Data Breach – es passiert am laufenden Band

Freitag, 17.07.2026

Unternehmen verarbeiten bei ihrer Tätigkeit umfangreiche Datenbestände, darunter auch personenbezogenen Daten, die von der DSGVO und weiteren Gesetzen geschützt werden. Daten haben im modernen Wirtschaftsleben aufgrund der Digitalisierung eine besondere Bedeutung und sie müssen stets sorgsam geschützt werden, denn die Kunden als Betroffenen erwarten sich von den Unternehmen die Geheimhaltung ihrer personenbezogenen Daten. Sollte jedoch die geforderte Geheimhaltung einmal nicht gewährleistet werden können, führt dies zu einer Verletzung der in der Datenschutzgesetzgebung definierten Schutzzwecke, die für die Verantwortlichen bestimmte Meldepflichten nach sich zieht.

Aus dem Tätigkeitsbericht der österreichischen Datenschutzbehörde (DSB) für das Jahr 2025 (abrufbar unter https://dsb.gv.at, S. 26f) geht hervor, dass in diesem Jahr 1.704 nationale Meldungen über Sicherheitsverletzungen nach Art 33 DSGVO erstattet wurden. Gegenüber 2024 (1.216) war somit eine starke Zunahme in Höhe von 40,13 % feststellbar. Dazu kamen 2025 noch 68 Meldungen, die einen grenzüberschreitenden Bezug hatten und 83 Sicherheitsverletzungen nach dem Telekommunikationsgesetz (TKG 2021).

Wie die DSB berichtet (Tätigkeitsbericht 2025, S. 48ff), betraf eine wesentliche Anzahl der gemeldeten Vorfälle Hackerangriffe mit „unzähligen“ verschiedenen Ransomware-Attacken, deren Ziel die Erpressung mit verschlüsselten Daten war. Zusätzlich wird in diesen Attacken versucht, Daten abzusaugen und in der Folge gedroht, die erbeuteten Daten zu veröffentlichen oder im Darknet zu verkaufen. Unter den betroffenen Daten waren auch Buchhaltungsplattformen, Lohnverrechnungs- und Personalverwaltungssoftwareanbieter, also überaus sensible personenbezogene Daten.

Weitere Sicherheitsverletzungen betrafen menschliches Fehlverhalten, wenn schutzwürdige Datenbestände an falsche Empfänger weitergeleitet wurden, beispielsweise Kontoauszüge, Verträge, Patientenakten oder Ähnliches. Es wurden aber auch Meldungen erstattet, die sich darauf bezogen, dass Unterlagen unsachgemäß entsorgt oder nicht korrekt gelöscht wurden.

Eine weitere gemeldete Missachtung des Datenschutzes betraf absichtliches, bewusstes Setzen von Handlungen, die den Bruch der Datensicherheit zur Folge hatten. Beispielsweise gehörten dazu die Weitergabe oder Veröffentlichung von Patientendaten und Fotos auf Plattformen im Internet oder auch der unberechtigte Zugriff auf vertrauliche Datenbestände innerhalb eines Unternehmens.

Eine andere Kategorie von Meldungen über Datenschutzverletzungen bezog sich auf technische oder organisatorische Mängel in der Datenverarbeitung, die negative Folgen nach sich zogen. Darunter fielen beispielsweise falsche Verknüpfungen von User-

Accounts oder falsche Zugriffsberechtigungen, die unberechtigten Personen Zugang zu sensiblen Datenbeständen ermöglichten. In diesem Zusammenhang ist besonders auf die dem gegebenen Risiko entsprechende Gestaltung von technisch organisatorischen Maßnahmen zu achten.

Mögliche Fehlerquellen sind also mannigfaltig, umso wichtiger ist jedoch der richtige Umgang mit zu Tage getretenen Verletzungen der Datensicherheit. Nach der Feststellung eines Vorfalles hat der Verantwortliche zu prüfen, ob aufgrund der Gegebenheiten von einem Risiko für die Betroffenen auszugehen ist. Wenn die Datenschutzverletzung voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist von der Kenntnisnahme bis zur Meldung an die Datenschutzbehörde, soweit möglich, eine kurze Frist von längstens 72 Stunden einzuhalten. Bei einer späteren Meldung sind jedenfalls Gründe für die erfolgte Verzögerung anzugeben. Die Meldung hat schon die wichtigsten Informationen zu enthalten, die es der DSB ermöglichen sollen, den Vorfall zu beurteilen.

Wenn eine Datenschutzverletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, ist eine Benachrichtigung der betroffenen Personen erforderlich.

Wenn der Verantwortliche die betroffenen Personen nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde im Rahmen ihrer Zuständigkeit verlangen, dies nachzuholen. Die Aufsichtsbehörde hat dabei die Wahrscheinlichkeit zu berücksichtigen, mir der die Verletzung zu einem hohen Risiko führt.

Um die notwendigen Informationen zusammenzustellen, stellt die DSB für die Meldung einer Datenschutzverletzung auf ihrer Webseite (dsb.gv.at) ein entsprechendes Formular zur Verfügung.

Wie die hohe Anzahl der gemeldeten Datenschutzverstöße zeigt, können nahezu alle Unternehmen von einem solchen Vorfall betroffen sein. Oft wird gesagt, dass sich nicht die Frage stellt, ob man Ziel eines Angriffs wird, sondern wann. Daher ist es sicher kein Fehler, sich bereits im Vorfeld darüber Gedanken zu machen, wer im Unternehmen für die Bearbeitung und für die Meldung eines Datenschutzvorfalls zuständig ist und wie der Bearbeitungsprozess ablaufen soll. Eine sorgfältige Planung dieses Abwicklungsprozesses kann zur erfolgreichen Bewältigung der wirtschaftlichen Folgen einer Datenschutzverletzung beitragen.

Mag. Rudolf Urban, MSc
geprüfter Datenschutzexperte