Dramatic Developments with GDPR

Business Bulletin

As followers of multinational business know, the EU's General Data Protection Regulation (GDPR) went into effect in May 2018, with more questions than answers in the minds of many observers. High on many lists was the uncertainty as to how aggressively the applicable regulatory bodies would be in terms of actually imposing the potentially enormous fines that GDPR made possible (up to 4% of a company's revenue).

Following implementation of GDPR, activity by regulators predominantly included fines of relatively nominal amounts. That changed sharply this month with the imposition of two enormous fines, one against Marriott International and one against British Airways, each of which has unique and interesting circumstances and implications for companies of all sizes in the EU and worldwide.

British Airways was subject to a sophisticated hacking in September 2018 which compromised the personal data of approximately 500,000 customers. The regulator concluded that inadequate security measures allowed this to happen and announced a fine on July 8 of the equivalent of $230,000,000, which is the highest GDPR fine ever, more than four times larger than the previous record.

Marriott was fined $124,000,000 on July 9 for allegedly conducting insufficient due diligence in their acquisition of Starwood, whose customer loyalty program was breached, leading to the compromise of approximately 339,000,000 customer records.

Aside from the sheer size of these fines, which each of the companies says will be appealed, there are a number of other interesting aspects to these developments which corporate executives around the world will likely be interested to follow, such as:

- The regulator that issued both fines is the U.K.'s Information Commissioner's Office (ICO), which raised eyebrows because GDPR is an EU regulation, and the UK is in the messy process of Brexit-ing.
- Marriott is a US-based company and even though some of the records compromised were residents of the UK and elsewhere in the EU, some considered it a reach for the ICO to impose a fine of 2.5% of its worldwide revenue.
- Both breaches were self-reported by the companies involved and both are said to have been fully cooperative with the investigations by the ICO. Circumstances vary in each case of course, but a situation like this wouldn't often expect one to see such record-breaking enforcement action.
- The Starwood breach occurred before Marriott's acquisition of Starwood, perhaps underscoring how important and challenging due diligence for these emerging issues can be.

Simkiss & Block will continue to monitor these and other privacy issues and advise our clients accordingly, both in the context of what their cyber/privacy liability coverage can address and beyond the policy as well.