

Datenschutz – Bußgeld in Höhe von 475.000 Euro wegen verspäteter Meldung eines Datenschutzvorfalls

Bußgeld in Höhe von 475.000 Euro wegen verspäteter Meldung eines Datenschutzvorfalls

Die niederländische Datenschutzbehörde (Autoriteit Persoonsgegevens – AP) hat gegen die Übernachtungs- und Reisevermittlungsplattform booking.com ein Bußgeld von 475.000 Euro verhängt, weil diese einen Datenschutzvorfall nicht rechtzeitig gemeldet hatte.

Bereits im Jahr 2019 war es Hackern gelungen auf die Daten von 4109 Kunden von booking.com (https://edpb.europa.eu/news/national-news/2021/dutch-dpa-fines-bookingcom-delay-reporting-data-breach_en) zuzugreifen. Bei den Daten handelte es sich neben Namen, Adressen, Telefonnummern und Details zu Hotelbuchungen auch um Kreditkarteninformationen von 283 Betroffenen, in 97 Fällen einschließlich der Sicherheitsnummern. Zugang zu den Daten erhielten die Hacker über Mitarbeiterkonten mehrerer Hotels in den Vereinigten Arabischen Emiraten, vermutlich durch „socialengineering“-Techniken oder Phishing. Darüber hinaus versuchten die Hacker Zugriff auf weitere Kreditkartendaten zu erlangen, indem sie Gäste der Hotels per E-Mail oder Telefon kontaktierten. Hierdurch bestand auch für diejenigen Kunden von booking.com, deren Kreditkartendaten nicht betroffen waren, ein hohes Sicherheitsrisiko.

booking.com sah sich nicht in der Verantwortung für den Datenschutzvorfall, da die Daten nicht über die eigene IT-Infrastruktur abgegriffen worden seien. Die AP sah hingegen Hinweise auf eine Mitverantwortung des Betreibers. Das Bußgeld erging jedoch unabhängig von dieser Frage allein auf Grund der Tatsache, dass booking.com den Datenschutzvorfall erst nach 22 Tagen den betroffenen Kunden und erst nach 25 Tagen der Aufsichtsbehörde gemeldet hatte. Eine Datenpanne dieses Ausmaßes hätte der Datenschutzbehörde gemäß Art.33 Abs.1 DSGVO spätestens binnen 72 Stunden nach Bekanntwerden bei booking.com gemeldet werden müssen.

Gegen das Bußgeld kann noch Widerspruch eingelegt werden. booking.com hat jedoch bereits erklären lassen, das Bußgeld zu akzeptieren. Die booking.com-Datenbank sei zu keinem Zeitpunkt kompromittiert worden, man wolle aber an einer Verbesserung der internen Prozesse arbeiten.

Bemerkenswert an dieser Bußgeldentscheidung ist, dass der eigentliche Vorfall nicht sanktioniert wurde. Vielmehr wurde allein die verspätete Meldung bestraft. Dies belegt, dass die Aufsichtsbehörden eben nicht nur die Maßnahmen zur Verhinderung von Datenschutzvorfällen prüfen und sanktionieren. Auch die verspätete Meldung von Vorfällen an die Aufsichtsbehörden und/oder die Betroffenen stellt einen eigenen und sanktionierungsfähigen Verstoß dar.

Verantwortliche sind daher gut beraten, ihre internen Prozesse zur Meldung von Datenschutzvorfällen zu überprüfen und sicherzustellen, dass eine erforderliche Meldung rechtzeitig erfolgen kann. Dabei ist insbesondere zu berücksichtigen, dass es sich bei der Frist von 72 Stunden um eine Maximalfrist handelt und diese – jedenfalls

nach Auffassung der deutschen Aufsichtsbehörden – auch am Wochenende oder an Feiertagen läuft. Vor dem Hintergrund der üblicherweise erforderlichen Sachverhaltsermittlungen im Unternehmen müssen hierfür entsprechende organisatorische Vorkehrungen getroffen werden.

Ansprechpartner:

Sebastian Hoegl, LL.M. (Wellington)

Tel: +49 761 769999-20

shoegl@kpmg-law.com