



Checklist: Protecting Personal Information



Questions to ask yourself to comply with the law: Did you...



Name a person responsible for the protection of personal information (privacy officer)?

The privacy officer is, by default, the highest-ranking person in the organization. It's possible to name someone else or to delegate certain responsibilities **in writing**.

You must publish the privacy officer's contact information on your website. If you don't have a website, you must inform the public some other way (email, announcement, etc.).



Adopt an internal governance policy?

You must develop a policy that explains the rules to collect, keep and destroy personal information, the division of responsibilities within the team, and the process for handling complaints.



Define the parameters of your personal information collection?

You must know what personal information you want to collect, for what purpose, and how long you plan on keeping it. The collection must be **limited to personal information that's necessary** to achieve your purposes. You must also know the means that will be used to collect the information.



Make a privacy policy available?

You must provide a clear and accessible privacy policy to the people concerned. If you have a website, the policy must be published there.

The policy explains how your organization collects, uses, and protects personal information.



Get valid consent?

You must, among other things, share with people why their personal information is being collected, how it's being collected, and that they have the right to withdraw their consent.

In practice, this information is usually included in a **privacy policy**.



Take adequate measures to protect personal information?

The more personal information you keep and the greater the risks involved in managing it, the more robust your security measures will need to be.

In particular, you must conduct privacy impact assessments (PIA) and include clauses on the protection of personal information in your service contracts when necessary.



After a confidentiality incident: Did you...

A **confidentiality incident** may happen when someone **accesses, uses, or shares** personal information **without being authorized to do so under the law**, or when personal information is **lost**.



Take adequate measures to limit the consequences?

You must **immediately** take adequate measures to limit the consequences of a confidentiality incident. For example, this may mean:

- disabling compromised access or changing passwords,
- requesting that the personal information shared by mistake be deleted.

You must also take measures to prevent similar incidents from happening in the future.



Assess the risk level?

When an incident happens, you must assess the level of risk it poses to the people concerned. You must consider, in particular:

- the sensitivity of the information concerned,
- the possible consequences of its use,
- the likelihood that the information will be used in a way that causes harm.

Your privacy officer must be involved in this assessment.



Notify the right people?

If you have determined that a **risk of serious harm** exists, you must report the incident to Quebec's access to information commission, the Commission d'accès à l'information (CAI).

In most cases, you must also notify the people involved. This notice must include information, such as:

- a description of the personal information involved in the incident,
- a description of the incident, including the date or period the incident occurred,
- a description of the measures taken to limit the consequences.



Fill out your register of confidentiality incidents?

You must fill out the register every time an incident occurs, no matter the incident's gravity.

Each incident must be kept in the register for at least five years.

A **serious harm** is an act or event that can cause a **significant negative consequence** for the person concerned, their property, or their interests. For example, it may result in:

- reputational damage,
- financial loss,
- identity theft.

