



Information Commissioners Office (UK) kündigt DSGVO-Geldstrafe in Höhe von £ 99 Mio gegen Hotelkette Marriott an

Ein Cyber-Vorfall, bei dem Daten von 339 Mio Betroffenen offengelegt wurde, führt zur Ankündigung einer hohen Geldstrafe

Bereits am [30.11.2018](#) hat ein Vertreter des ICO erklärt, dass die Aufsichtsbehörde von Marriott Hotels eine **Datenschutz-Vorfallmeldung** erhalten hatte, die die Starwood Hotels betroffen hat.

Es wurden **Ermittlungen** eingeleitet.

Die Behörde riet den betroffenen Personen wachsam zu sein, den Empfehlungen des ICO und des National Cyber Security Center zu folgen, um sich und ihre Daten schützen zu können.

Am [9. Juli 2019](#) hat das ICO bekannt gegeben, dass es beabsichtigt, eine **Geldstrafe in Höhe von £ 99.200.396,--** (umgerechnet ca. 110 Mio Euro) zu verhängen.

Dies war die Folge einer (verpflichtenden) **Mitteilung von Marriott Hotels Inc.** selbst, die am selben Tag an die us-amerikanische Börsenaufsicht

(Securities and Exchange Commission, SEC) eine [Mitteilung](#) übermitteln musste. Es wurde bereits in dieser Mitteilung angekündigt, dass die Geldstrafe nicht akzeptiert werden würde.

Die Geldstrafe betrifft einen Cyber-Vorfall. Es wird vermutet, dass die **Systeme der Starwood-Hotel-Gruppe im Jahr 2014 kompromitiert** wurden. Eine Anzahl von rund **339 Mio Gästedatensätzen**, davon Datensätze von ca. 30 Mio Einwohnern aus dem Europäischen Wirtschaftsraum sind betroffen.

Die **Offenlegung der Kundendatensätze** wurde erst im Jahr 2018 entdeckt, nachdem Marriott die Starwood-Gruppe im Jahr 2016 erworben hat. Die Ermittlungen des ICO ergaben, dass Marriott im Rahmen der Akquisition den Sorgfaltspflichten nicht nachkam, und mehr hätte tun müssen, um die Systeme sicher zu gestalten.

Information Commissioner Elizabeth Denham sagte dazu:

“The GDPR makes it clear that organisations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected.

“Personal data has a real value so organisations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the public.”

„Die DSGVO macht deutlich, dass Organisationen für die personenbezogenen Daten, die sie verwahren, verantwortlich sind. Das inkludiert auch die Durchführung einer angemessenen Due-Diligence-Prüfung bei einem Unternehmenserwerb, sowie die Einführung angemessener Maßnahmen zur Rechenschaftspflicht, nicht nur um beurteilen zu können, welche personenbezogenen Daten erfasst wurden, sondern auch, wie sie geschützt sind.“

„Personenbezogene Daten haben einen echten Wert, daher sind Unternehmen gesetzlich verpflichtet, ihre Sicherheit zu gewährleisten, genau wie bei jedem anderen Vermögenswert. Wenn dies nicht der Fall ist, werden wir jederzeit entschlossen handeln, um die Rechte der Öffentlichkeit zu schützen.“

Marriott hat an der ICO-Untersuchung mitgearbeitet und die Sicherheitsmaßnahmen verbessert, seit diese Ereignisse bekannt wurden.

Das Unternehmen hat nun die Möglichkeit, sich gegenüber dem ICO zu den vorgeschlagenen Feststellungen und Sanktionen zu äußern.

Das **ICO** hat diesen Fall als **federführende Aufsichtsbehörde** im Auftrag anderer Datenschutzbehörden der EU-Mitgliedstaaten untersucht. Es hat auch mit anderen Aufsichtsbehörden zusammengearbeitet.

Nach den Bestimmungen der DSGVO über eine zentrale Anlaufstelle (one-stop-shop) haben die Datenschutzbehörden in der EU, deren Einwohner betroffen sind, auch die Möglichkeit, sich zu den Ergebnissen des ICO zu äußern.

Das ICO wird die Erklärungen des Unternehmens und der anderen betroffenen Datenschutzbehörden sorgfältig prüfen, bevor es seine endgültige Entscheidung trifft.

Die [Mitteilung des ICO](#) ist in englischer Sprache auf der Website veröffentlicht.