Up to Data: Die Datenpanne

Im letzten Newsletter hatte Sie die RKM Data GmbH darüber informiert, was ein Cyber-Angriff ist und welche Konsequenzen in datenschutzrechtlicher Sicht damit einhergehen. Hierbei hatten wir erwähnt, dass ein Cyber-Angriff auf Unternehmen meistens auch mit einer meldepflichtigen Datenpanne verbunden ist. Was genau unter einer Datenpanne zu verstehen ist und wie Sie damit als Unternehmen umzugehen haben, erfahren Sie in diesem Newsletter.

1. Was ist eine Datenpanne?

Eine Datenpanne stellt die Verletzung des Schutzes von personenbezogenen Daten dar. Nach Art. 4 Nr. 12 DSGVO liegt eine Verletzung von personenbezogenen Daten dann vor, wenn diese Daten verloren gegangen sind, vernichtet oder unbefugt offengelegt wurden.

Um diese abstrakten Begriffe genauer zu erläutern, haben wir Ihnen Beispiele für mögliche Datenpannen aufgelistet. In diesen Fällen sollten Sie aufmerksam werden und sich an den Datenschutzbeauftragten und die Geschäftsleitung wenden:

- E-Mail wird an falschen Empfänger gesendet und kommt nicht zurück
- Gehaltsabrechnung wird an falschen Empfänger übermittelt
- Firmeninternes Speichermedium (unverschlüsselt) wird verloren
- Firmenhardware (Laptop / Handy) mit Kunden- und/oder Mitarbeiterdaten wird gestohlen
- Hacker-Angriff z.B. durch manipulierte E-Mail, bei dem personenbezogene Daten offengelegt werden
- Falsche Auskunft am Telefon
- Einbruch im Betrieb, Geräte werden gestohlen oder Daten abgezogen

2. Fahrplan: Was ist zu tun?

Wenn eine Datenpanne vorgefallen ist, sollte jedes Unternehmen einen „Fahrplan“ implementiert haben, auf den sofort zurückgegriffen werden kann.

1. Schritt: Datenpanne umgehend bemerken

Löst ein Mitarbeiter eine Datenpanne aus oder findet ein Angriff von außen auf die IT-Systeme statt, ist es wichtig, den Datenverlust überhaupt zu bemerken. Bei einer falsch versendeten E-Mail dürfte die Datenpanne meistens dadurch auffallen, dass der falsche Empfänger sich meldet und mitteilt, dass die E-Mail ihn nicht betrifft.

2. Schritt: Erfassen Sie, was passiert ist

Um angemessen auf einen Datenvorfall reagieren zu können, müssen Sie zunächst genau erfassen was passiert ist. Dafür sollten eindeutige Zuständigkeiten definiert sein. Im Anhang finden Sie ein Formular, welches die wesentlichen Fragen stellt, die im Falle einer Datenpanne beantwortet werden müssen.

3. Schritt: Meldepflichten beachten

Auf Grundlage der erfassten Daten wird Ihr Datenschutzbeauftragter eine Risikoabwägung treffen. Ergibt die Risikoabwägung, dass durch die Datenpanne ein Risiko für die Rechte und Freiheiten natürlicher Personen entstanden ist, ist der Vorfall der Behörde (und ggfs. dem Betroffenen) zu melden. Eine Meldung an die Behörde muss in 72 Stunden erfolgen! Wird kein Risiko erkannt, kann die Meldung unterbleiben.

Schritt 4: Dokumentation

Gleichgültig, ob eine Meldung vorzunehmen ist oder ob diese unterbleiben kann: Eine saubere Dokumentation einer jeden Datenpanne ist unabdingbar.
Sie sollten daher das Meldeformular nebst Anhängen und der entsprechenden Einschätzung Ihres Datenschutzbeauftragen zusammen in einem Ordner „Datenschutzvorfallmanagement“ ablegen.

Schritt 5: Schulen und sensibilisieren Sie Ihre Mitarbeiter

Nur wenn Ihre Mitarbeiter über das richtige Vorgehen bei Datenpannen geschult sind, ist eine genaue und fristgerechte Dokumentation möglich.

3. Konsequenzen

Die DSGVO verpflichtet Unternehmen und andere verantwortliche Stellen, beim Bekanntwerden einer Datenpanne die zuständige Aufsichtsbehörde zu informieren. Damit stellt sich die Frage, ob dies nicht automatisch einer „Selbstbezichtigung“ gleichkommt und ein Bußgeld nach sich zieht.

Zu dieser Frage hat der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) in einer Pressemitteilung aus August 2019 Stellung bezogen. Hierin heißt es:

„Dabei stellt sich natürlich die Frage, ob die Meldung einer Datenschutzverletzung zu einem Bußgeldverfahren führt; also quasi die Verpflichtung besteht, sich selbst zu belasten. Das ist nicht der Fall!

Mit der Vorschrift des § 43 Abs. 4 Bundesdatenschutzgesetz (BDSG) wird klargestellt, dass die Meldung einer Datenpanne in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder seine Angehörigen nur mit Zustimmung des Meldepflichtigen verwendet werden darf. Gleiches gilt bei der Einleitung eines Strafverfahrens nach § 42 BDSG. Verantwortliche müssen daher bei einer Meldung nicht fürchten, dass auf dieser Grundlage ein Bußgeldverfahren eingeleitet wird.“

Zusammengefasst heißt das für Sie: Scheuen Sie sich nicht davor, Datenpannen auch wirklich zu melden, wenn der Datenschutzbeauftragte zu einer Meldepflicht gelangt. Die Verhängung eines Bußgeldes ist nicht automatisch mit der Meldung einer Datenpanne verbunden.

4. Anhang: Das Meldeformular (s. Anhang)

Sollten Sie zu diesem Themenbereich weitere Fragen haben, stehen wir Ihnen jederzeit gerne zur Verfügung.

Ihr Team der RKM Data GmbH