SAXE DOERNBERGER & VITA, P.C.

Nov. 2018

The Alphabet Soup of International Data Privacy Rules Thickens – PIPEDA Regulations Took Effect in Canada on Nov. 1 and They May Affect You

Stella Szantova Giordano and Anastasiya Collins*

Just as the businesses in the US were becoming familiar with the EU General Data Protection Regulation ("GDPR") and realizing it may apply to them, Canada came out with its own data privacy regulations under the Personal Information Protection and Electronic Document Act ("PIPEDA"). While PIPEDA has been in place since 2000, the amendments and corresponding regulations make mandatory reporting and keeping records of data privacy breaches as of November 1. These regulations impose financial penalties of up to CAD$100,000 and apply to US-based businesses with certain commercial ties to Canada.

The PIPEDA regulations have many similarities with the GDPR (which we previously wrote about here) and were directly influenced by the sweeping European regulation. As noted by the Canadian government, the new PIPEDA amendments were created with the goal of aligning and harmonizing Canadian regulations with the breach reporting requirements of the GDPR to allow for the "free flow of personal information" between the EU and Canadian organizations.

Foreign businesses, including those in the United States, should be wary of these changes due to PIPEDA's broad extra-territorial reach. Its breach notification requirements apply to every private-sector foreign organization with a real and substantial connection to Canada that collects, uses or discloses personal information in the course of its commercial activities. Unlike the GDPR, there is no limitation on the size of the business governed by PIPEDA, which means that a relatively small US business which markets goods or services to Canadian customers could be subject to the regulation.

Breach Reporting and Notification Requirements Under New PIPEDA Regulations

Starting November 1, 2018, businesses are required to both report to the Office of the Privacy Commissioner of Canada and to notify affected individuals of "a breach of security safeguards" involving compromised personal information[1] under their supervision if it is reasonable to believe that the breach creates a "real risk of significant harm" to affected individuals. Additionally, businesses may need to notify government institutions or other organizations if the risk of harm to affected individuals could be reduced or mitigated by doing so. "Significant harm" is defined as, among other things, humiliation, damage to reputation or relationships, damage to or loss of property, financial loss, and identity theft. The regulations also take into account the sensitivity of the information and the probability that it may be misused in determining the real risk of harm.

PIPEDA also outlines specific reporting provisions as to the form and content of mandatory notices, which differ depending on the recipient: the Commissioner, an affected individual, or a government institution. The regulations do not state a specific period of time when one must provide notification, only that the required notice must be sent "as soon as feasible" after an organization determines that a breach has occurred. While this is not as stringent as the 72-hour rule under the GDPR, its vagueness does not give businesses the necessary guidance in how swiftly they must react in the event of a breach. The sanctions for failure to report a breach involving personal information are twofold: if a business fails to notify the federal Privacy Commissioner of a breach, it is subject to a fine of up to CAD$100,000. If a business fails to notify the affected individuals, it may be ordered to pay damages to such individuals.

[1] PIPEDA's definition of "personal information" is broad and somewhat vague, including factual or subjective information about an identifiable individual. These encompass the more traditional categories such as name, age, ID numbers, income, but also more unusual ones such as the existence of a consumer-merchant dispute or intention to change jobs. There is some overlap with the definition of "personal data" under the GDPR, but the definitions are different enough that, in the event of a breach, a separate analysis as to whether protected data has been lost/compromised should be conducted to determine whether the notice obligation pursuant to either or both regulations has been triggered.

Mandatory Record-Keeping Provisions

In addition to the reporting and notification requirement, PIPEDA obligates organizations to create and maintain records of all privacy breaches for two years from the time a breach was discovered, regardless of whether the notification requirement was triggered. Upon request, the organizations will be obligated to provide such records to the Commissioner, who can investigate the breach and/or publicize it.

Organizations should take this new record-keeping provision seriously, particularly in light of the financial penalties for non-compliance. Furthermore, careful record-keeping may become a useful risk management tool – for example, should a company's data breach be made public by the Commissioner, prospective cyber insurers may access this information, which could cause an increase in insurance premium rates.

Recommendations for Businesses in the United States

The new PIPEDA regulations should be carefully reviewed by US-based private-sector businesses who have commercial contacts with Canada (whether through marketing or direct business relations). They should familiarize themselves with the PIPEDA notice and reporting requirements so that they are prepared to issue the requisite notices in the event of a breach. Additionally, they should discuss with their broker and/or coverage counsel whether the company's cyber insurance policy covers any PIPEDA-related liabilities and expenses.

If you have any questions about the above or any other international insurance topics, please contact Stella Szantova Giordano at ssg@sdvlaw.com.

*Anastasiya Collins is a law clerk at Saxe Doernberger & Vita, P.C.