

Record GDPR fine for data breach: UK regulator has a bite as big as its bark

July 9, 2019

The UK privacy regulator, the ICO, has announced its intention to impose the largest fine to date under the GDPR. The announcement follows British Airways' failure to protect the personal data of 500,000 customers from malicious hackers.

The proposed fine of over £183 million (approximately NZ\$346 million) was announced yesterday, and will be issued under the GDPR and the UK Data Protection Act (the UK legislation that complements the GDPR). It represents approximately 1.5% of British Airways' worldwide revenue in 2017. The previous largest fine issued under the GDPR was a €50 million fine issued to Google by the French data protection watchdog in January this year.

British Airways had notified the ICO of a cyber incident in September 2018. Malware on British Airways' website led to the diversion of users to a fraudulent site. This diversion enabled malicious hackers to harvest customer details. The personal data of approximately 500,000 customers were compromised during the incident, which the ICO found to be the result of "poor security arrangements".

The fine has particular significance given that British Airways cooperated with the ICO investigation. The potential fine could have been even higher if British Airways had been less cooperative.

British Airways now has the opportunity to make written representations to the ICO in response to the ICO's notice of intent, before the ICO confirms the level of the fine by issuing a penalty notice. British Airways will also have the opportunity to appeal the fine after the penalty notice is issued, and it is expected to do so.

New Zealand Privacy Commissioner John Edwards described the proposed fine as "taking privacy seriously".

Although the "teeth" available to New Zealand's Privacy Commissioner are nowhere near as "sharp" as those of his UK counterpart, New Zealand-based organisations should know that:

- Some New Zealand organisations are subject to the GDPR, and it is hugely important that those organisations take their GDPR compliance seriously and get it right.
- If your organization deals with personal information, you must look after it: This means taking appropriate steps to protect your systems against cyber-crime – especially when the data is sensitive.
- As consumers grow increasingly aware of the value of their personal information, the reputational effect of damaged consumer trust from data breaches is likely to be of more consequence than the fine itself.

Your Key Contacts



Hayden Wilson

Partner, Wellington

D +64 4 915 0782

M +64 21 342 947

hayden.wilson@dentons.com



Hayley Miller

Partner, Auckland

D +64 9 915 3366

M +64 21 870 477

hayley.miller@dentons.com



Campbell Featherstone

Senior Associate, Wellington

D +64 44 98 0832

M +64 21 80 9779

campbell.featherstone@dentons.com