Nach einer Datenpanne tickt die Uhr

Dominik Schelling, 1. Mai 2018, 11:00

Im Notfall zwingt die DSGVO zur umfassenden Benachrichtigung der Behörde – innerhalb von 72 Stunden

Wien – Selbst das sicherste IT-System kann Datenpannen nicht ganz verhindern. Für diesen datenschutzrechtlichen Worst Case sieht die Datenschutz-Grundverordnung (DSGVO), die ab 25. Mai anzuwenden ist, ein straffes Prozedere samt Melde- und Benachrichtigungspflichten vor. Dies stellt eine deutliche Verschärfung der bisherigen Rechtslage dar. Um diese neuen Regeln innerhalb der sehr kurzen gesetzlichen Fristen einhalten zu können, müssen sich die Unternehmen proaktiv auf den Datennotfall vorbereiten.

Meldepflichtig ist jede Verletzung der Sicherheit personenbezogener Daten, die zu Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu Daten führt. Ein Data-Breach liegt z. B. bei Verlust oder Diebstahl von Laptops oder Geschäftstelefon mit personenbezogenen Daten, Liegenlassen eines USB-Sticks in der U-Bahn, aber auch bei einem Hackerangriff oder einer Infektion eines Computersystems mit Ransomware vor.

Im Fall einer Datenpanne ist neben der Ergreifung von Sofortmaßnahmen – etwa der Sperrung des Geräts oder der Trennung vom Internet – binnen 72 Stunden nach Bekanntwerden des Vorfalls eine Meldung an die Datenschutzbehörde zu erstatten. Die Uhr tickt also spätestens mit tatsächlicher Kenntnis der Datenpanne. Aber auch bei einem bloßen Verdacht sind sofort interne Untersuchungen zur Aufklärung einzuleiten. Diesfalls läuft die 72-Stunden-Frist, sobald die Datenpanne mit "hinreichender Sicherheit" identifiziert wurde.

Detaillierte Meldung

Die Meldung an die Datenschutzbehörde hat sehr detailliert zu sein und folgenden Mindestinhalt abzudecken:

- Beschreibung der Datenpanne inklusive Angabe der betroffenen Personen und Datenarten;
- Kontaktdaten für Rückfragen der Datenschutzbehörde;
- Schilderung der voraussichtlichen Folgen des Data-Breach;
- Beschreibung der Gegenmaßnahmen zur Behebung bzw. zur Abmilderung der Auswirkungen.

Diese umfangreichen Informationen können in der Praxis nur dann innerhalb der kurzen Frist erstattet werden, wenn das Unternehmen über ein aktuelles Verarbeitungsverzeichnis verfügt und etwaige Folgeabschätzungen im Vorfeld durchgeführt hat. Dort sind nämlich die wesentlichsten Informationen, die der Behörde im Anlassfall zu melden sind, bereits aufgearbeitet.

Resultiert aus der Datenpanne "voraussichtlich ein hohes Risiko" für die Betroffenen, so sind auch diese "unverzüglich" direkt zu informieren – z. B. wenn den Betroffenen materielle oder immaterielle Schäden aus dem Datenschutzverstoß drohen, wie etwa Bloßstellung, Identitätsdiebstahl, Betrug, finanzielle Schäden oder Reputationsschäden. Vor allem wenn der Data-Breach sensible Daten betrifft, ist eine Benachrichtigung der Betroffenen unumgänglich.

Ist sich das Unternehmen unsicher, ob eine unmittelbare Information der Betroffenen erforderlich ist, kann es von der Datenschutzbehörde eine Einschätzung anfordern. Diese kann eine solche Benachrichtigung aber auch proaktiv verpflichtend auferlegen.

Weiterer Verstoß

Die Nichtmeldung von Datenschutzverstößen selbst stellt einen – weiteren – Datenschutzverstoß dar und unterliegt dem strengen Strafenregime. Gleichzeitig wirkt aber auch eine rechtzeitig erstattete Meldung zwar mildernd, aber nicht strafbefreiend, wenn die Datenpanne auf einem DSGVO-Verstoß beruht – etwa weil ein nicht ausreichendes Sicherheitssystem verwendet oder eine generell unzulässige Datenverarbeitung betrieben wurde.

derStandard(Dominik Schelling, 30.4.2018)

Dominik Schelling ist Rechtsanwaltsanwärter bei Dorda Rechtsanwälte und auf Datenschutz- und IT-Recht spezialisiert.