Print Form

# PIPEDA breach report form

For use by private sector organizations reporting breaches of security safeguards to the Office of the Privacy Commissioner (OPC).

**What is a breach of security safeguards?**

A breach of security safeguards is defined in the Personal Information Protection and Electronic Documents Act (PIPEDA) as: the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 of PIPEDA or from a failure to establish those safeguards.

**Am I required to submit a report to the OPC if there has been a breach at my organization?**

On June 18, 2015, the Digital Privacy Act was passed into law. This Act includes an amendment to PIPEDA requiring organizations to report breaches of security safeguards to the OPC involving personal information under their control where it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

This requirement came into effect on November 1, 2018. Read our guidance, what you need to know about mandatory reporting of breaches of security safeguards, for more information. This form can be used by organizations that have experienced a breach to meet their legal obligations under PIPEDA and the Breach of Security Safeguards Regulations: SOR/2018-64.

**I am an individual affected by a privacy breach. Should I use this form?**

No. Individuals who wish to make a complaint about a breach of their privacy by an organization should not use this form. Instead, consult the report a concern section of our website.

**Should I include personal information in this form?**

No. The form should not include personal information other than the business contact information of the person(s) at the organization that the OPC can contact to get answers to any follow-up questions. The form should not include the names or other identifying details of affected individuals. It is intended to provide information about the breach and the type of information that was breached.

**How soon after a breach should I submit this form?**

Organizations must report a breach of security safeguards to the OPC as soon as feasible after the organization determines that the breach has occurred, even if not all information (for example, the cause or planned mitigation measures) is known or confirmed. You can add or correct information as it becomes available.

**What happens after an organization reports a breach to the OPC?**

When the OPC becomes aware of a breach, we might seek more information from the organization involved and then work to identify and resolve any PIPEDA compliance issues and mitigate any of the incident's damaging effects.

**How will the OPC handle information provided by organizations in a breach report?**

The OPC generally has a duty to maintain the confidentiality of breach reports submitted to the Privacy Commissioner under PIPEDA. However, there are some exceptions to this obligation. For instance, the OPC may disclose information in a breach report to:

- domestic and international counterparts in accordance with information sharing agreements or arrangements
- a government institution if the Commissioner has reasonable grounds to believe that the information could be useful in investigating a contravention of the laws of Canada or a province.

The Commissioner may also disclose information publicly where he believes it is in the public interest to do so. Public interest disclosures are considered carefully on a case-by-case basis. The Commissioner would normally not publicly disclose information that would pose a security risk.

Information provided to the OPC in a breach report could sometimes be used as the basis for starting an investigation and in any ensuing investigation.

The Digital Privacy Act also amends the federal Access to Information Act (ATIA) to create a statutory exemption from the disclosure of any data breach of security safeguards report in response to access to information requests under the ATIA.

**Where can I get more information on responding to a privacy breach?**

Please see our office's guidance, what you need to know about mandatory reporting of breaches of security safeguards.

# PIPEDA Breach Report

**Throughout this form, the asterisk (*) indicates mandatory fields required by law. Other fields are optional.**

- ◉ original report
- ○ amended or updated report

## Information about the organization

* Legal name of the organization:

* Address of organization

* City:

* Postal code:

* Province/Territory/State:

* Country:

*** Contact information of a person who can answer, on behalf of the organization, OPC's questions about the breach.**

* Please choose one: ○ Internal representative ○ External representative

* First Name:

* Last Name:

* Title/position:

* Country Code:

* Telephone:

Extension:

* Email:

* Street address:

* City:

* Province/Territory/State:

* Postal code:

* Country:

## Breach description

* **Is the provided number of affected individuals an approximation?**

Yes No

* **Number of individuals affected by the breach or, if unknown, the approximate number:** (If possible, please also provide the total number of Canadians affected by the breach)

* Total number of individuals affected:

Total number of Canadians affected:

Comment:

* When the breach occurred:

Please indicate start date or approximate start date and provide further details below in comments.

* Start date of breach occurrence:

End date of breach occurrence:

Comment:

### Type of breach:

(Please select the option that best fits from the list below.)

## * Description of the circumstances of the breach, and, if known, the cause:

1. Description of all organizations involved in the breach including their role(s) with respect to the personal information in question.
2. How and why the breach occurred (please include some technical detail regarding the breach including an explanation of the methodology of the attack if one took place).
3. When the breach was discovered.
4. Where the breach occurred.
5. Who may have had access to the personal information (to the extent known).

