PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

55

Landmark Fines against British Airways and Marriott for Data Breaches


Samantha V. Ettari,
Privacy Counsel, Special Counsel Litigation Department, Kramer Levin
Hélène Berion,
avocat aux barreaux de Paris et de New York, Kramer Levin, membre Club Alumni Master DEA

Le 30 octobre 2020, l'autorité de protection des données britannique en coopération avec la CNIL a infligé des amendes records à l'encontre de British Airways et Marriott suite à des violations de données. Ces deux sanctions illustrent l'efficacité de la coopération entre les autorités de protection des données via le mécanisme de guichet unique prévu par le règlement général sur la protection des données.

CNIL, communiqué, 2 nov. 2020

1. An Efficient Cooperation under the "One-Stop-Shop" Mechanism

A. - Context

On October 30, 2020, the United Kingdom's data protection authority ("DPA") the Information Commissioner's Office ("ICO"), in connection with France's *Commission nationale de l'informatique et des libertés* (the "CNIL"), announced the largest security fines, jointly imposed by the authorities under the General Data Protection Regulation (the "GDPR")[1], against British Airways ("BA") and Marriott International, Inc. ("Marriott"). The fines totaled more than €40M.

The fines follow investigations into well-known data security breaches in 2018. In the case of BA, the data hack involved approximately 430,000 individuals and included the unauthorized disclosure of their names and addresses, and, for more than 200,000 data subjects, their sensitive bank account information (including credit card numbers and CVV codes). With respect to Marriott, 339 million customer accounts were affected, including 30 million European accounts containing names, email addresses, phone numbers, passport numbers, arrival and departure information, VIP status, and loyalty program information. Considering that these organizations process very large amounts of personal data and benefit financially from that data, they are subject to high expectations from the data authorities.

B. - Cooperation between DPAs

These are ICO's first major fines under the GDPR. ICO worked with CNIL under the GDPR's "one-stop-shop" provision[2]. Pursuant to the "one-stop-shop" cooperation mechanism, provided for by the GDPR, ICO's draft decisions were sent to other European DPAs and carefully examined by the CNIL. This is a key process under the GDPR where the leading authority has to co-ordinate with and work along-side other regulatory bodies in countries affected by a breach. Findings and proposed fines are shared by the leading authority with the applicable regulatory bodies which review the proposed fines and hold discussions with the leading authority on the review process implemented before confirming the proposed fines or recommending revisions. The CNIL endorsed the final outcome before the decisions and fines were published by ICO. The companies are given an opportunity to argue, comment, and make written observations on proposed fines after being notified of the DPA's proposed fines.

1 Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("GDPR").

2 Article 60 of the GDPR.