Goodmans LLP Update

Record Breaking Proposed Fines Against British Airways and Marriott International Under GDPR

The Information Commissioner's Office (ICO), the UK's independent authority on data privacy, issued notices of its intention to fine British Airways and Marriott International £183,390,000 and £99,200,396, respectively, for infringement of the EU *General Data Protection Regulations* (GDPR). The proposed fines arise from unrelated data breaches at the two companies. These fines are of interest to Canadian businesses both because some Canadians do business in the EU and in light of recent government indications that Canada may revise its privacy laws in a manner bringing them closer to GDPR.

The proposed fine against British Airways relates to a cyber incident beginning in June 2018. The personal data of approximately 500,000 customers was harvested by attackers as user traffic was diverted from the British Airways website to a fraudulent site. The ICO asserts that information such as log in details, payment cards, travel booking details, names and addresses were compromised as a result of poor security arrangements by British Airways.

The proposed fine against Marriott International relates to a cyber incident involving the exposure of the personal data contained in approximately 339 million guest records globally. The vulnerability is believed to have begun within the systems of the Starwood Hotels Group in 2014, which was subsequently acquired by Marriott International in 2016. The exposure was not discovered until 2018. The ICO asserts that Marriott International failed to undertake sufficient due diligence for the 2016 purchase, and failed to ensure proper security of its systems.

British Airways and Marriott International will have the opportunity to make representations to the ICO regarding the ICO's findings and these proposed large fines.

The EU General Data Protection Regulations

GDPR, which came into effect in May 2018, is directed at protecting the security of, and providing greater control for, personal information collected by organizations. The regulations apply to any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier (e.g., name, IP address). The regulations impose significant accountability obligations on both data controllers (the entity determining how data is collected and used by the organization) and processors (third parties engaged in processing personal data for controllers).

Under the regime, organizations engaged in serious breaches of the GDPR can be fined up to 4% of annual global turnover or €20,000,000, whichever is greater. Less significant infringements, such as not notifying the supervising authority and data subject about a breach, or failing to conduct an impact assessment, can result in lesser fines.

Why This Matters to Canadian Businesses

GDPR can apply to Canadian businesses that conduct business in the EU. This does not just mean having physical offices in the EU but includes offering goods and services to individuals in the EU through websites or mobile apps. In some circumstances, collecting personal information about individuals in the EU can also engage GDPR. In light of the large fines that can potentially be levied, businesses that collect personal information about individuals in the EU should seek professional advice.

Authors

Daniel Cohen
dcohen@goodmans.ca
416.597.5494

Kirby Cohen
kcohen@goodmans.ca
416.849.6912

Peter Ruby
pruby@goodmans.ca
416.597.4184

Canada's own privacy regime may also be headed toward a more GDPR-like approach. The Privacy Commissioner of Canada has recently taken aggressive actions based on a potential interpretation of Canadian legislation that incorporates concepts found in the GDPR, such as recently making a reference to the Federal Court of Canada seeking a ruling about whether Canadian law includes a GDPR-type "right to be forgotten". The Government of Canada has also announced a *Digital Charter*, that appears to foreshadow an evolution of Canadian privacy law toward a GDPR-like system. Canadian businesses should ensure not only that they have the safeguards to comply with current law but also the ability to adapt to future requirements.

Should you wish to discuss privacy issues relating to your business, please contact the authors or any member of our Litigation Group.