Cybersecurity and Privacy Bulletin

March 2019

Frequently Asked Questions – Compliance with PIPEDA's Security Breach Obligations

Canada's federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") imposes obligations on private sector organizations that suffer a breach of security safeguards affecting personal information under their control.

Details of those obligations are set out in PIPEDA, the *Breach of Security Safeguards Regulations* and the guidance document titled "What you need to know about mandatory reporting of breaches of security safeguards" issued by the Office of the Privacy Commissioner (OPC) (the "Guidance").

Following are some frequently asked questions about the breach of security safeguards obligations and related issues.

A. Background and Definitions

What activities are regulated by PIPEDA?

PIPEDA regulates the collection, use and disclosure of "personal information" in the course of a "commercial activity" by private sector organizations in all provinces and territories except British Columbia, Alberta and Québec (each of which has a substantially similar personal information protection law).

PIPEDA also applies in all provinces and territories to the collection, use and disclosure of personal information in the course of a commercial activity 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.

What is "personal information"?

"Personal information" is defined in PIPEDA as "information about an identifiable individual". Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of the information, alone or in combination with other information. Certain kinds of personal information (e.g. certain business contact information and information about an employee of an organization that is not a federal work, undertaking or business) are not regulated by PIPEDA.

What is a "commercial activity"?

"Commercial activity" is defined in PIPEDA as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists".

What is a "breach of security safeguards"?

"Breach of security safeguards" is defined in PIPEDA 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 the information is held) against loss, theft and unauthorized access, disclosure, copying, use or modification.

What are the security breach obligations?

A "breach of security safeguards" gives rise to three obligations on the organization in control of personal information affected by the breach: (1) report the breach to the Privacy Commissioner of Canada (the "Privacy Commissioner"); (2) give notice of the breach to all affected individuals and to certain other organizations and government institutions; and (3) keep records of the breach.

The reporting and notification obligations apply only if it is reasonable to believe the breach of security safeguards presents a "real risk of significant harm" to an individual. The record-keeping obligation applies to every breach of security safeguards.

What is a "real risk of significant harm"?

"Significant harm" is defined 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 factors relevant to determining whether a breach of security safeguards creates a "real risk of significant harm" include: (1) the sensitivity of the personal information involved in the breach; (2) the probability that the personal information has been, is being or will be misused; and (3) other prescribed factors (none of which have been prescribed at this time).

The Guidance explains that some personal information (e.g. medical records and income records) is almost always considered to be sensitive, but most information can be sensitive, depending on the context. Consequently, when assessing the sensitivity of personal information affected by a breach, it is important to consider the circumstances of the breach and the potential resulting harms to individuals. The Guidance provides a number of questions to consider when assessing the probability of misuse of personal information. For example:

- Who actually accessed or could have accessed the personal information?
- Is there evidence of malicious intent (e.g., theft, hacking)?
- Were a number of pieces of personal information breached, thus raising the risk of misuse?
- Has harm materialized (demonstration of misuse)?
- Was the information lost, inappropriately accessed or stolen?
- Has the personal information been recovered?
- Is the personal information adequately encrypted, anonymized or otherwise not easily accessible?

What organization is responsible for compliance with the security breach obligations?

The security breach obligations apply to the organization that has "control" over the personal information affected by the breach. 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 following 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 explains that if an organization (the "principal organization") transfers personal information to a third party for processing and a breach occurs while the information is with the processor, then the security breach obligations remain with the principal organization (which is the organization in control of the personal information).

The Guidance cautions that business relationships can be complex with organizations playing shifting roles regarding personal information, and determining which organization has personal information "under its control" requires a case-by-case assessment. For example, if a processor uses or discloses personal information for purposes other than providing services for the principal organization, then the processor is acting as a principal organization in control of the information when used or disclosed for those other purposes and must therefore comply with the security breach obligations.

Do the security breach obligations apply only to incidents caused by hacking or other criminal activities?

No. The security breach obligations apply to any breach of security safeguards, regardless of the cause, that affects personal information under an organization's control. For example, the security breach obligations would apply to a breach involving paper records of personal information or a breach caused by an error by an organization's personnel.

Are there any exemptions for small businesses?

