Client Alert: Canadian Privacy Commissioner Releases Data Breach Notification Guidance

Related Professionals

John L. Landolfi

Christopher L. Ingram

Christopher A. LaRocco

Related Services

Data Strategy, Privacy and Security

Litigation and Appeals

CLIENT ALERT | 10.31.2018

Canada's new mandatory breach-notification requirements in the Personal Information Protection and Electronic Documents Act (PIPEDA) take effect on November 1, 2018. Earlier this week, the Canadian Privacy Commissioner released guidance that provides an overview of what companies should know about PIPEDA's new requirements to (1) report certain breaches to the Privacy Commissioner, (2) notify affected individuals, and (3) keep records of all breaches for at least two years. While the text of PIPEDA is silent as to its geographical reach, case law suggests that companies who collect, use, or disclose Canadian residents' personal information in connection with commercial activities will be subject to the law's requirements.

Under the new guidance, companies must notify the Canadian Privacy Commissioner and affected individuals "as soon as feasible" about incidents that pose "a real risk of significant harm" to affected individuals. "Significant harm" is defined as "bodily harm, humiliation, damages to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property." Under the guidance, the sensitivity of the information involved and the probability that information will be misused are key factors for companies' consideration of whether notification is required.

Companies must also keep detailed records of any breach for two years and ensure that their third-party partners are following PIPEDA's rules. The guidance offers some insights into circumstances where a company collects personal information and shares that information with a third-party. Typically, the company that originally collects or obtains the personal information will ultimately be held responsible for compliance with the breach notification and record keeping requirements, even where the third-party is breached while processing the information for the company. However, the guidance also notes that these scenarios should be assessed on a case-by-case basis. For example, where a company provides personal information to a third-party processor and the processor uses or discloses that same personal information in a manner that is beyond the scope of processing for the

original company, the third-party processor may then be the responsible entity. Companies should therefore ensure that their contracts with third-party data processors address these new obligations and clarify the scope of use of personal information collected during the relationship.

Non-compliance with the new rules leads to staggering penalties: up to C$100,000 ($79,139) per day for each individual who should have been notified of the breach. The Privacy Commissioner also suggested that the new requirements should include financial sanctions for having inadequate data security safeguards in place to begin with, instead of just for failing to report breaches after they occur.

Ensuring your incident response plan reflects recent changes in the law is vital to protecting your company in the event of a suspected cyberattack or security breach. In addition to working with you to update your incident response plan, Vorys also offers tabletop trainings aimed at preparing incident response team members to execute your incident response plan. We also routinely advise companies on best practices for privacy and cybersecurity considerations in third-party agreements. For any questions on the new Canadian breach rules, data privacy, vendor management, or cybersecurity programs, please contact John Landolfi, Chris Ingram, Chris LaRocco, or your Vorys attorney.