Insurance Brokers Association of Alberta
iboa
strengthening insurance brokers.

PIPEDA Privacy Breach Notifications, Effective November 1, 2018

PIPEDA regulations regarding notification for breaches of personal information will come into force on **November 1, 2018**. The Office of the Privacy Commissioner of Canada (and likely others) will need to be notified if a breach of security safeguards or a failure to establish those safeguards occurs. PIPEDA regulations and requirements for breach reporting are substantially similar to those in Alberta's Personal Information Protection Act (PIPA). They also update PIPEDA to establish greater consistency with the privacy regulations in the European Union.

The specific privacy regulations that apply (e.g., inter-provincial, Canadian, American, or European) pertain to the jurisdiction where the client lives or could be multi-jurisdictional (e.g., a French citizen living in Canada). PIPEDA applies to all inter-provincial, federally regulated, and international organizations.

Ensure you know and are prepared for the upcoming regulations, and train and monitor all employees on recording and security measures, office procedures for personal information, and the 10 PIPEDA privacy principles. You may want to review your cyber coverage, security, and automated record keeping.

Brokers who share personal information with commercial clients must both report any breaches of personal-information safeguards. Brokers should ensure their commercial clients are aware of these requirements and have appropriate security measures and cyber coverage in place.

A privacy officer should be appointed to manage the organization's privacy measures and breach record keeping and notifications.

Personal Information

Case law sets precedents for a broad definition of "personal information" that can be used alone or in combination with other information to identify an individual. Personal information (data) could be just a name. Each case is decided on its own merits and depends on the sensitivity and the impact of the information released, including the probability that the personal information has been, is being, or will be misused. Sources of personal information could include paper records, call recordings, social media, digital media, and hackable information such as shared files and document transfers, among other sources.

Business Contact Information

While an employee's business contact information does not constitute personal information when used to facilitate the business, business email addresses and other contact information used outside of that context do, as do all messages. Work cell-phone records may constitute personal information.

Record Keeping for Breaches Posing a "Real Risk of Significant Harm"

Organizations must keep a record of all breaches to "security safeguards" (data breaches or failure of security measures) that pose a "real risk of significant harm" to individuals. These records should document all thought processes, work that has been done since the breach was discovered, a risk-of-harm analysis, and a legal analysis. Records of each breach must be kept for at least 24 months after the breach was determined to occur. "Significant harm" includes bodily injury, personal injury, loss of employment or business professional opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property, among other types of harm. Each case will be assessed on its own merits.

Breach Reporting and Notifications

Reporting and notification is required as soon as feasibly possible after an organization determines a breach has occurred. The Office of the Privacy Commissioner of Canada must be notified, likely the individuals affected, and possibly relevant third parties.

Notifying the Privacy Commissioner

A breach report must be submitted in writing to the privacy commissioner through a secure manner to maintain confidentiality. It must include all the following details:

1. A description of the circumstances of the breach and, if known, the cause
2. The dates or the period during which the breach occurred and was discovered—if the occurrence date or period is not known, then the approximate period
3. A description of the personal information that was breached
4. The number of individuals affected by the breach—if unknown, then the approximate number—and type of individuals affected (e.g., customers, employees)
5. Action taken to contain the breach or to reduce risk or mitigate harm to those affected by the breach
6. Whether anyone has been notified of the incident (e.g., affected individuals, law enforcement, other) and when
7. The name and contact information of a person who can answer, on behalf of the organization, the commissioner's questions about the breach
8. The organization's business sector.

A Privacy Breach Incident Report Form can be downloaded from the Office of the Privacy Commissioner of Canada at https://www.priv.gc.ca/en/report-a-concern/report-a-privacy-breach-at-your-organization/report-a-privacy-breach-at-your-business/.

Legal experts suggest reporting all privacy breaches to the privacy commissioner, rather than having the regulator find out independently (and impose a $100,000 fine). Updates with further information are permitted. A small breach may not require notification to the individual affected by the breach, but should be documented and reported to the regulator who will decide who else needs notification and provide other guidance.

Notifying Affected Individuals

Individuals who have been affected by a breach that poses risk of significant harm need to be notified by direct or indirect methods, as appropriate to the circumstances. Notification must include sufficient information to allow the individual to understand the significance of the breach and to take any possible steps to reduce or mitigate the harm. All the following details should be included:

1. A description of the circumstances of the breach and, if known, the cause
2. The dates or the period during which the breach occurred and was discovered—if the occurrence date or period is not known, then the approximate period
3. A description of the personal information that was breached
4. A description of the steps that the organization has taken to reduce the risk of harm that could result from the breach
5. A description of the steps that the affected individual could take to reduce the risk of harm from the breach (e.g., contact the police, insurance, etc.)
6. Contact information that the affected individual can use to obtain further information about the breach.

The method of direct notification (e.g., mail, email, telephone, and in-person communication) should be what a reasonable person would consider appropriate in the circumstances.

Indirect communication (any means of public communication such as public announcements, advertisements, and notices that are likely to reach the affected individuals) is permitted in any of the following circumstances:

1. When direct notification may cause further harm to the affected individual
2. When the organization does not have contact information for the individual
3. When providing direct notification to all individuals within the required timeframe would result in undue hardship for the organization.

Notifying Other Organizations

Other organizations or government institutions need to be notified if they may be able to mitigate harm to the affected individuals (e.g., a credit-card issuing bank or a law enforcement agency). In Alberta, the provincial privacy commissioner determines whether such notification is required and which organizations to notify. The individual's consent for disclosure will not be required in such mitigation efforts.

Third-Party Breaches

The company that employs the third party will still be responsible for any breaches made by the third party (even if it is a shipping company). Some may arrange contracts that assume various levels of responsibility (e.g., payment for breaches), but the employing company may still be required to report the breach.

Commissioner's Powers

Where the privacy commissioner believes an organization has contravened or is about to contravene PIPEDA or a recommendation under the 10 PIPEDA principles (Schedule 1 of the Act), the commissioner may enter into agreements with the organization (guaranteeing that the organization undertake certain

actions to ensure compliance). These agreements preclude the commissioner from commencing or continuing court actions unless the organization fails to live up to the agreements.

Penalties

The cost of violating PIPEDA could be huge:

- Organizations that knowingly fail to maintain a record of these breaches or knowingly fail to report these breaches could face fines of up to $100,000 from the Office of the Privacy Commissioner of Canada
- Individuals subject to breach of privacy may launch a lawsuit
- Information on breaches will be public and may lead to class-action lawsuits
- Privacy breaches may damage a business's reputation.

Help with PIPEDA Compliance

Check out the Office of the Privacy Commissioner of Canada's PIPEDA Self-Assessment Tool (includes security, risk assessment, and procedures under the 10 PIPEDA principles).

PIPEDA Resources

- What You Need to Know About Mandatory Reporting of Breaches of Security Safeguards
- Privacy Breach Incident Report Form
- Office of the Privacy Commissioner homepage (with Frequently Asked Topics)
- Personal Information Protection and Electronic Documents Act (PIPEDA)