Privacy Primer: 5 Things Businesses Need to Do Now to Comply with PIPEDA

Introduction

Uber. Equifax. Yahoo. Hardly a month went by in 2017 without news of yet another major privacy breach at a multi-national corporation. Sensitive personal information of an estimated one billion-plus customers landed in the hands of hackers, subjecting those customers to potentially serious consequences, including identity theft. Although investigations into the breaches continue, the damage is already done: customers have lost their trust, corporate reputations suffered a black eye and some organizations may face criminal charges.

If you think data breaches befall only large companies, think again. The reality is no company is immune to the mishandling of customer personal information – whether that vulnerability comes from external threats like cybercriminals or from human error within the company's own walls. It is likely not a matter of *if* it will happen to your business, but *when*.

To prevent your business from becoming the latest headline and subject to the scrutiny of government regulators, become informed about the privacy legislation that governs the conduct of Ontario businesses, how to comply with it and a significant legislative change that is around the corner.

Legislative Framework

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is a federal law that establishes rules for how businesses collect, use or disclose personal information in the course of their commercial activities. It also provides standards that businesses must meet to safeguard personal information. PIPEDA currently applies to private-sector businesses in Ontario.

In 2015, the federal government amended PIPEDA. The changes require businesses to notify individuals of a breach involving their personal information and to report the breach to the Office of the Privacy Commissioner of Canada (OPC). While these mandatory breach reporting requirements are set out in PIPEDA, they won't come into force until the government passes regulations with details of the reporting requirements. This past fall, the government released draft breach reporting regulations for a 30-day public comment period.

Proposed Corporate Obligations under the Draft Regulations

The draft federal regulations include requirements that a business must:

(a) report to the OPC any breach of security safeguards involving personal information under its control if the breach creates a real risk of significant harm to an individual;
(b) notify individuals of loss of, unauthorized access to or unauthorized disclosure of their personal information if the breach creates a real risk of significant harm to the individual;
(c) provide enough details in the notice to the individual to allow the individual to understand the significance of the breach and what steps they can take to reduce the risk of harm;
(d) notify any other organization, including a government institution, if the business believes that the organization or government institution may be able to reduce the risk of harm to the individual; and
(e) keep a record of the breach for a 24-month period after the breach occurred.

The content of both the report and notice are generally the same and must include, among other things, the circumstances of the breach, when it occurred, the personal information exposed by the breach, what the business is doing to reduce the harm to the individual, and who can be contacted at the business for additional information.

The proposed regulations also require that the report to the OPC (which must be in writing), and notice to affected individuals (which need not be in writing and may be provided indirectly such as on a website), must occur as soon as possible after the breach is discovered.

While we await the finalized regulations, here is a checklist of what your business should do to be compliant now and in the future with PIPEDA. This checklist reflects best practices in accordance with the 10 privacy principles provided in Schedule 1 of PIPEDA.

5 Things You Can Do Now to Protect Your Business and Customers

1. Designate a Privacy Officer within your organization to be responsible for compliance with PIPEDA and who can respond to inquiries from customers.
2. Implement the following procedures to protect the personal information of your customers while it is in your possession and when it is transferred to third parties for processing:
   - Explain to customers what personal information you are collecting and for what purpose.
   - Obtain consent at the time of collection; the customer must understand what he/she is consenting to. Consent can be written or oral, but keep proof of the consent.
   - Do not require the collection of personal information as a condition of providing the service.
   - Do not collect more personal information than you need. Limit it to only what you need in order to provide the service.
   - Do not use personal information for purposes other than what it was collected for. If you want to use the personal information for another purpose, get consent.
   - Make sure the personal information you collect is accurate and complete.
   - Do not retain personal information indefinitely; once the information has served its purpose it should be destroyed, erased, or made anonymous.
   - Implement appropriate safeguards in accordance with the sensitivity of the personal information. This can include physical safeguards such as storing the information in locked cabinets with limited access, or can include technological safeguards such as encrypting the information or making it accessible via use of passwords.
3. Educate your employees about your organization's procedures and the importance of protecting personal information.
4. Upon request, give individuals access to their personal information.
5. Implement procedures to deal with a breach. Ensure they include:
   - Immediate steps to take in order to contain the breach.
   - A process to notify those individuals whose personal information was the subject of the breach. The notice must include the steps you are taking to contain it, your complaint procedure and their right to make a complaint to the OPC.
   - Assigning an internal team responsible for investigating the breach.
   - An assessment of procedures to ensure they are reasonably sufficient to prevent further breaches.
   - A process to document details of the breach. Retain these records for at least 2 years after the breach is identified.

Pallett Valo Privacy Law Practice

Privacy and data protection are very important considerations for both private and public sector organizations. At Pallett Valo LLP, our Privacy Law Group advises and supports private sector organizations to comply with their obligations under both federal and provincial laws including the: *Personal Information Protection and Electronic Documents Act* (PIPEDA), *Personal Health Information Protection Act, Freedom of Information and Protection of Privacy Act, Municipal Freedom of Information and Protection of Privacy Act, Canada's Anti-Spam Legislation* (CASL) and the *Digital Privacy Act*. We assist our clients in developing privacy policies and practices to meet strategic business needs and to ensure compliance with privacy legislation.

Contact Members of our Privacy Law Practice:

Andy Balaura
abalaura@pallettvalo.com • (905) 273.3022 ext. 225

Joe Conte
jconte@pallettvalo.com • (905) 273.3022 ext. 217

Nishi Malik
nmalik@pallettvalo.com • (905) 273.3022 ext. 315

PALLETT VALO LLP
Lawyers & Trade-Mark Agents

77 City Centre Drive, West Tower, Suite 300, Mississauga, Ontario L5B 1M5 • 1.800.323.3781