Reaktionsplan bei Datenpanne

Für

Sandra Wirtz, Praxis für Psychotherapie nach Heilpraktikergesetz

Lisztstrasse 3, 65520 Bad Camberg

1. Schnelle Kenntniserlangung von Datenpannen
2. Bewertung
3. Maßnahmen zur Abwendung/Eindämmung
4. Entscheidung ob eine Meldung erfolgen soll
5. Meldung an die Aufsichtsbehörde oder den Betroffenen

Schnelle Kenntniserlangung

Durch zügiges Handeln kann viel Schaden abgewendet.

Bewertung von Datenpannen

Wird der Vorfall zügig an den Datenschutzbeauftragten herangetragen, so kann dieser anschließend eine Bewertung der Datenpanne durchführen. Der Reaktionsplan sollte Leitlinien oder Kriterienkataloge enthalten, die eine zügige Bewertung und Risikoanalyse ermöglichen. Mögliche Kriterien zur Ermittlung des Risikos einer Datenschutzpanne sind u.a. die Kategorien der betroffenen Daten oder die Art der Verletzung.

Durchführung von Gegenmaßnahmen

Ein Reaktionsplan sollte für die verschiedenen Arten von Datenschutzpannen entsprechende Gegenmaßnahmen enthalten und deren Durchführung hinreichend beschreiben. Hierfür kann insbesondere auf die Erfahrung aus der Bewältigung vergangener Datenpannen zurückgegriffen werden.

Entscheidung über die Meldung des Vorfalls

An die Bewertung der Datenpanne schließt sich die Entscheidung an, ob eine Meldung an die Aufsichtsbehörde und/oder an den Betroffenen erfolgen soll. Bei der Entscheidung ist in Unternehmen die Geschäftsführung mit einzubeziehen. Bei positiver Entscheidung erfolgt dann die Meldung an die Aufsichtsbehörde und/oder den Betroffenen. Nähere Informationen zu den formalen Anforderungen an die Mitteilung finden Sie in unserem Beitrag zur Data Breach Notification.

Beispiele für Datenpannen, die eine Meldung an die Aufsichtsbehörde und den Betroffenen erfordern:

- Ein großes E-Commerce-Unternehmen wird Opfer eines Cyper-Angriffs und Hacker veröffentlichen Namen und Passwörter von Kunden
- Für die Behandlung von Patienten notwendige Gesundheitsdaten sind in einem Krankenhaus für einen Zeitraum von über 24 Stunden nicht abrufbar

- Eine große Zahl personenbezogener Daten von Studenten wird an eine falsche Empfängerliste mit über 5000 Empfängern geschickt

Beispiele für Datenpannen, die in der Regel keine Meldung erfordern:

- Abhandenkommen eines mobilen Datenträgers, der nach aktuellem Standard verschlüsselt ist
- Ein kurzer Stromausfall in einem Call-Center, der dazu führt, dass Kunden vorübergehend die für sie relevanten Daten nicht abfragen können

Meldung an Aufsichtsbehörde und Betroffenen

Zuständige Aufsichtsbehörde für Sandra Wirtz, Praxis für Psychotherapie nach Heilpraktikergesetz

Der Hessische DatenschutzbeauftragteGustav-Stresemann-Ring 1 • 65189 Wiesbaden

Tel.: 0611 1408-0

Fax : 0611 1408-900 oder -901

E-Mail: poststelle@datenschutz.hessen.de

Web: www.datenschutz.hessen.de

Formale Anforderungen an die Data Breach Notification

Hinsichtlich der formalen Anforderungen an die Data Breach Notification werden in den Art. 33, 34 DSGVO jeweils Mindestanforderungen geregelt. Notwendig ist bei der Meldung an die Aufsichtsbehörde:

- 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;
- der Name 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 gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die letzten drei Punkte sind auch bei der Benachrichtigung der Betroffenen zu berücksichtigen. Zudem ist in diesen Fällen die Meldung in einer klaren und einfachen Sprache zu verfassen.

Meldefristen

Sowohl die Data Breach Notification an die Aufsichtsbehörde als auch die Benachrichtigung der Betroffenen haben, wie bisher nach § 42a BDSG unverzüglich, also ohne schuldhaftes Zögern, nach Kenntniserlangung zu erfolgen.

Jedoch wird in Art. 33 Abs. 1 DSGVO für die Meldung an die Aufsichtsbehörde im Gegensatz zum BDSG ein gesetzlicher Richtwert von 72 Stunden für den Ablauf der Unverzüglichkeit angenommen. Erfolgen Data Breach Notifications erst nach Ablauf dieser Frist, muss die Verzögerung gesondert begründet werden.

Dokumentationspflichten

DSGVO-typisch werden dem Verantwortlichen nach Art. 33 Abs. 5 DSGVO in Bezug auf die Data Breach Notification außerdem Dokumentationspflichten hinsichtlich aller Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen auferlegt.