NOVEMBER 2017

CYBERSECURITY BULLETIN

Borden Ladner Gervais

Preparing for Compliance with Canadian Personal Information Security Breach Obligations

Canada's federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") will soon impose record-keeping, reporting and notification obligations on organizations that suffer a "breach of security safeguards" regarding personal information. The federal government has issued proposed regulations to provide some details regarding those obligations, but uncertainties and compliance challenges remain. Preparing for compliance with the personal information security breach obligations may require significant effort, time and expense, and the assistance of technical experts and legal advisors. Canadian organizations should now be taking steps to prepare for compliance.

PIPEDA

PIPEDA regulates the collection, use and disclosure of personal information in the course of commercial activities by private sector organizations in all provinces except British Columbia, Alberta and Québec (each of which has a substantially similar personal information protection law) and by all organizations that operate a "federal work, undertaking or business" (e.g. banks, telecommunications and transportation companies) or that transfer personal information across a provincial border for consideration.

PIPEDA includes obligations for record-keeping, reporting and notification regarding personal information security breaches, but those obligations are not in force because regulations prescribing required details have not yet been enacted. In September 2017, the Canadian government published for comment proposed *Breach of Security Safeguards Regulations*. Final regulations are expected soon, and the personal information security breach obligations are expected to come into force afterwards.

Breach of Security Safeguards – General Requirements

PIPEDA's record-keeping, reporting and notification obligations apply to a "breach of security safeguards", which is broadly defined as "the loss of, unauthorized access to or disclosure of personal information resulting from a breach of an organization's security safeguards [required by PIPEDA] or from a failure to establish those safeguards." The required security safeguards include physical, organizational and technological measures, appropriate to the sensitivity of the personal information, to protect the personal information (regardless of the format in which it is held) against loss, theft and unauthorized access, disclosure, copying, use or modification.

PIPEDA imposes the following obligations on an organization in respect of every breach of security safeguards involving personal information under the organization's control:

1. **Record-keeping:** The organization must create and maintain a record of the breach (even if there is no obligation to report or give notice of the breach), and provide the record to the Privacy Commissioner on request.
2. **Report to Commissioner:** If the breach creates a "real risk of significant harm to an individual", then the organization must report the breach to the Privacy Commissioner.
3. **Notification to Individual:** If the breach creates a "real risk of significant harm to an individual", then the organization must notify the individual of the breach, unless giving notice is otherwise prohibited by law. The notification must be conspicuous and contain sufficient information to allow the individual to understand the significance of the breach and to take steps, if possible, to reduce the risk of harm that could result from the breach or to mitigate that harm.
4. **Notification to Other Organizations/Government:** If the organization gives notice of the breach to an individual, then the organization must notify any other organization or government institution that may be able to reduce the risk of harm that could result from the breach or mitigate that harm.

PIPEDA broadly defines "significant harm" as including "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property". PIPEDA provides that the circumstances relevant to determining whether a breach of security safeguards creates a "real risk of significant harm" include: (a) the sensitivity of the personal information involved in the breach; (b) the probability that the personal information has been, is being or will be misused; and (c) other factors prescribed in regulations.

PIPEDA requires that reports and notifications of a breach of security safeguards be given as soon as feasible after the organization determines that the breach has occurred, and contain prescribed information and be given in the prescribed form and manner. PIPEDA provides that notifications to individuals must be given directly unless regulations permit indirect notification.

PIPEDA provides that an organization's knowing contravention of an obligation to report, notify or keep records of a breach of security safeguards is an offence punishable by a fine of up to $100,000.

Breach of Security Safeguards – Proposed Regulations

The proposed *Breach of Security Safeguards Regulations* provide some of the details contemplated by PIPEDA. Following is a summary:

1. **Record-keeping:** An organization must maintain a record of each breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred. The record must contain sufficient information pertaining to the breach to enable the Privacy Commissioner to verify the organization's compliance with breach reporting and notification obligations. If the organization submits a report regarding a breach of security safeguards to the Privacy Commissioner, then that report may be used as a record of the breach.
2. **Report to Commissioner:** A report to the Privacy Commissioner regarding a breach of security safeguards must be in writing and must contain: (a) specified information regarding the nature and extent of the breach; (b) a description of the steps the organization has taken or intends to take to notify individuals affected by the breach and to reduce the risk of harm to those individuals or to mitigate that harm; and (c) the name and contact information of a representative of the organization who can respond to the Privacy Commissioner's questions.
3. **Notification to Individuals:**

- **Content:** A notification to an individual affected by a breach of security safeguards must contain: (a) specified information regarding the nature and extent of the breach; (b) a description of the steps the organization has taken or intends to take to reduce the risk of harm to the individual or to mitigate that harm; (c) a description of the steps the individual could take to reduce the risk of harm resulting from the breach or to mitigate that harm; (d) a toll-free number or email address the individual can use to obtain information about the breach; and (e) information about the organization's internal complaint process and the individual's right to file a complaint with the Privacy Commissioner.
- **Direct Notification:** A direct notification to an individual affected by a breach of security safeguards must be given: (a) by email or any other secure form of communication, if the affected individual has consented to receiving information from the organization in that manner; (b) by letter delivered to the last known home address of the affected individual; (c) by telephone; or (d) in person.
- **Indirect Notification:** A notification to an individual affected by a breach of security safeguards may be given indirectly in the following limited circumstances: (a) direct notification would cause further harm to the individual; (b) the cost of giving direct notification is prohibitive for the organization; or (c) the organization does not have current contact information for the individual. Indirect notification must be given by either: (i) a conspicuous message posted on the organization's website for at least 90 days; or (ii) an advertisement that is likely to reach the affected individual.

