November 2018

PIPEDA

New mandatory data breach reporting requirements

The new mandatory data breach reporting provisions enacted under the **Personal Information Protection and Electronic Documents Act (PIPEDA)** came into force on 1 November 2018, setting out the rules and requirements that may apply in the event of loss, unauthorized access or unauthorized disclosure of personal information (breach of security safeguards) affecting personal identifiable information (PII).

Organizations that experience breach of security safeguards involving PII which result in a "real risk of significant harm" to affected individuals will be required to notify both the individual(s) whose PII was compromised and the Privacy Commissioner of Canada. A record of the breach will also have to be maintained for 24 months after the day on which the organization determines that the breach occurred. Failure to report a privacy breach in compliance with PIPEDA is punishable by a fine of up to CAD $100,000, in addition to the consequential reputational damage that the disclosure process can create.

Privacy law in Canada

PIPEDA applies to the collection, use and disclosure of personal information by private sector organizations in the course of commercial activity in Canada, except where a province has enacted privacy legislation deemed substantially similar to PIPEDA (currently Quebec, British Columbia and Alberta; with regard to personal health information specifically, Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have enacted legislation substantially similar to PIPEDA).

It is important to note that PIPEDA, along with the mandatory breach notification requirements contained therein, does not apply to personal information of employees, with the exception of federally regulated businesses (such as banks, airlines, telecommunications companies and other organizations engaged in federal works, undertakings or businesses).

AON
Empower Results®

Employee benefit plan information

Employee benefit plan information held by an employer could be viewed as employment related information to which PIPEDA may not apply, except in regard to federally regulated employers.

Provinces may have privacy legislation in force that applies to employee information, including benefit plan related information. Employee privacy in private sector organizations that operate within Quebec, Alberta and British Columbia are governed by provincial privacy legislation, with Alberta being the only province to have mandatory breach reporting requirements.

While the privacy legislation in B.C. and Quebec has been deemed "substantially similar" to PIPEDA, these provincial statutes contain no formal data breach reporting provisions. However, it is widely considered a best practice for organizations operating within those provinces to disclose breaches of data security and voluntary notification to affected individuals may be a beneficial step in mitigating potential liability. It remains to be seen whether legislative amendments will follow to crystalize current best practices into formal legal requirements.

If PII related to a benefit plan is transferred to a third-party, including an insurer, PIPEDA, and its mandatory breach notification regime, may then apply at least where no substantially similar legislation has been enacted. The party responsible for meeting any necessary notification and reporting obligations may depend on the particulars of the situation, effective control of the information and applicable contractual provisions.

Security breaches of employee PII pose liability concerns for employers, more so now than ever. First-party breach response and notification costs can escalate quickly when the volume of records compromised in a single incident is high.

To reduce risk related to personal information, an organization should implement suitable data management and protection practices and policies, enact compliant incident response plans, review applicable third-party agreements, educate their employees on data protection and may also wish to consider cyber risk insurance coverage.