COMPLIANCE BULLETIN

HIGHLIGHTS

- Starting Nov. 1, 2018, Canada's federal PIPEDA will require organizations that suffer a data breach involving personal information to:
  - Report the breach to the OPC.
  - Give notice of the breach to affected individuals.
  - Maintain records of data breaches that affect personal information.
- In order to avoid fines and penalties, organizations will need to understand the basic requirements of PIPEDA. To help organizations better understand their obligations, the OPC recently published final guidance on the law.

Privacy Commissioner's Final Guidelines on Mandatory Breach Reporting

OVERVIEW

Starting Nov. 1, 2018, Canada's federal Personal Information Protection and Electronic Documents Act (PIPEDA) will require organizations that suffer a data breach involving personal information to:

1. Report the breach to the Office of the Privacy Commissioner of Canada (OPC).
2. Give notice of the breach to affected individuals.
3. Maintain records of data breaches that affect personal information.

To help organizations better understand their obligations, the OPC recently published final guidance on the law. This Compliance Bulletin provides a general overview of this guidance.

UPDATED GUIDANCE FROM THE OPC

The main component of PIPEDA relates to data breach reporting. When an organization suffers a **breach of security safeguards** involving personal information **under its control** and there's reason to believe that the breach creates a **real risk of significant harm** to an individual, the organization must report the breach.

In its final guidance, the OPC clarified a number of concepts to help organizations better understand this requirement and what's expected of them.

- **Breach of security safeguards**—PIPEDA broadly defines a breach of security safeguards as "the loss of, unauthorized access to or disclosure of personal information resulting from a breach of an organization's security safeguards or from a failure to establish those safeguards." Per the OPC, security safeguards include physical, organizational and technological measures designed to protect against the loss, theft and unauthorized access, disclosure, copying, use or modification of personal information.
- **Personal information under the control of an organization**—Under PIPEDA, the obligation to report a hack rests with the organization that controls the personal information implicated in the breach itself. PIPEDA does not explicitly define what it means by "control." However, PIPEDA's accountability principle states that an organization remains responsible for personal information even if it has transferred it to a third party for processing. As such, in the event that a third party is breached, the organization originally in control of the information would have to submit a report to the OPC and affected individuals. As a result, organizations need to ensure their third-party contracts address PIPEDA compliance and state who is responsible for reporting a breach should one occur.
- **Reporting breaches and significant harm**—Not every breach needs to be reported to the OPC—just the ones that create a real risk of significant harm. The guidance from the OPC clarifies significant harm to include bodily harm, humiliation, damage to reputations or relationships, loss of employment, loss of business or professional opportunities, financial loss, identity theft, negative effects on credit records, and damage to or loss of property. In its guidance, the OPC noted that, even if just one record is compromised in a breach, it must still be reported if significant harm exists. When determining whether a breach of security safeguards creates a real risk of significant harm, organizations must consider the sensitivity of the personal information involved and the probability that the personal information has been, is or will be misused. Failure to report a breach could result in a fine as high as $100,000.
- **The format of breach reports**—In its guidance, the OPC provides a model form organizations are encouraged to use to report a breach. The OPC also clarified that information can be added to reports that have already been submitted. Organizations must submit these reports as soon as feasible and, at a minimum, must specify the following:
    - The date or estimated date of the breach
    - A general description of the circumstances of the breach
    - The nature of information involved in the breach
    - Whether or not the breach was reported to the OPC and the affected individuals

LEARN MORE ABOUT PIPEDA

This Compliance Bulletin, as well as the guidance provided by the OPC, does not cover every obligation detailed in PIPEDA. Now that mandatory data breach reporting is required, organizations must have a thorough understanding of their obligations. To learn more about PIPEDA, organizations can visit the OPC's website.

Additionally, Henderson Insurance Inc. can provide you with a general guide on PIPEDA, which goes into more depth on the law and its requirements.