APRIL 2018

PRIVACY BULLETIN

Borden Ladner Gervais

Canadian Personal Information Security Breach Obligations – Preparing for Compliance

Commencing November 1, 2018, Canada's federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") will require an organization that suffers a "breach of security safeguards" involving personal information under its control to keep prescribed records of the breach and, if the breach presents a "real risk of significant harm to an individual", to promptly report the breach to the Privacy Commissioner and give notice of the breach to affected individuals and certain other organizations and government institutions. Preparing for compliance with the personal information security breach obligations may require significant effort, time and expense. Canadian organizations should now be taking steps to prepare for compliance.

Background

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 was amended in 2015 by the *Digital Privacy Act* to add obligations for reporting, notification and record-keeping regarding certain personal information security breaches, but those obligations were not in force because regulations prescribing required details were not enacted. In March 2018, the Government of Canada issued an *Order in Council* to bring those obligations into force on November 1, 2018. The Canadian government published the required *Breach of Security Safeguards Regulations* on April 18, 2018.

Reporting, Notification and Record-Keeping Obligations

Following is a summary of the personal information security breach reporting, notification and record-keeping obligations as set out in PIPEDA and the *Breach of Security Safeguards Regulations*.

Key Concepts – Breach of Security Safeguards and Real Risk of Significant Harm

The reporting, notification and record-keeping obligations invoke two key concepts: "breach of security safeguards" and "real risk of significant harm to an individual".

PIPEDA broadly defines "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 [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 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 prescribed factors (none at this time).

Reporting to the Commissioner

If an organization suffers a breach of security safeguards involving personal information under its control and it is reasonable to believe that the breach creates a real risk of significant harm to an individual, then the organization must report the breach to the Commissioner as soon as feasible after the organization determines that the breach has occurred. The report may be sent to the Commissioner by any secure means of communication.

The report must be in writing and must contain: (a) a description of the circumstances of the breach and, if known, the cause; (b) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period; (c) a description of the personal information that is the subject of the breach to the extent that the information is known; (d) the number of individuals affected by the breach or, if unknown, the approximate number; (e) a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm; (f) a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach; and (g) the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach.

An organization may submit to the Commissioner any new information the organization becomes aware of after the organization submits its breach report to the Commissioner.

Notice to Affected Individuals

If an organization suffers a breach of security safeguards involving an individual's personal information under the organization's control and it is reasonable to believe that the breach creates a real risk of significant harm to the individual, then the organization must notify the individual of the breach as soon as feasible after the organization determines that the breach has occurred, unless giving notice is otherwise prohibited by law.

The notification must contain sufficient information to allow the affected 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. In addition, the notification must contain: (a) a description of the circumstances of the breach; (b) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period; (c) a description of the personal information that is the subject of the breach to the extent that the information is known; (d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach; (e) a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and (f) contact information that the affected individual can use to obtain further information about the breach.

The notification must be conspicuous and must be given directly to an affected individual except in specified circumstances in which indirect notification is required. Direct notification must be given to an affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances. Indirect notification to an affected individual must be given in the following circumstances: (a) direct notification would be likely to cause further harm to the affected individual; (b) direct notification would be likely to cause undue hardship for the organization; or (c) the organization does not have contact information for the affected individual. Indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individual.

Notification to Other Organizations/Government

If an organization notifies an individual about a breach of security safeguards, then the organization must give notice of the breach to any other organization or government institution that the notifying organization believes may be able to reduce the risk of harm that could result from the breach or mitigate that harm.

Record-Keeping Obligations

An organization must keep and maintain a record of every breach of security safeguards involving personal information under its control, even if there is no obligation to report or give notice of the breach (i.e. the breach does not create a real risk of significant harm to an individual). The record must contain any information that enables the Commissioner to verify the organization's compliance with the breach reporting and notification obligations. An organization must maintain the record of a breach for 24 months after the day on which the organization determines that the breach has occurred, and must provide the record to the Commissioner on request.

Enforcement

The Commissioner may investigate an alleged contravention of the personal information security breach reporting, notification and record-keeping obligations either as a result of a complaint filed by an individual or on the Commissioner's own initiative, and publish a report of findings and recommendations after completing the investigation.

The Commissioner's statutory confidentiality obligations include reports and records obtained as a result of the personal information security breach reporting, notification and record-keeping obligations, but the Commissioner is permitted to "make public any information that comes to his or her knowledge" if the "Commissioner considers it in the public interest to do so". In addition, the Commissioner may also disclose to a government institution any information contained in a breach report or record of a breach "if the Commissioner has reasonable grounds to believe that the information could be useful in the investigation of a contravention of the laws of Canada or a province that has been, is being or is about to be committed".

After the Commissioner issues an investigation report in response to a complaint about an alleged contravention of the personal information security breach reporting, notification and record-keeping obligations, or gives notice that the investigation has been discontinued, the individual complainant may apply to the Federal Court of Canada for an award of damages (including damages for any humiliation) and other remedies.

An organization's knowing contravention of the personal information security breach reporting, notification (to individuals, but not to organizations or government institutions) and record-keeping obligations is an offence punishable by a fine of up to $100,000.

Compliance Challenges

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

- **Significant Harm:** When must 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?
- **Reporting/Notification:** When will an organization be considered to have "determined" that a personal information security breach has occurred? What financial costs or other circumstances will constitute "undue hardship" to an organization to 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)? What "secure means of communication" may be used to deliver a report to the Commissioner?
- **Withholding/Delaying Reporting and Notification:** In what circumstances (if any) may an organization delay reporting or notification of a personal information security breach, or withhold information about a breach? For example, may an organization delay reporting or notification of a breach to avoid compromising an investigation of the breach, at the request of law enforcement, to protect commercially sensitive information or to comply with confidentiality obligations?
- **Record-keeping:** Are there any practical 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?
- **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 Commissioner.

Preparing for Compliance

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 occur or will result in 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 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 to 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. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Éloïse Gratton
T 416.367.6225
egratton@blg.com

Katherine McNeill
T 604.640.4150
kmcneill@blg.com

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

Key Contacts

Bradley J. Freedman	Vancouver	604.640.4129
Éloïse Gratton	Montréal	514.954.3106
Ira Nishisato	Toronto	416.367.6349
Robert J. C. Deane	Vancouver	604.640.4250

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