Frankfurt Kurnit Klein + Selz PC

Focus on the Data

Unique Insights and Practical Guidance on Privacy and Data Security Issues Worldwide

PIPEDA Data Breach Reporting is in Effect

By Lyric Kaplan on November 12, 2018

While new EU breach notification requirements have received significant media attention, closer to home are the **data breach reporting obligations** under Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), which took effect on November 1. PIPEDA is a Canadian federal privacy law that broadly governs the collection, maintenance, use and disclosure of Canadian citizens' personal information during commercial activities. Unlike U.S. privacy laws currently in effect that form a regulatory patchwork of sectoral and industry-specific laws, PIPEDA follows an omnibus approach.

On June 18, 2015, Canada passed various amendments to PIPEDA, including the Digital Privacy Act. Most of the changes were simultaneously effective. However, the mandatory data breach reporting and its related reporting requirements just came into full force on November 1, 2018. Many U.S. companies are not aware that PIPEDA may apply to them.

Does PIPEDA apply?

The law may apply to U.S. based organizations that collect, use or disclose the personal information of Canadian citizens during commercial activities. For example, if a California company is collecting personal information from Canadian consumers (whether in its own capacity or as a service provider to another business), it should seek advice from privacy counsel regarding PIPEDA

applicability and compliance. If PIPEDA applies and the California company fails to comply with the new requirements, Canada's Office of the Privacy Commissioner (OPC) may have the right to investigate. Publication of adverse findings can cause substantial damage to reputation. Non-compliance may also subject the company to Canadian Federal Court jurisdiction and damages or fines up to $100,000 CAD.

Data Breach Reporting Requirements.

PIPEDA requires organizations to give affected individuals and the OPC notice of data breaches. Under Section 10.1 of PIPEDA, organizations must notify when the breach creates a "real risk of significant harm to the individual." To determine whether there is a "real risk," various factors must be considered, including the sensitivity of the information and the likelihood of misuse. "Significant harm" can include identity theft, damage to reputation, and humiliation.

After a breach, notice must be given "as soon as feasible." This uniform national standard is similar to GDPR's "without undue delay" standard but different from GDPR's 72 hour requirement. Both PIPEDA and the GDPR are somewhat different from the U.S., where data breach notification varies from state to state, and many are in as expedient a manner as possible, but occasionally with a 30 or 45 day outer limit. Companies subject to the Health Insurance Portability and Accountability Act (HIPAA) must provide notices within 60 days. Also, some companies may be subject to different time requirements for notice based on their contracts with business partners from whom they receive personal information of individuals. These distinct standards create challenging risk decisions for companies that need to comply with many data breach notification obligations.

Klein+Selz