No. All businesses that collect personal information in the course of a commercial activity are subject to the security breach obligations. There are no exemptions for small businesses.

Are there any exemptions for small breaches?

No. The security breach obligations apply to any breach of security safeguards that affects personal information under an organization's control, regardless of the number of individuals affected or the amount of personal information involved.

The record-keeping obligation applies to every breach of security safeguards. The reporting and notification obligations apply only if it is reasonable in the circumstances to believe the breach of security safeguards presents a real risk of significant harm to an individual.

Do other laws impose similar personal information security breach obligations?

Yes. It depends on the nature of the organization handling the personal information, the province/territory in which the organization is based or where the information was collected, and the type of personal information involved.

The Alberta *Personal Information Protection Act* imposes similar reporting and notification obligations regarding incidents involving the loss of, or unauthorized access to or disclosure of, personal information that present a real risk of significant harm to an individual.

As of March 1, 2019, the British Columbia *Personal Information Protection Act* and Québec's *Act respecting the protection of personal information in the private sector* do not impose similar obligations regarding breaches of security safeguards for personal information, but the provincial privacy commissioners have encouraged private sector organizations to voluntarily report and give notice of personal information security breaches.

There are various provincial/territorial health information protection statutes that impose similar obligations on health information custodians regarding breaches of security safeguards for personal health information.

Some sector-specific statutes impose similar cybersecurity incident reporting obligations.

Canadian common law and civil law might also impose obligations to give notice of a personal information security breach to affected individuals and organizations.

B. Breach Reporting Obligations

If an organization suffers a breach of security safeguards involving personal information under the organization's 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 Privacy Commissioner.

How quickly must a report be filed?

A report must be filed with the Privacy Commissioner "as soon as feasible after the organization determines that the breach has occurred". There is no statutory definition of "as soon as feasible", or any maximum reporting period.

What information must be contained in a report?

A report of a breach of security safeguards must be in writing and must contain:

(1) a description of the circumstances of the breach and, if known, the cause;

(2) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;

(3) a description of the personal information that is the subject of the breach to the extent that the information is known;

(4) the number of individuals affected by the breach or, if unknown, the approximate number;

(5) 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;

(6) a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach; and

(7) the name and contact information of a person who can answer, on behalf of the organization, the Privacy Commissioner's questions about the breach.

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

Since all required information might not be immediately available, an organization may file an initial report and later file supplementary reports when the organization obtains additional information about the breach.

The OPC has provided a template PIPEDA breach report form, but organizations can report in any format they see fit provided that the report includes all required information.

How should a report be filed with the Privacy Commissioner?

A breach report may be sent to the Privacy Commissioner by any secure means of communication. The OPC recommends that encrypted/password protected reports be submitted by email, with the password delivered by separate email.

Will a report be confidential to the Privacy Commissioner?

The Privacy Commissioner's statutory confidentiality obligations apply to security breach reports and records, but the Privacy Commissioner is permitted to "make public any information that comes to his or her knowledge" if the "Privacy Commissioner considers it in the public interest to do so". In addition, the Privacy Commissioner may disclose to a government institution any information contained in a breach report or record "if the Privacy 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".

For those reasons, organizations should assume that security breach reports and records may be disclosed by the Privacy Commissioner or otherwise become publicly available.

C. Breach Notification Obligations

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

If an organization gives notice of a breach to an affected individual, then the organization must also give notice of the breach to certain other organizations and government institutions.

How quickly must notice be given to an affected individual?

Notice must be given to an affected individual "as soon as feasible after the organization determines that the breach has occurred", unless giving notice is otherwise prohibited by law. There is no statutory definition of "as soon as feasible", or any maximum notice period.

What information must be contained in a notice?

Notice of a breach must contain sufficient information to allow an 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. The notice should not be overly legalistic, and should be easily understandable.

The notice must include:

(1) a description of the circumstances of the breach;

(2) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period;

(3) a description of the personal information that is the subject of the breach, to the extent that the information is known;

(4) a description of the steps the organization has taken to reduce the risk of harm that could result from the breach;

(5) a description of the steps affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and

(6) contact information affected individuals can use to obtain further information about the breach.