Compliance Challenges

PIPEDA's personal information security breach obligations present a number of uncertainties and compliance challenges. For example:

- **Record-keeping:** Are there any thresholds or exceptions to the obligation to create a record of a personal information security breach that does not present a risk of significant harm to an individual? What information should be included in a record of a breach?
- **Significant Harm:** When and how should an organization assess whether a personal information security breach presents "a real risk of significant harm to an individual", and how should that assessment be documented for future reference? In what circumstances will data encryption support a determination that a personal information security breach does not present a "real risk of significant harm"?

- **Reporting/Notification:** When will an organization be considered to have "determined" that a personal information security breach has occurred? How should an organization comply with reporting and notification obligations before the breach is fully investigated? Is phased reporting/notification permitted? How should an organization update or correct previously reported/notified information? What magnitude of financial or other costs of direct notification of a breach will justify indirect notification? Is indirect notification always required if direct notification to any affected individual is unsuccessful (e.g. email or postal mail notification is undeliverable/rejected)? How should an organization obtain an individual's valid consent to receive email notifications of a breach?
- **Withholding/Delaying Disclosure:** In what circumstances may an organization delay disclosure or withhold information about a personal information security breach? For example, may an organization delay disclosure or withhold information about a breach to avoid compromising the investigation of the breach, at the request of law enforcement, to protect commercially sensitive information, to comply with confidentiality obligations or to protect privileged information?
- **Data Controllers/Processors:** How do the personal information security breach obligations apply to an organization that processes or stores personal information (a "data processor") on behalf of another organization (a "data controller"), particularly if the data controller fails or refuses to comply with personal information security breach reporting and notification obligations? How should a data controller comply with its personal information security breach obligations if relevant data processors fail or refuse to cooperate?

Some of those issues might be addressed in guidance documents issued in the future by the government or the Privacy Commissioner.

Preparing for Compliance

The proposed Regulations allow for a delayed coming into force of the personal information security breach obligations after the final regulations are published, to allow organizations time to prepare for compliance. Nevertheless, the length of that delay is uncertain, and it would not be surprising if the personal information security breach obligations came into force by May 2018, when the European Union General Data Protection Regulation comes into force. For more information, see BLG bulletin *The European Union General Data Protection Regulation – A Primer for Canadian Organizations*.

Canadian organizations should now be taking steps to prepare for compliance with PIPEDA's personal information security breach obligations. Following are some suggestions:

- **Security Safeguards:** An organization should assess its security safeguards for personal information and consider whether additional or enhanced safeguards (e.g. robust encryption with a secured encryption key) will reduce the risk that a personal information security breach will result in a real risk of significant harm to individuals.
- **Policies/Procedures – Assessment and Response:** An organization should have written policies and procedures so that each potential personal information security breach is immediately escalated to designated and properly trained personnel for investigation, assessment and response in accordance with a written incident response plan that is consistent with applicable legal requirements, regulatory guidance and relevant best practices. For more information, see BLG bulletins *Cyber Incident Response Plans – Test, Train and Exercise* and *Data Security Incident Response Plans – Some Practical Suggestions*.
- **Policies/Procedures – Record-keeping:** An organization should have written policies and procedures so that designated and properly trained personnel create and securely retain (for applicable retention periods) legally compliant records of every detected personal information security breach.
- **Policies/Procedures – Reporting, Notifications and Disclosures:** An organization should have written policies and procedures so that designated and trained personnel make and document informed decisions about reporting personal information security breaches to the Privacy Commissioner, giving notice of those breaches to affected individuals and relevant government agencies and other organizations, and making timely disclosures of those breaches to other interested persons (e.g. investors and business partners). Legal obligations to report, notify and disclose personal information security breaches may be imposed by statute and by common law and civil law. For more information, see BLG bulletins *Cyber-Risk Management – Data Incident Notification Obligations* and *Cyber Risk Management – Regulatory Guidance for Reporting Issuers' Continuous Disclosure of Cybersecurity Risks and Incidents*.
- **Legal Privilege:** An organization should have a legal privilege strategy that is consistent with personal information security breach reporting, notification and record-keeping obligations and will help avoid inadvertent and unnecessary disclosure of privileged legal advice. For more information, see BLG bulletins *Cyber Risk Management – Legal Privilege Strategy (Part 1)*, *Cyber Risk Management – Legal Privilege Strategy (Part 2)* and *Legal Privilege for Data Security Incident Investigation Reports*.

- **Contracts with Data Processors:** An organization should ensure that its contracts with service providers contain appropriate provisions so that the organization is able to comply with personal information security breach obligations in respect of information that is processed or stored by service providers. An organization that provides data processing services should ensure that its contracts with customers address personal information security breach obligations.
- **Customer Consent to Email Notification:** An organization should take steps to obtain consents from its customers to receive email notifications of personal information security breaches. ■

Author

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

BLG's Cybersecurity Law Group and Privacy/Data Protection Law Group help clients manage cyber risks, achieve legal compliance and respond to security incidents across Canada. More information is available at blg.com/cybersecurity and blg.com/privacy.

BLG Cybersecurity Group – Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Kevin L. LaRoche	Ottawa	613.787.3516
David Madsen	Calgary	403.232.9612
Ira Nishisato	Toronto	416.367.6349

Borden Ladner Gervais

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900
Montréal, QC, Canada H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Bay Adelaide Centre, East Tower
22 Adelaide St W, Suite 3400, Toronto, ON, Canada M5H 4E3
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com