7 Umgang mit Datenschutzverstößen

Der beste Schutz von personenbezogenen Daten kann niemals zu einhundert Prozent vor einer Schutzverletzung von personenbezogenen Daten schützen. Davon ausgehend ist bereits vor einer eventuellen Datenschutzverletzung ein Prozess zum korrekten Umgang mit dem Fall der Fälle zu entwickeln und zu implementieren.

7.1 Was sind Datenschutzverstöße?

Die Definition für Datenschutzverstöße finden wir in Art. 4 Nr. 12 DS-GVO.

Eine „Verletzung des Schutzes personenbezogener Daten" ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von – bzw. zum un-

> *befugten Zugang zu – personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.*

Die reine Offenlegung von personenbezogenen Daten gegenüber Unbefugten ist also schon ein Datenschutzverstoß. Ein solcher Verstoß passiert recht schnell. In einer E-Mail mit mehreren Empfängern wird versehentlich ein falscher Empfänger ausgewählt. Das bedeutet, dass die anderen E-Mail-Adressen, also personenbezogene Daten, dem versehentlich ausgewählten Empfänger offengelegt werden. Gleiches passiert regelmäßig bei der Arbeit in der Bahn, am Flughafen oder an anderen öffentlichen Plätzen. Es ist oftmals ein leichtes, die Inhalte auf Smartphones und Laptops einzusehen oder die von lauten Telefonaten mitzuhören zu können. Aber auch unter Kollegen ist eine Offenlegung von personenbezogenen Daten schnell passiert. Sie sitzen an Ihrem Platz und bearbeiten personenbezogene Daten von Kunden oder anderen Kollegen (Personalabteilung). Ein Kollege kommt vorbei und steht plötzlich direkt neben Ihnen mit Blick auf Ihren Monitor. Sind die Daten nicht für den Kollegen zur Durchführung seiner Tätigkeit notwendig, so liegt eine Offenlegung von personenbezogenen Daten gegenüber einem Unbefugten vor.

Es gibt aber weitaus schlimmere Datenschutzverstöße. Ein verlorenes, unverschlüsseltes oder gestohlenes Notebook, offene und ungesicherte Server im Internet, gestohlene Zugangsdaten von Onlineportalen, versehentlich oder mutwillig gelöschte Daten usw. – die Liste ist beinahe unendlich.

Eine wichtige Überlegung für die nächsten Schritte ist an dieser Stelle wieder die Risikobewertung. Welche Auswirkungen sind für die betroffenen Personen im schlimmsten Fall zu erwarten? Bei Datenschutzverstößen rund um Namen oder E-Mail-Adressen sind diese sicherlich überschaubar.

Bei der Offenlegung von Zugangsdaten, Bankdaten oder Gesundheitsdaten sind die zu erwartenden Risiken für den Betroffenen unter Umständen existenzgefährdend oder sogar lebensbedrohlich.

Sie erinnern sich sicherlich an die Risikobetrachtungen aus dem Kapitel 6 „Technische und organisatorische Maßnahmen“. Diese Risikobetrachtungen finden hier erneut Anwendung.

Im Falle einer Datenschutzverletzung sind zwei Artikel der DS-GVO zu berücksichtigen.

Artikel 33 DS-GVO beschreibt die Meldung von Verletzungen des Schutzes personenbezogener Daten bei der Aufsichtsbehörde und Artikel 34 DS-GVO

beschreibt die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person(en).

Es ist unbedingt zu beachten, dass in beiden Fällen die Meldung vom Verantwortlichen vorzunehmen ist. Hier sollte der Datenschutzbeauftrage also lediglich Unterstützung leisten bei der Erarbeitung des Vorfalls und bei den zu treffenden Gegenmaßnahmen.

7.2 Meldung an die Aufsichtsbehörde

Nach Artikel 33 DS-GVO sind Datenschutzverstöße unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde zu melden. Wurde die Schutzverletzung bei einem Auftragsverarbeiter bekannt, so meldet sie dieser unverzüglich dem Verantwortlichen, aber niemals direkt an die zuständige Aufsichtsbehörde.

Die Meldung umfasst zumindest folgende Informationen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
- die Kategorie der Daten
- die ungefähre Zahl der betroffenen Personen
- die Kategorie der betroffenen Personen
- die ungefähre Anzahl der betroffenen Datensätze
- den Namen und die Kontaktdaten des Datenschutzbeauftragten
- eine Beschreibung der wahrscheinlichen Folgen und
- eine Beschreibung der ergriffenen Maßnahmen zur Behebung der Schutzverletzung und zur Abmilderung der Folgen.

Sollte es nicht möglich sein, all diese Informationen innerhalb der genannten Frist zu melden, so können die Informationen auch ohne weitere Verzögerung nachgereicht werden. Zusätzlich dokumentiert der Verantwortliche die Datenschutzverstöße und sollte diese Dokumentation aufbewahren.

Datenschutzverstöße sind nicht zu melden, wenn voraussichtlich nicht mit einem Risiko für die Rechte und Freiheiten natürlicher Personen zu rechnen ist. Hierzu ein Beispiel: Eine Instanz der Kundendatenbank wird versehentlich oder unberechtigt gelöscht. Die Datenbank wurde aber bereits auf einen anderen Server umgezogen und sollte in der nächsten Woche nach einem Test der neuen Datenbank gelöscht werden. An dieser Stelle ist nicht mit ei-