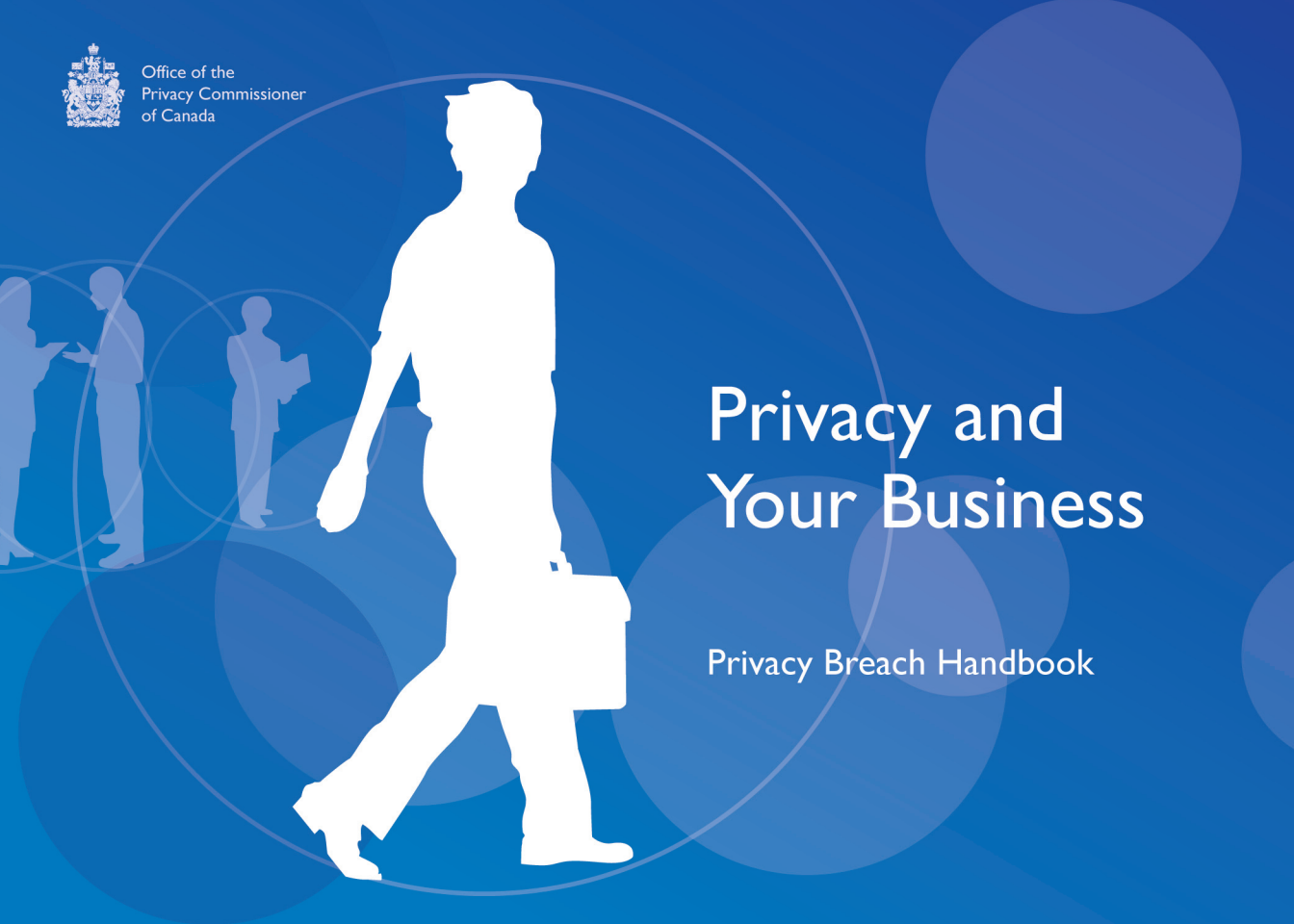

Office of the
Privacy Commissioner
of Canada
Privacy and
Your Business
Privacy Breach Handbook

What is a breach?

A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information.

Such activity is "unauthorized" if it occurs in contravention of applicable privacy legislation, such as the *Personal Information Protection and Electronic Documents Act* (PIPEDA), or similar provincial privacy legislation.

Some of the most common privacy breaches happen when personal information is stolen, lost or mistakenly disclosed. A privacy breach may also be a consequence of faulty business procedure or operational breakdown.

