OCTOBER 2018

PRIVACY BULLETIN

Borden Ladner Gervais

Privacy Commissioner's Guidance for Compliance with PIPEDA's Breach of Security Safeguards Obligations

On October 29, 2018 the Office of the Privacy Commissioner of Canada ("OPC") issued a guidance document titled "*What you need to know about mandatory reporting of breaches of security safeguards*" (the "Guidance") to help organizations comply with personal information security breach obligations under Canada's federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

PIPEDA breach reporting requirements as of November 1st, 2018

Commencing November 1, 2018, PIPEDA's personal information security breach provisions will come into force.

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.

The *Breach of Security Safeguards Regulations* (the "Regulations"), which were published on April 18, 2018 clarified certain key concepts of PIPEDA's security breach provisions (see our bulletin on the topic).

The Guidance contains useful clarifications regarding the respective responsibilities of organizations "in control" of personal information and of organizations which merely process same. It also provides details regarding the assessment of a "real risk of significant harm" to individuals and the obligations to report breaches to the Commissioner, to notify individuals and to keep records of all breaches.

Key concepts

The security breach provisions require an organization that suffers a "**breach of security safeguards**" involving personal information **under the organization's 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 OPC and give notice of the breach to affected individuals and certain other organizations and government institutions.

- **Breach of security safeguards**

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.

- **Organisation "in control" (principal organization) and processor**

PIPEDA does not define the word "control". Nevertheless, "control" is generally understood to reflect PIPEDA's accountability principle, which provides that an organization is responsible for personal information "under its control". PIPEDA provides the paradigmatic example of control – "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing". The Guidance clarifies that, where an organization has transferred personal information to a third party for processing and a breach occurs while the information is with the processor, the obligation to report the breach rests with the principal organization – which is the one "in control" of the personal information and therefore responsible for breach reporting. This approach is consistent with the European one (which imposes breach reporting and notification obligations on data controllers at articles 33 and 34 of the General Data Protection Regulation ("GDPR") and, in the same vein, highlight the importance of contractual arrangements which must include requirements for the processor (i.e. the service provider) to notify the principal organization upon the occurrence of a breach. Again similarly to GDPR's requirements, the Guidance indicates that when a processor uses or discloses the personal information for purposes other than the ones documented in the agreement with the principal organization, it is no longer acting as a processor but rather as a principal organization and must therefore comply with breach reporting, notification and recording obligations.

- **Significant 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". It also provides that the circumstances relevant to determining whether a breach of security safeguards creates a "real risk of significant harm" ("RROSH") include the sensitivity of the personal information involved in the breach, the probability that the personal information has been, is being or will be misused and other prescribed factors (none of which have been defined at this time).

The Guidance now clearly requires organizations to develop a framework for assessing RROSH to ensure that all breaches are assessed consistently. Specifically, to evaluate such risk, the OPC reminds that organizations must take into consideration:

- The **sensitivity** of the personal information involved in the breach since certain information may on its face be clearly sensitive (e.g.: medical records, income records) whether other may be sensitive depending on the context (e.g.: name and address of subscribers of some special-interest magazines might be sensitive). The circumstances of the breach and the potential harms that could be caused to individuals should also be accounted for;
- The **probability of misuse** of the personal information. In that respect, a review of the facts and circumstances surrounding the breach should be conducted by organizations. The Guidance lists a series of elements that organizations should consider when creating their RROSH framework, such as the likelihood of someone being harmed by the breach and to understand who has accessed the information, for how long, whether there are evidence of malicious intent, the number of records exposed etc.

Obligation to report to the Office of the Privacy Commissioner

If an organization suffers a "breach of security safeguards" involving personal information in 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. A model report, which organizations are encouraged to use, is posted on the OPC website. The report may be sent to the Commissioner by a secure means of communication and must contain details prescribed by the Regulations. Since details about the exact circumstances and impact of a breach may not be immediately available to the reporting organization, the Guidance clarifies this requirement and indicates that as a starting point, the OPC expects the record to include at minimum:

- date or estimated date of the breach;
- general description of the circumstances of the breach;
- nature of information involved in the breach; and
- whether or not the breach was reported to the OPC/individuals were notified.

The report does not need to include personal details unless necessary to explain the nature and sensitivity of the information.

The principal organization may then submit to the Commissioner additional information regarding the breach to the OPC once it becomes aware of same.

Obligation to notify Affected Individuals and Organizations

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 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 the harm, including details prescribed by the Regulations. PIPEDA and the Breach of Security Safeguards Regulations specify the circumstances and manner in which direct notification and indirect notification may be given to an individual.

When the principal organization notifies an individual about a breach of security safeguards, then it must also give notice of the breach to any other organization or government institution that the organization believes may be able to reduce the risk of harm that could result from the breach or mitigate the harm. The Guidance illustrates this requirement by indicating for instance that a principal organization must notify law enforcement when its computer system is attacked by bad actors and it believes that law enforcement may be able to reduce or mitigate the risk of harm.

Record-Keeping obligation

The principal 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. The principal organization must maintain the record for 24 months after the day on which it determines that the breach has occurred (and may retain same longer to comply with other legal requirements), and must provide the record to the Commissioner on request.

Enforcement

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

After the Commissioner concludes an investigation, an individual complainant may apply to the Federal Court of Canada for an award of damages (including damages for humiliation) and other remedies. An organization's knowing contravention of the personal information security breach obligations is an offence punishable by a fine of up to $100,000.

Preparing for Compliance

Canadian organizations should be prepared 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 – Risk Assessment:** An organization must have written policies and procedures so that designated and trained personnel (including legal counsel) promptly assess each detected personal information security breach to determine whether the incident presents a "real risk of significant harm" to an individual.
- **Policies/Procedures – Reporting, Notifications and Disclosures:** Principal organizations should have written policies and procedures so that designated and trained personnel (including legal counsel) 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). Processors should also have written policies and procedures so that designated and trained personnel report breaches to principal organizations for whom they process personal information. 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*.
- **Policies/Procedures – Record-keeping:** Principal organizations should have written policies and procedures so that designated and trained personnel (including legal counsel) create and securely retain (for applicable retention periods) legally compliant records of every detected personal information security breach.
- **Legal Privilege:** An organization should have a documented legal privilege strategy that is consistent with personal information security breach reporting, notification and record-keeping obligations to help avoid inadvertent and unnecessary disclosures of privileged legal advice and advice provided by technical consultants engaged by legal counsel for the purpose of providing 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 Processors:** A principal 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. Processors should ensure that their contracts with clients address personal information security breach obligations. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Elisa Henry
T 514.954.3113
ehenry@blg.com

Éloïse Gratton
T 416.367.6225
egratton@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

BLG Vancouver
1200 Waterfront Centre, 200 Burrard St
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415
blg.com