Confidentiality incident involving personal information

What to do when a confidentiality incident occurs?

In this section, the term "organization" is used to designate public bodies, private enterprises and professional orders, to the extent provided in the Professional Code.
In addition, the term "acts" refers to both the *Act respecting Access to documents held by public bodies and the protection of personal information* (Access Act) and the *Act respecting the protection of personal information in the private sector* (Private Sector Act).

What is a confidentiality incident?

By law, a confidentiality incident is any access, use or communication of personal information that is not authorized by law, as well as the loss of personal information or any other breach of the protection of such information.

For example, a confidentiality incident could occur when:

- a staff member accesses personal information without authorization;
- a staff member discloses personal information to the wrong recipient;
- the organization is the victim of a cyberattack: phishing, ransomware, etc.

If an organization has reason to believe that a confidentiality incident involving personal information in its possession has occurred, it must take reasonable steps to reduce the risk of injury and prevent similar incidents from occurring in the future.

The obligations in the event of a confidentiality incident are listed in the left-hand menu:

- Take measures to reduce risks and avoid future incidents
- Assess whether the incident poses a risk of serious injury
- Notify:
    - The Commission and the persons whose information is compromised
    - Persons likely to prevent or reduce the risk of serious injury
- Keep a confidentiality incident register

The Commission's order powers

Responsibility for personal information held by a third party

Updated: September 20, 2022

TRANSLATION SOURCE: CAI.GOUV.QC.CA/INCIDENT-DE-CONFIDENTIALITE-IMPLIQUANT-DES-RENSEIGNEMENTS-PERSONNELS/ AS LAST ACCESSED ON JANUARY 25, 2024, AT 4:30 P.M.

Take measures to reduce risks

Take measures to reduce risks and avoid future incidents

If the organization has reason to believe that a confidentiality incident has occurred involving personal information in its possession, it must take **reasonable measures** to **reduce the risk** of injury **and prevent similar incidents from occurring in the future.**

The following questions are useful to quickly assess the situation:

- **Who:** Who are the persons affected by the incident? Are they employees, customers or business partners? Who may have had access to the personal information?
- **How many:** How many persons are affected by the incident?
- **What:** What is the nature of the personal information covered by the incident? Is it sensitive information? What are the risks to the individuals concerned?
- **When:** When did the incident occur? When was it discovered?
- **Where:** Where did the incident occur? Within the organization? If so, in which department? Did the incident occur at a third party holding personal information on behalf of the organization (e.g. agent, supplier)?
- **Why:** What are the causes? What security measures were in place at the time of the incident? Why were they not effective?

The reasonable measures to be put in place depend on the situation. Every situation is different. Even if all the relevant information is not known at the outset, it is important to react quickly. As required, the organization continues to **adapt its measures or adopt new ones** as the circumstances and impacts of the incident become clearer.

Updated: September 20, 2022

Assess the risks

Assess whether the incident poses a risk of serious injury

For any confidentiality incident, the organization must assess the seriousness of the risk of injury to the individuals concerned. To do so, it must consider, in particular:

- the sensitivity of the information concerned;
- the anticipated consequences of its use;
- the likelihood that it will be used for injurious purposes.

The organization must consult its privacy officer. It may also involve other persons, such as the information security officer or external experts.

If the analysis identifies a risk of serious injury, the organization must notify the Commission and the individuals affected by the incident.

If not, the company must continue to work to reduce the risk and prevent a similar incident from occurring in the future.

Updated: September 20, 2022

Notify the Commission and the persons concerned

Notify the Commission and persons whose information is compromised

Where there is a risk of serious injury to the individuals whose information is compromised, the organization must promptly notify the Commission. All individuals whose personal information is compromised by the incident must also be notified by the organization. If the organization fails to notify the persons concerned, the Commission may order it to do so.

However, the organization need not notify individuals whose personal information is compromised if such notification could interfere with an investigation conducted under the law to prevent, detect or repress crime or statutory violations.

The *Regulation respecting confidentiality incidents* determines the content and terms of the notices that must be sent to the Commission and the persons concerned.

- **NOTICE TO THE COMMISSION D'ACCÈS À L'INFORMATION**

When a confidentiality incident presents a risk of serious injury, the organization must notify the Commission in writing. The **notification form** specifies all the information to be provided.
Once the notification form has been sent, the organization receiving the new information must promptly communicate it to the Commission.

- **NOTICE TO THE PERSONS CONCERNED**

The notice to the person concerned must inform them of the scope and consequences of the incident presenting a risk of serious injury.

The notice must contain:

- A description of the personal information covered by the incident. If this information is not known, the organization must provide the reasons why it is impossible to provide such a description.
- A brief description of the circumstances of the incident.
- The date or time period when the incident occurred or, if that is not known, the approximate time period.