## Description of relevant security safeguards in place at the time of the breach to prevent the type of incident that occurred:

## * The nature of the personal information that was breached

Select all that apply.

- ☐ Account information (credit card number, customer account number, debit card expiry, etc.)
- ☐ Assigned identifying number or symbol (driver's license number, SIN, passport number, etc.)
- ☐ Biometric information (facial image, fingerprints, etc.)
- ☐ Contact information (first and/or last name, email address, civic address, etc.)
- ☐ Credential information (cell phone password, credit card PIN, online banking password, etc.)
- ☐ Demographic information (DOB, relationship status, ethnic origin, etc.)
- ☐ Education information
- ☐ Employment information (employer or formal organization, income, years at current job, etc.)
- ☐ Financial and credit information (credit bureau information, etc.)
- ☐ Genetic information (DNA profile or other information indicative of genetics, etc.)
- ☐ Government-issued information (driver's license card, social insurance card, passport, etc.)
- ☐ Health information (fitness monitoring data, medical history, medical (including psychological) records, etc.)
- ☐ Law enforcement and administration information (incarceration history, criminal record, etc.)
- ☐ Other information indicative of preferences, opinions or behaviour (political opinions, etc.)
- ☐ Security / surveillance information (login for home alarm system, GPS location data, identifiable physical characteristics, etc.)
- ☐ Other (other information permitting physical monitoring, other information supporting bank account fraud, sex or gender, etc.)

## * Description of the personal information that is the subject of the breach to the extent known:

List the elements of personal information that were breached (for example, driver's license, civic address, social insurance number). Please specify if client or employee information was accessed.

**IMPORTANT:** This section should not include any identifying information.

## Notification

The Breach of Security Safeguard Regulations stipulate that any notification where the breach represents a real risk of significant harm (RROSH) must contain specific elements laid out in section 3 of the regulations.

### * Description of the steps that the organization has taken or intends to take to notify affected individuals:

* Have affected individuals been notified?

◯ Yes ◯ No

If no, is notification planned?

◯ Yes ◯ No

Date notification began (or is planned):

Date notification was completed:

Method of notification used for affected individuals (please select one of the options below)

Some or all affected individuals not notified.

☐ We confirm that the contents of the notification contain all of the elements listed in section 3 of the Breach of Security Safeguards Regulations.

If individuals have not been notified, and notification is not planned, please provide the rationale:

If you have chosen to notify individuals indirectly, describe the rationale for doing so as well as the type of indirect notification used:

## * Form of notification

Select all that apply.

- ☐ Letter
- ☐ Email
- ☐ Telephone
- ☐ Public announcement (for example, newspaper, website)
- ☐ Other (describe below)

### Describe the form of notification, for example the rationale for using multiple forms of notification.

**Important:** Do not include any identifying personal information.

If possible, please attach a copy of the notification (or script of notification). Do not include personal information.

## Risk mitigation

*** Description of any steps (apart from notification to affected individuals) taken by the organization to reduce the risk of harm to affected individuals, or to mitigate that harm:**

For example, this can include:

- taking steps such as resetting passwords, offering credit monitoring services where appropriate, recovering misdirected information, seeking confirmation from unintended recipients that they have destroyed and not circulated the information
- notifying third parties or organizations that can reduce the risk of harm, such as the police, payment Processors or credit card companies

*** Have any other organizations and/or government institutions been notified about the breach?**

◯ Yes ◯ No

If yes, please list and provide the date of notification:

Name of organization(s): Date(s) notified:

## Description of the steps taken to reduce the risk of a similar event occurring in the future:

For example:

- an experienced IT security firm has been hired to review the organization's security program and we are committed to making any recommended improvements
- all new contracts with web service providers will include the following quality control provisions ...
- a privacy training module has been developed and is now mandatory for all staff
- all laptops will be encrypted
- software change management protocol has been updated

## Please submit this form through one of the following means:

### By Secure breach reporting portal:

Submit a privacy breach report
We encourage all organizations to submit their breach report through our online secure breach reporting portal.

### By postal mail or by hand:

PIPEDA breach response officer
Office of the Privacy Commissioner of Canada
30 Victoria Street, 1st Floor
Gatineau, QC K1A 1H3

Should you require additional information about breach reporting requirements under PIPEDA, please see our office's guidance entitled What you need to know about mandatory reporting of breaches of security safeguards.