Canada's New Data Breach Disclosure Rules

By Nicholas R. Merker and Martha Kohlstrand

This article was originally published by Ice Miller, LLP on March 7, 2019.

Mandatory data breach disclosure rules took effect in Canada on November 1, 2018, adding new breach notification requirements to the Personal Information and Electronic Documents Act (PIPEDA)[1]. All businesses that operate in Canada and handle personal information which crosses either national or provincial borders must adhere to PIPEDA, whether or not they are based in Canada. This even includes businesses that have no operations in Canada whatsoever, so long as they collect the personal information of Canadian citizens.

PIPEDA contains three requirements related to breach notification: first, the organization must keep records of all data breaches[2]; second, the organization must provide written notice to the Office of the Privacy Commissioner if the breach reasonably creates a real risk of significant harm to an individual.; and third, organizations must notify the subjected individuals if it is reasonable to believe that the breach poses a real risk of significant harm. There are additional requirements laying out exactly what the notices must contained and how long records of the breach must be kept. Penalties under PIPEDA can reach $100,000 for each time an individual is affected by the breach.

Given these new regulations, companies doing business in Canada should review their privacy policies and data breach response plans to ensure compliance. Companies should also stay abreast of privacy developments in Canada. For instance, Canadian privacy advocates are calling for even stricter data security regulations. Canadian Privacy Commissioner Daniel Therrien has criticized current laws, saying new marketing techniques powered by big data are raising ethical questions about data privacy.

To remedy these issues, Therrien advocates giving his office more enforcement powers and extending privacy regulations to political parties, which are currently exempt from the strictures of PIPEDA. He says the new data breach disclosure rules mean little in the light of the poor funding for his office and the lack of time to investigate and review breaches. Rather, he wants a sweeping new law, reflecting the principles of Privacy by Design drafted by former Ontario Privacy Commissioner Ann Cavoukian. As yet, the only new requirements on the horizon to the North are the data breach disclosure rules – but stay tuned for wider-reaching laws in the future.

For more information, contact Nick Merker, Martha Kohlstrand or another member of our Data Security and Privacy Group.

This publication is intended for general information purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstances.

About the Authors

Nicholas R. Merker is a partner and co-chair of Data Security and Privacy Practice at Ice Miller Strategies LLC. He can be reached at nicholas.merker@icemiller.com.

Martha Kohlstrand is an associate in the Litigation and Data Security and Privacy Groups at Ice Miller Strategies LLC. She can be reached at martha.kohlstrand@icemiller.com.

1. S.C. 2000, c. 5 (Nov. 1, 2018)
2. Loss of personal information that can be linked to an individual, such as age, name, ID numbers, income, ethnic origin, blood type, evaluations, comments, social status.