Bennett Jones

10-Step Guide to New Mandatory Breach Reporting Regulations

This 10-step guide will walk you through the upcoming changes to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), the factors to consider in being prepared under PIPEDA and other related considerations. This guide is no replacement for targeted legal advice. If you are an organization affected by the changes to PIPEDA, please contact us to determine what you need to do to be prepared and how you can minimize your organization's potential legal exposure. There is no "one size fits all" when it comes to managing compliance with privacy regulation.

The biggest changes, which will be **coming into force on November 1, 2018**, are:

1. Mandatory breach reporting to the Office of the Privacy Commissioner (OPC).
2. Mandatory breach notification to impacted individuals.
3. Mandatory breach record-keeping.
4. Financial penalties of up to $100,000 for non-compliance with items 1 to 3.

Background

PIPEDA applies to the collection, use or disclosure of *personal information* in the course of a *commercial activity*.[1]

Personal information includes any factual or subjective information about an identifiable individual. Information will be about an "identifiable individual" when there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other information. Examples include: email addresses, credit card numbers, name, the contents of a safe deposit box, financial records, biometric records, and information collected through GPS or RFID chips.

A **commercial activity** is conduct that is of a commercial character (including the selling, bartering or leasing of donor, membership or other fundraising lists).

PIPEDA does not generally apply to:

- business contact information;
- information used by an individual for only personal purposes;
- information used only for journalistic, artistic or literary purpose;
- information about an employee if it is not used or disclosed in connection with the operation of a federal work, undertaking or business;
- information handled by municipal, provincial, territorial, or federal governments;
- municipalities, universities, schools, and hospitals (they are covered by provincial laws); or
- political parties, political associations, charities or not-for-profits unless they are engaging in commercial activities that are not central to their mandate.

Step 1: Identify What Information You Have

Primary Considerations

- Identify categories of **personal information** for which your organization is responsible and which of those fall within the scope of PIPEDA.
  - Not all information falls within the same degree of sensitivity. Consider what information is high-risk. For example, financial and medical records have been considered as very sensitive by the OPC.
- Was the personal information collected by fair and lawful means?
  - Do you have documentation on why the personal information was collected?
  - Do you have documentation of the individuals' consent?
  - The purpose for which the personal information is being collected must be identified by the organization before or at the time of collection.
  - The collection and use of information must be limited to the identified purpose.
- Consider whether you **need** the personal information you are gathering.
  - If not required to fulfill the identified purpose, information should be destroyed, erased or made anonymous.
  - Develop guidelines and implement procedures to govern destruction of personal information.

Other Considerations

- Does your organization have personal information affected by the legislation in other jurisdictions? For example, if your organization offers goods or services to, or monitors the behaviour of, EU data subjects, the General Data Protection Regulation (GDPR) may apply.
  - Non-compliance with the GDPR can result in administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher).
- Does your organization have any contractual obligations with third parties should there be any incident affecting any category of confidential information?
- If a consumer or individual calls and requests access to their information, can you give it to them in a timely manner?
- Is the personal information as accurate, complete, and up-to-date as possible?

Step 2: Understand How Information is Stored

Primary Considerations

- Understand where and how the personal information is stored and the means by which it could be accessed.

Other Considerations

- Limit internal access to those employees who require access in order to carry out the purpose for which the information was collected.

Step 3: Implement Safeguards to Protect Your Information

Primary Considerations

- Implement safeguards appropriate to the sensitivity of the information, including:
  1. **Physical measures** (e.g., locked filing cabinets; restricted access to offices).
  2. **Organizational measures** (e.g., security clearances and limiting access on a "need to know" basis).
  3. **Technological measures** (e.g., use of passwords and encryption).
- Make employees aware of importance of maintaining confidentiality of personal information—develop, document and deliver appropriate and mandatory privacy training for all employees.
- Use care in disposal or destruction of personal information. For example, are your printers wiped before they are thrown out?

Other Considerations

- Implement measures so that your organization can detect unauthorized access to or disclosure of personal information. A failure to implement any detection measures may expose an organization to an invader without even knowing about it.
- Are your security measures regularly reviewed and updated?