- A brief description of the measures taken or planned to reduce the risk of injury as a result of the incident.
- The measures that the organization suggests the person concerned take in order to reduce the risk of injury or mitigate any such injury.
- The contact information for a person or department that the individual concerned can contact for more information about the incident.

In addition, an organization may notify the person concerned via public notice if it needs to act quickly to reduce the risk of serious injury or mitigate any such injury. However, the organization is still required to send a notice directly to the person concerned as soon as possible.

There are only three situations where a public notice can be issued without sending a notice directly to the person concerned:

- when sending such notice may cause greater harm to the person concerned;
- when sending such notice is likely to cause undue hardship for the organization;
- when the organization does not have the contact information for the person concerned.

A public notice may be made by any method that could be reasonably expected to reach the person concerned.

Notify the persons likely to prevent or reduce the risk of serious injury

The organization may notify any person or organization that is likely to reduce the risk of serious injury. Only the necessary personal information can then be disclosed, without the consent of the person concerned. The organization's privacy officer must record this disclosure.

Updated: May 2, 2023

TRANSLATION SOURCE: CAI.GOUV.QC.CA/INCIDENT-DE-CONFIDENTIALITE-IMPLIQUANT-DES-RENSEIGNEMENTS-PERSONNELS/AVISER-COMMISSION-ET-PERSONNES-CONCERNEES/ AS LAST ACCESSED ON JANUARY 25, 2024, AT 4:30 P.M.

Confidentiality incidents register

Keep a confidentiality incidents register

Every organization must keep a register of all confidentiality incidents involving personal information. It must include in this register even incidents that do not present a risk of serious injury. At the request of the Commission, the organization must provide a copy of its register.

The confidentiality incidents register must contain the following:

- A description of the personal information covered by the incident. If this information is not known, the organization must provide the reasons why it is impossible to provide such a description.
- A brief description of the circumstances of the incident.
- The date or time period when the incident occurred or, if that is not known, the approximate time period.
- The date or time period when the organization became aware of the incident.
- The number of persons affected by the incident or, if that is not known, the approximate number.
- A description of the elements that led the organization to conclude that there is a risk of serious injury to the persons concerned, such as:
    - the sensitivity of the personal information concerned;
    - any possible ill-intentioned uses of such information;
    - the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes.
- If the incident presents a risk of serious injury, the dates when the notices were sent to the Commission and to the persons concerned. The organization must also indicate whether it issued public notices and, if so, the reasons for doing so.
- A brief description of the measures taken by the organization after the incident in order to reduce the risk of injury.

The information in the registers must be kept up to date and kept for at least five years after the date or time period when the organization became aware of the incident.

Updated: May 2, 2023

TRANSLATION SOURCE: CAI.GOUV.QC.CA/INCIDENT-DE-CONFIDENTIALITE-IMPLIQUANT-DES-RENSEIGNEMENTS-PERSONNELS/REGISTRE/ AS LAST ACCESSED ON JANUARY 25, 2024, AT 4:30 P.M.

Powers of the Commission

The Commission's order powers

The Commission may order any person, after providing them with an opportunity to make representations, to take any measure to protect the rights of the persons concerned. It may, among other things, order the return of the personal information concerned to the organization or its destruction. A person who is the subject of an order without prior notice because, in the opinion of the Commission, there is an emergency or risk of irreparable injury, may, within the time specified in the order, make representations to allow for reconsideration by the Commission.

If the incident poses a risk of serious injury, the Commission may also order the organization to notify the persons concerned if the organization did not do so when it was required to do so.

Updated: September 20, 2022

TRANSLATION SOURCE: CAI.GOUV.QC.CA/INCIDENT-DE-CONFIDENTIALITE-IMPLIQUANT-DES-RENSEIGNEMENTS-PERSONNELS/POUVOIRS-COMMISSION/ AS LAST ACCESSED ON JANUARY 25, 2024, AT 4:30 P.M.

Responsibility for personal information held by a third party

In various situations, organizations entrust personal information to third parties to hold. Organizations remain responsible for all of their obligations in the event of a confidentiality incident, such as measures to be taken, register to be kept and updated, and notices to be given.

Updated: September 20, 2022

TRANSLATION SOURCE: CAI.GOUV.QC.CA/INCIDENT-DE-CONFIDENTIALITE-IMPLIQUANT-DES-RENSEIGNEMENTS-PERSONNELS/RESPONSABILITE-TIERS-DETENTEUR/ AS LAST ACCESSED ON JANUARY 25, 2024, AT 4:30 P.M.