GDPR Key Enforcement Actions: Fine Imposed by UK's ICO for Insufficient Due Diligence in Business Acquisition and Romania's First GDPR sanction

TOPICS: Fines, Mergers and Acquisitions, Due Diligence, Data Breach, Data Minimization, GDPR, ICO, Romania, EU

ICO Fines Marriot International for insufficient due diligence in acquisition, which resulted in data breach caused by vulnerability in system of acquired company

The Information Commissioner Office (**"ICO"**), UK's Data Protection Authority, issued a notice of its intention to fine Marriott International £99,200,396 for infringements of the GDPR.

Following a cyber-incident notified to the ICO by Marriott in November 2018, investigations concluded that a variety of personal data contained in approximately 339 million guest records were exposed by the incident.

According to the notice, **the vulnerability started in the systems of Starwood hotels group, which was acquired by Marriott in 2016.** Although Starwood's system was compromised in 2014, **Marriott failed to undertake sufficient due diligence when it bought Starwood and did not do enough to check and secure its systems.**

The GDPR makes organizations accountable for the personal data they hold, **including those obtained as a result of mergers and acquisitions**. As such, according to the notice, organizations must treat data security as an asset and perform proper due diligence when making a corporate acquisition to assess not only what personal data has been acquired, but also how it is protected.

In a similar vein, the ICO also issued a notice of its intention to fine British Airways £183.39M, following a cyber-incident notified in September 2018.

In this case, an investigation concluded that personal data of approximately 500,000 customers were compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information.

Romania's Supervisory Authority issues its first GDPR fine against UNICREDIT S.A

Romania's National Supervisory Authority (**"ANSPDCP")** issued its first GDPR fine against UNICREDIT Bank S.A., following an indication that data concerning the personal identification number and the

address of the persons performing payments to the bank, via online transactions, were disclosed to the beneficiary of the transaction through the account statement/details.

According to the notice, **this is a result of the bank's failure to implement appropriate technical and organizational measures to comply with data protection principles**, such as data minimization, and to protect the rights of the data subjects.