Lack of due diligence

Threat of € 110 million fine against Marriott International

Article by Dr. Carlo Piltz and Moritz zur Weihen

On 9 July 2019, following an extensive investigation, the UK supervisory authority ICO (Information Commissioner’s Office) announced that it intended to impose a fine of £99,200,396 on Marriott International for breaches of the General Data Protection Regulation (GDPR).

The proposed fine relates to an incident notified by Marriott to the ICO in November 2018. A large amount of personal data, contained in some 339 million guest records worldwide, was compromised by a data leak, encompassing some 30 million guests domiciled in 31 countries of the European Economic Area.

It is believed that the main data leak originated as early as 2014 with the compromise of the Starwood Hotel Group's systems. Marriott acquired Starwood in 2016, but the disclosure of customer information was not discovered until 2018. The ICO’s investigation revealed that Marriott had failed to exercise due diligence in its purchase of Starwood and should have done more to secure its systems.

According to the ICO, the GDPR makes it clear that companies are responsible for the personal data they store. This may include conducting due diligence on a business acquisition and introducing appropriate accountability measures to assess not only what personal data are being processed but also how and whether they are adequately protected in accordance with the legal requirements of the GDPR.

According to the ICO, Marriott did not exercise sufficient due diligence in the acquisition of the Starwood chain, which made the data breach possible in the first place. The security gaps that already existed when the company was acquired should therefore have been noted and subsequently eliminated in order to guarantee an adequate level of security. Buyer companies must therefore carry out an in-depth examination of technical systems with a view to the security of processing prior to acquiring a company in order to be able to preventively identify any weak points.
Marriott has been involved in the ICO investigation and has improved its security arrangements since these events became known. The company will now have the opportunity to comment to the ICO on the proposed findings and sanctions.

The ICO has investigated this case as the lead supervisory authority on behalf of the data protection authorities of other EU Member States. It has also cooperated with other regulatory authorities.

The threat of a fine shows that data protection has become an essential part of corporate compliance, the negligent handling of which can result in immense economic sanctions. Another noteworthy aspect of the ICO’s reasoning is that this view is apparently being applied retroactively, since the acquisition of the company being protested here was already completed in 2016, i.e. two years before the GDPR became applicable.

About us:
reuschlaw Legal Consultants advise companies active on a national and international scale in more than 30 countries in the areas of product liability, product safety law, recall management, insurance law, cybersecurity and data protection, compliance management and contract law.

Company contact: Marketing & Communications I T > +49 30 / 2332895 0 I E > marketing@reuschlaw.de