Step 4: Ensure Third-Party Contracts Protect You

Primary Considerations

- **Contracting third parties to process personal information on your behalf does not relieve you of responsibility under PIPEDA.**
- Have a recorded basis for selecting the third-party vendor and for your satisfaction that they have appropriate safeguards in place.
- Contractual provisions with third parties should identify items such as:
  1. Their obligation to safeguard the personal information.
  2. Their obligation to notify you about security incidents.
  3. Your ability to oversee and potentially audit their operations as it concerns the personal information they process on your behalf.
  4. Who bears the burden of the costs associated with a data security incident.

Other Considerations:

- When the contract is completed, ensure the information is returned or disposed of.
- Limit all information sent to the third party to that required for the fulfilment of the contract.
- Consider requiring certification of cyber hygiene from a third party.
- Consider requiring insurance for data breaches as part of any contract.
- If there is a data security incident, can your third party afford to deal with the resulting costs or will they fold and leave you hanging?

Step 5: Institute Breach Response Plan

Primary Considerations

- Who will be informed of a data security incident? A security breach response team typically includes someone from:
  - counsel (external and internal);
  - information technology;
  - security;
  - communications/media relations;
  - executive team; and
  - privacy/compliance.
- How will your team be informed of the breach?
  - Specific mechanisms of notification for each team member should be instituted.
  - Identify responsibilities of each team member in managing incident and response to that incident.
  - Are there "understudies" available if one of your team is unavailable?
- Your plan should include:
  - procedures for analyzing a potential data security incident;
  - procedures for containing a potential data security breach;
  - procedures for remediation measures following a data security breach;
  - insurance information;
  - plan for notifications; and
  - counsel contact information.

Other Considerations

- Are there backups of all of your business information?
- What if...
  1. You're locked out of your email?
  2. The data security incident happens during off hours or on a holiday?
  3. You're locked out of your network?

Step 6: Evaluate for a Real Risk of Significant Harm

Primary Considerations

Was there a breach of security safeguards?

- Breach of security safeguards means loss of, unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards or from failure to establish those safeguards (see Step 3).

If so, is there a real risk of significant harm?

- "Significant harm" includes: humiliation, damage to reputation or relationships and identity theft.
- When analyzing whether there is a real risk of significant harm, look at what personal information has been breached and the circumstance through the following factors:

1. **The sensitivity of the personal information involved in the breach.**
   - Some information (SIN, health information, income records, etc.) are almost always considered to be sensitive information.
   - Some information can be sensitive depending on the context. For example, a subscription to a news magazine would not be considered sensitive, but a subscription to certain special-interest magazines might be.
   - Look at the harms that can be accrued to the individual to determine sensitivity.
2. **The probability that the personal information has been, is being, or will be, misused.** Ask yourself the following questions, for example:
   - What happened?
   - How likely is it that someone would be harmed by the breach?
   - Who actually accessed or could have accessed the personal information?
   - How long has the personal information been exposed?
   - Is there evidence of malicious intent?
   - Were a number of pieces of personal information breached?
   - Is the breached information in the hands of an individual/entity that represents a reputational risk to the individual(s) in and of itself?
   - Was the information exposed to limited/known entities who have committed to destroy and not disclose the data?
   - Was the information exposed to individuals/entities who have a low likelihood of sharing the information in a way that would cause harm?
   - Was the information exposed to individuals/entities who are unknown, or to a large number of individuals, where certain individuals might use or share the information in a way that would cause harm?
   - Is the information known to be exposed to entities/individuals who are likely to attempt to cause harm with it?
   - 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?

- **Consult external legal counsel to determine if security incident needs to be reported if it is in grey zone.**
- **Consult external legal counsel on content of assessment as it may have legal implications for the organization.**

Step 7: Maintain Privilege

Primary Considerations

- Your written assessment of whether the security incident gives rise to a real risk of significant harm can have legal implications for your organization, and may be producible in investigations or litigation concerning this event or future events.
- Maintain privilege through correspondence with external counsel with respect to the written assessment of whether there is breach of security safeguards that has given rise to a real risk of significant harm.
- Correspondence with in-house counsel is not always protected by solicitor-client privilege.

