digital), spielt keine Rolle.

IT-Sicherheitsvorfälle sind häufig auch mit Risiken für Rechte und Freiheiten von Personen verbunden. Aus diesem Grund sind Verantwortliche nach § 33 KDG (Gesetz über den Kirchlichen Datenschutz) grundsätzlich verpflichtet eine Verletzung des Schutzes personenbezogener Daten (ein sogenannter Datenschutzvorfall) an die zuständige Datenschutzaufsicht zu melden. Unter bestimmten Umständen sind nach § 34 KDG auch davon betroffene Personen zu benachrichtigen.

1. Was ist eine „Verletzung des Schutzes personenbezogener Daten“?

Eine „Verletzung des Schutzes personenbezogener Daten“ liegt vor, sobald unberechtigte Personen vermutlich oder erwiesenermaßen Kenntnis von personenbezogenen Daten nehmen können oder könnten.

Der Begriff „Verletzung des Schutzes personenbezogener Daten“ wird in § 4 Nr. 14 KDG definiert als „eine 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“.

2. Gibt es Ausnahmen zur Meldepflicht an die Datenschutzaufsicht?

Eine Meldepflicht besteht laut § 33 Abs.1 KDG sobald eine Verletzung des Schutzes personenbezogener Daten eine Gefahr für die Rechte und Freiheiten natürlicher Personen (Betroffene) darstellt. Im Umkehrschluss kann eine Meldung ausnahmsweise unterbleiben, wenn der Vorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Demnach hat vor einer Meldung an die Datenschutzaufsicht eine risikobasierte Einschätzung des Vorfalls zu erfolgen. Dabei ist mit einem Restrisiko zu rechnen, weil nicht immer zeitnah alle Auswirkungen des Vorfalls überblickt werden können. Als Beispiel wäre ein Cyberangriff bei dem u.a. erfolgreich Daten verschlüsselt werden konnten (Ransomware). Wieweit personenbezogene Daten abgeflossen sein könnten, ist zum Entdeckungszeitpunkt nicht immer sofort ersichtlich.

Daher unsere Empfehlung, Sicherheits- und Datenschutzvorfälle zeitnah zu melden.

3. Gibt es Ausnahmen zur Benachrichtigung der betroffenen Personen?

Wie unter Punkt 2, handelt es sich auch hier um einen risikobasierten Ansatz. Eine Benachrichtigung hat aber erst dann zu erfolgen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten betroffener Personen zur Folge hat (§ 34 Abs.1 KDG).

Für die Benachrichtigung der betroffenen Personen gilt demnach ein höherer Schwellenwert als bei der Meldepflicht an die Datenschutzaufsicht.

4. Welchen gesetzlichen Mindestinhalt muss eine Meldung an die Datenschutzaufsicht haben?

Die Meldung muss mindestens die inhaltlichen Angaben nach § 33 Abs. 3 KDG enthalten:

a. 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 personenbezogenen Datensätze;

b. den Namen und die Kontaktdaten des betrieblichen Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c. eine Beschreibung der möglichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Ein Formular finden Sie auf unserer Website unter https://www.kdsa-ost.de/meldestelle

5. Gibt es Fristen für die Melde- und Benachrichtigungspflichten?

Nach den gesetzlichen Bestimmungen hat der Verantwortliche eine Datenschutzverletzung unverzüglich zu melden. Spätestens jedoch innerhalb von 72 Stunden nach Bekanntwerden des Vorfalls. Zu beachten ist, dass diese Frist auch an Wochenenden und an Feiertagen einzuhalten ist.

Nach Ablauf der Meldefrist ist zusätzlich zur Meldung an die Datenschutzaufsicht eine Begründung für die Verzögerung beizufügen.

6. Wie geht das Verfahren bei der KDSA Ost nach der Meldung weiter?

Die KDSA Ost prüft die eingegangene Meldung des Datenschutzvorfalles auf ihre Zuständigkeit und bearbeitet diese nach den internen Prozessen. Für den Fall das wir nicht zuständig sind, leiten wir die Meldung eine zuständige Datenschutzaufsicht weiter (§ 46 KDG).

Der Verantwortliche erhält an seine Postadresse eine Eingangsbestätigung mit ggfs. weiteren Informationen.

7. Ist ein Verstoß gegen die Melde- und Benachrichtigungspflichten bußgeldbewehrt?

Bei einem Verstoß gegen die Bestimmungen des KDG kann die Datenschutzaufsicht eine Geldbuße verhängen (§ 51 KDG).

8. Ist bei einer Datenschutzverletzung ein Schadensersatzanspruch möglich?

Hat die Datenschutzaufsicht die Feststellung getroffen, dass eine Datenschutzverletzung objektiv vorliegt, kann die betroffene Person vor den staatlichen Zivilgerichten einen Schadensersatzanspruch geltend machen.

KDSA Ost
Die Kirchliche Datenschutzaufsicht
der ostdeutschen Bistümer und des
Katholischen Militärbischofes

Platz für Notizen