Why you should notify individuals in certain circumstances:

Your customers and employees expect businesses to protect their personal information. They want to be informed about privacy risks associated with your personal information handling practices.

Through notification, you are demonstrating good privacy practices and building trust into your brand.

Good privacy means good business.

What to do after discovering a breach:

Incident description:

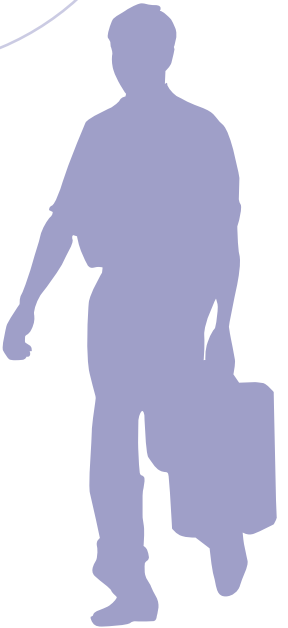
- ☐ What was the date of the incident?
- ☐ When was the incident discovered?
- ☐ How was it discovered?
- ☐ What was the location of the incident?
- ☐ What was the cause of the incident?

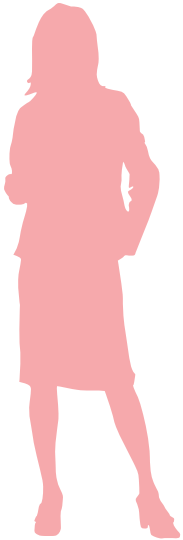
Breach containment and preliminary assessment:

- ☐ Immediately contain the breach.
- ☐ Designate an appropriate individual to lead the initial investigation. This individual should have appropriate scope within the organization to conduct the initial investigation and make initial recommendations.
- ☐ Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your organization responsible for privacy compliance.
- ☐ If the breach appears to involve theft or other criminal activity, notify the police. Do not compromise the ability to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.

Evaluate the risks associated with the breach. Determine:

- ☐ what personal information was involved.
- ☐ what the cause and extent of the breach was.
- ☐ how many individuals have been affected and who they are.
- ☐ what harm could result from the breach.





Notification:

- ☐ Determine whether affected individuals should be notified.
- ☐ If they are to be notified, determine when and how, and who will notify them.
- ☐ Decide what should be included in the notification.
- ☐ Determine if others should be informed (i.e. privacy commissioners, police)

Prevent future breaches:

- ☐ Determine what short- or long-term steps would be needed to correct the situation.

For the complete Privacy Breach Checklist, visit the Office of the Privacy Commissioner website at ***www.privcom.gc.ca***

To report a breach, contact us:

Tel: 613-995-2042

Fax: 613-947-6850

notification@privcom.gc.ca


Limiting Use, Disclosure and Retention
Safeguards
Individual Access
Accountability
Consent
10 PRIVACY PRINCIPLES
Limiting Collection
Challenging Compliance
Accuracy
Identifying Purposes
Openness

10 Privacy Principles

These principles define fundamental privacy rights for individuals and obligations for business. The best way to prevent a privacy breach is to adopt these principles and implement fair information practices into your everyday business.

1. Accountability:

You are accountable for personal information in your custody or transferred to a third party for processing.

2. Identifying Purposes:

You must identify and document your purposes before you can collect and use personal information.

3. Consent:

Knowledge and consent are required to collect, use or disclose personal information. However, there are some exceptions to this principle. Visit www.privcom.gc.ca to learn more.

4. Limiting Collection:

You can only collect personal information that is required to meet your identified purposes and you must use fair and lawful means to collect this information.

5. Limiting Use, Disclosure and Retention:

You can only use or disclose personal information for purposes identified to the individual, unless you obtain further consent. You can only retain personal information as long as you actually require it.

6. Accuracy:

Personal information must be as accurate, complete and up-to-date as its purposes require.

7. Safeguards:

You must protect personal information with safeguards appropriate to its sensitivity.

8. Openness:

You must be open about your policies and procedures to protect personal information and these policies and procedures should be understandable and easily available.

9. Individual Access:

Individuals have a right to know if you hold any personal information about them, have a right of access to it, and they may have a right to have it corrected.

10. Challenging Compliance:

Individuals have a right to challenge your compliance with these privacy principles or any other aspect of PIPEDA.

For more information on how to meet your responsibilities for each of these principles, see *Your Privacy Responsibilities: A Guide for Businesses and Organizations* at www.privcom.gc.ca.

1 800 282-1376

privcom.gc.ca

1 800 282-1376

privcom.gc.ca