

/ Datenschutzbehörde kündigt mehrstellige Millionenbußgelder wegen Datenschutzverletzungen an - Risiken für Unternehmen steigen

19.07.2019

[Datenschutz](#) | [Digital Business](#) | [Einkauf, Logistik & Vertrieb](#) | [IT & Outsourcing](#) | [Compliance & Interne Ermittlungen](#) | [Regulierung & Governmental Affairs](#)

Empfehlungen zum Data Breach Management

SQL-Injections, Bugs oder andere Sicherheitslücken - dass Daten in unserer zunehmend digitalisierten Welt in falsche Hände geraten, ist sicherlich kein Einzelfall. Sei es ein gezielter Hacking-Angriff auf digitale Assets oder auch nur der versehentliche Verlust von Daten - die Szenarien denkbarer **Datenschutzverletzungen** sind schier unbegrenzt. Hinzu kommt eine nicht unbeachtliche Dunkelziffer nicht erkannter Datenschutzvorfälle. Kürzlich angekündigte Millionenbußgelder lassen nun aufhorchen: Datenschutzpannen bergen erhebliche finanzielle Risiken für Unternehmen.

Bekanntermaßen hat die **Datenschutz-Grundverordnung (DS-GVO)** die Anforderungen an den Umgang mit Datenpannen erheblich verschärft. Nicht zuletzt der vergleichsweise weite Begriff der meldepflichtigen Datenschutzverletzung und die für die Meldung an die zuständige Behörde vorgesehene 72-Stunden-Frist stellen Unternehmen vor enorme Herausforderungen beim Management von Data Breaches.

Schon vor Anwendung der DS-GVO hatten die europäischen Datenschutzbehörden [Leitlinien zur Handhabung von Datenschutzverletzungen](#) veröffentlicht. Auch die deutschen Datenschutzbehörden haben schon früh auf die verschärften Anforderungen beim [Umgang mit Datenpannen](#) und die drohenden Bußgelder bei Verstößen hingewiesen. Zum Teil haben deutsche Aufsichtsbehörden sogar bereits gezielte [Datenschutzprüfungen](#) zum „Incident Response“ angekündigt.

Erste Bußgelder verhängt

Zwar üben sich die deutschen Datenschutzbehörden bei der Verhängung von Bußgeldern für Datenschutzverletzungen bislang noch in Zurückhaltung. Das erste deutsche Bußgeld für Datenschutzverletzungen hatte die **baden-württembergische Datenschutzbehörde (LfDI Baden-Württemberg)** im September 2018 in Höhe von **20.000 Euro** gegen den Social-Media-Anbieter [Knuddels](#) verhängt. Nach Angaben der Datenschutzbehörde war das betroffene Unternehmen wegen konstruktiver Zusammenarbeit mit der Behörde und umfangreicher Verbesserungen bei der Sicherheit glimpflich davongekommen.

Die kürzlich verlautbarten Ankündigungen der **britischen Datenschutzbehörde (ICO)** gleichen demgegenüber einem Paukenschlag: Die Behörde möchte Bußgelder in Höhe von umgerechnet etwa **110 Millionen** und **203,7 Millionen Euro** für Datenschutzverletzungen bei [Marriott](#) und [British Airways](#) verhängen - obwohl auch in diesen beiden Fällen die betroffenen Unternehmen nach Angaben der Datenschutzbehörde bei der Untersuchung der Vorfälle mit der Datenschutzbehörde kooperiert und nach Bekanntwerden der Vorfälle Verbesserungen der Sicherheitsmaßnahmen getroffen haben. Ob die vom ICO angekündigten Bußgelder Ausnahmefälle bleiben werden oder nur einen ersten Vorgeschmack auf die zukünftige Bußgeldpraxis der europäischen Datenschutzbehörden geben, steht in den Sternen. Dennoch dürfte den Ankündigungen eine gewisse Signalwirkung nicht abzusprechen sein.

Weitere Folgeschäden

Ungeachtet etwaiger Bußgelder drohen bei Datenschutzverletzungen und besonders auch bei falscher Handhabung solcher Verletzungen allerdings vor allem erhebliche **Reputationsschäden** für betroffene Unternehmen. Möglicherweise droht auch der **Verlust wichtiger Geschäftsgeheimnisse**. Nicht ausgeschlossen sind im Extremfall außerdem **Schadensersatzforderungen** betroffener Personen.

Wie schützen Sie sich am besten?

Um negative Konsequenzen von Datenpannen bestmöglich zu vermeiden, empfehlen wir die **Sensibilisierung von Mitarbeitern** zur Erkennung und zum richtigen Umgang mit Datenschutzvorfällen und die **Implementierung robuster Data Breach Management Prozesse**. Vorbeugende Maßnahmen und Reaktionspläne gilt es durch gezielte **Trainings** und regelmäßige **Probelaufe** im Sinne eines **kontinuierlichen Prozesszyklus** zu bewerten und zu verbessern. Mit beteiligten Dienstleistern und Kooperationspartnern sollten **praxisgerechte Vereinbarungen zur Unterstützung bei Datenpannen** getroffen werden.

Haben Sie Fragen? Kontaktieren Sie gerne: [Dr. Daniel Rücker](#) oder [Sebastian Dienst](#)

Practice Group: [Datenschutz](#)

Contact Person



Dr. Daniel Rücker, LL.M.

Leiter Datenschutz

Mitglied der Practice Group Digital Business

Rechtsanwalt

T +49 89 28628457



Sebastian Dienst

Mitglied der Practice Group Datenschutz

Mitglied der Practice Group Digital Business

Rechtsanwalt

T +49 89 28628457