How must notice be given to affected individuals?

Notice must be conspicuous and must be given directly to each affected individual, except in the following circumstances in which indirect notification is required: (1) direct notification would be likely to cause further harm to the affected individual; (2) direct notification would be likely to cause undue hardship for the organization; or (3) the organization does not have contact information for the affected individual.

"Direct notification" means notice 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" means notice given to an affected individual by public communication or similar measure that could reasonably be expected to reach the individual. For example, advertisements in online or offline newspapers and other ways in which the organization makes public announcements (e.g. a prominent notice on the organization's website or other online/digital presence).

When must notice be given to other organizations or government institutions?

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.

For example, an organization may be required to give notice of a breach to law enforcement (if the breach resulted from criminal activity) or to a payment processor (if the breach involved payment card information) if they may be able to reduce the risk of harm that could result from the breach or mitigate the harm.

There is no prescribed form or content of notice to another organization or government institution.

D. Record-Keeping Obligations

If an organization suffers a breach of security safeguards involving personal information under the organization's control, then the organization must keep a prescribed record of the breach, and must provide the record to the Privacy Commissioner on request.

When must a record be created and kept?

An organization must create and keep a record of every breach of security safeguards involving personal information under the organization's 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).

What information must be contained in a record?

A record of a security breach must contain any information that enables the Privacy Commissioner to verify the organization's compliance with the security breach obligations, including:

(1) the date or estimated date of the breach;

(2) a general description of the circumstances of the breach;

(3) the nature of information involved in the breach; and

(4) whether or not the breach was reported to the Privacy Commissioner and individuals were notified of the breach.

The record should also contain sufficient details for the Privacy Commissioner to assess whether the organization has correctly applied the real risk of significant harm standard, and otherwise met its obligations to report and notify in respect of a breach that poses a real risk of significant harm to an individual. This could include a brief explanation of why the organization did not report the breach to the Privacy Commissioner and notify individuals of the breach.

The record does not need to include personal details about affected individuals unless necessary to explain the nature and sensitivity of the information.

How long must a record be retained?

A record of a security breach must be retained for 24 months after the day on which the organization determines that the breach has occurred.

An organization may be subject to other legal obligations that require the organization to retain a record for a longer period.

E. Enforcement and Compliance

What are the potential consequences of non-compliance with the security breach obligations?

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

After the Privacy Commissioner issues an investigation report in response to a complaint about an alleged contravention of the security breach 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 humiliation) and other remedies.

An organization's knowing contravention of the security breach reporting, notification to affected individuals (but not to other organizations or government institutions) and record-keeping obligations is an offence punishable by a fine of up to $100,000. The OPC does not prosecute offences under PIPEDA or issue fines, but can refer information regarding the possible commission of an offence to the Attorney General of Canada, who would be responsible for any ultimate prosecution.

What should an organization do to prepare for compliance with the security breach obligations?

There are a number of steps organizations could take to prepare for compliance with the personal information security breach obligations, including:

- Assess existing security safeguards for personal information, and consider whether additional or enhanced safeguards (e.g. robust encryption with a secured encryption key or multi-factor authentication) will reduce the risk that a personal information security breach will occur or will result in significant harm to individuals.
- Establish written policies and procedures so that each personal information security breach is promptly escalated to properly trained personnel for response in accordance with a suitable written incident response plan.
- Establish written policies and procedures, including a written framework for assessing whether a personal information security breach presents a real risk of significant harm, so that trained personnel make and document consistent 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).
- Establish written policies and procedures so that properly trained personnel create and securely retain (for applicable retention periods) legally compliant records of every personal information security breach.
- Establish a legal privilege strategy to help avoid inadvertent and unnecessary disclosure of privileged legal advice.
- Ensure that contracts with data processors and other service providers contain appropriate provisions for compliance with personal information security breach obligations.
- Obtain legal advice suitable for the organization's specific circumstances and regarding each personal information security breach. This FAQ provides general information only, and is not a substitute for legal advice. ■

Authors

Bradley J. Freedman
T 604.640.4129
bfreedman@blg.com

Éloïse Gratton
T 514.954.3106
egratton@blg.com

Elisa Henry
T 514.954.3113
ehenry@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