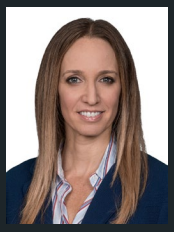
Step 8: Record All Breaches

Primary Considerations

- You must maintain a record of every breach of security safeguard for at least 24 months after the date on which your organization learned of the breach. This record can be requested by the Office of the Privacy Commissioner.
- Record all breaches of personal information under your control—whether there is a real risk of significant harm or not.
- The record should include:
  1. date or estimated date of the breach;
  2. general description of the circumstances of the breach;
  3. nature of information involved in the breach;
  4. whether or not the breach was report to the Privacy Commissioner of Canada/individuals were notified;
  5. if the breach was not reported to the Privacy Commissioner/individuals, a brief explanation of why the breach was determined not to pose a "real risk of significant harm"; and
  6. the individual responsible for report.

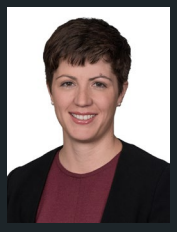
Other Considerations

- Appoint one specific senior individual (e.g., CEO or privacy officer) to record the information and maintain the breach.
- Keep the board of directors apprised of management of security events.
  - Consider issues of privilege when reporting to the board as the board minutes may be producible in litigation or investigations concerning this event or future events.
- If cybersecurity incidents or risks materially affect a company's products, services, relationships or competitive conditions, publically traded companies must provide appropriate disclosure.
- The breach record may have legal implications as it may be producible in investigations or litigation concerning this event or future events. Consider consulting external counsel.



Ruth Promislow
Partner

416.777.4688
promislowr@bennettjones.com



Kate Rusk
Associate

416.777.6159
ruskk@bennettjones.com

Step 9: Reporting and Notification Obligations

Non-compliance with the notification obligations listed below can result in:

- The court ordering an organization to correct its practices, pay damages to the complainant, including damages for humiliation; and publish a notice of any action taken to correct its practices.[2]
- Fines of up to $100,000.

Office of the Privacy Commissioner

- Report to the Office of the Privacy Commissioner as soon as feasible after you have determined a breach involving a real risk of significant harm has occurred.
- The report must contain prescribed elements such as:
  1. a description of the circumstances of the breach;
  2. the date of the breach;
  3. a description of the personal information involved;
  4. an estimate of the number of individuals impacted;
  5. a description of any steps the organization has taken to reduce the risk of harm;
  6. a description of any steps the organization has taken to notify individuals of the breach; and
  7. the name of and contact information for a person who can answer the Commissioner's questions about the breach.
- **Consult external legal counsel on content of report as it may have legal implications for organization.**

Affected Individuals

- Notify affected individuals. The notification must include certain prescribed elements, including:
  1. a description of the breach;
  2. the date of the breach;
  3. a description of the personal information that is the subject of the breach;
  4. the steps that the organization has taken to reduce the risk of or mitigate any harm to the affected individual;
  5. the steps that the affected individual could take to reduce the risk of or mitigate any harm; and
  6. a toll-free number or email address that the affected individual can use to obtain further information.
- The notification can be provided in any "reasonable" manner, including in person, by email, or by telephone. Some exemptions for broader notifications (eg newspaper ads) instead of individually addressed notification are possible in certain circumstances.
- **Consult external legal counsel on content of report as it may have legal implications for the organization.**
- The organization is not required to notify the individual of a breach in some specific circumstances (e.g., if doing so is prohibited by law).

Organizations That Can Help Mitigate Harm

- Notify any institutions or organizations that you believe can reduce the risk of harm that could result from the breach or mitigate the harm.
- For example:
  1. notify law enforcement; and
  2. notify everybody who processes your payments, including your payment processor or acquiring bank in the case of a breach affecting individual.
- **Consult external legal counsel on content of notification as it may have legal implications for organization.**

Step 10: Review and Learn

Primary Consideration:
Once the crisis is past, take this opportunity to review your operations. Look for areas of weakness and areas that can be improved for the next breach.

Notes:

1. With respect to organizations that are not a federal work, undertaking or business, PIPEDA does not apply with respect to the collection, use or disclosure of personal information occurring within British Columbia, Alberta or Québec, as each of those provinces have privacy legislation that has been deemed substantially similar to PIPEDA. Several other provinces have health information privacy legislation that have been deemed substantially similar to PIPEDA. PIPEDA does not apply to employee information if it is not a federal undertaking, but other provincial legislation may apply.
2. In certain circumstances, the Federal Court may order an organization to correct its privacy practices and award damages to a complainant as a private right of action.