Rédiger une politique de confidentialité

Guide explicatif pour les entreprises

Drafting a Privacy Policy: Explanatory Guide for Businesses
Unofficial translation by McCarthy Tétrault LLP

CAI Commission d'accès à l'information du Québec

As of September 22, 2023, you must publish a privacy policy if your organization collects personal information through a technological means (for example an email address, a website or an application).[1] This policy must be written in clear and simple terms

This short guide aims to answer the following questions:

- **What is a privacy policy?**
- **What should such a policy contain?**
- **How to draft such a policy in clear and simple terms?**

[1] This obligation is set out at Article 8.2 of the *Act respecting the protection of personal information in the private sector*.

1. What is a privacy policy?

1.1 A way to inform individuals from whom you collect personal information

A privacy policy is used to inform individuals whose personal information is collected by a technological means, such as individuals who visit a website.

When an organization collects personal information from someone, it must provide them with certain information.[2] If the collection is done by a technological means, no one provides this information on behalf of the organization. The privacy policy therefore aims to provide the same information to the individual concerned. It can also include other useful information for making an informed decision.

It must be published on the organization's website, if it has one. It must also be disseminated in a way that reaches the people concerned, depending on the context. For example:

- A link to consult before placing an online order;
- A message displayed at the first use of a mobile application;
- A booklet included in the packaging of a connected object, intended to be read before first use.

[2] See article 8 of the *Act respecting the protection of personal information in the private sector*.

1.2 What is not a privacy policy?

The privacy policy is part of a set of documents related to your services and your personal information management practices. It is important not to confuse these documents.

Personal Information Governance/Framework Policy	Consent	Terms of Use or Terms of Service
This policy describes how your organization manages personal information in the course of its activities. Notably, it sets out: • The roles and responsibilities of personnel in the governance of personal information, from its collection to its destruction; • The rules pertaining to the retention and destruction of personal information; and • The complaint process related to the protection of personal information. This policy primarily targets your organization, as it frames your activities, but it also concerns the people from whom you collect personal information. You can make it public and you must at least publish detailed information about your practices.	This is the process that allows your users to accept your practices related to personal information. It can take different forms, depending on the context. For example: • A paper or online form to authorize you to obtain a credit report to assess a financing request; • A verbal request in person or on the phone to send a survey to a customer; or • A cookie banner. To be valid, consent must meet the criteria listed in the law.[3] Depending on the case, the consent request may contain a hyperlink to the privacy policy.	These are the rules that govern the use of your website, your application, or your services. They define what users and you are allowed to do, and everyone's responsibilities. For example, they may include: • The permitted and prohibited uses of your services; • The cases where you can terminate a user's access; and • The prohibition to reproduce the content of your site or other rules related to intellectual property. The terms of use or service are not related to personal information. They may refer to a privacy policy, governance, or personal information protection policy, but they should not be merged.

[3] These criteria are listed in Article 14 of the *Act respecting the protection of personal information in the private sector (RLRQ, c. P-39.1)*. Consult the Guidelines on the criteria for valid consent to learn more - available in French only.

2. What should your privacy policy contain?

A regulation describes the information to include in the privacy policies of public organizations. This regulation mainly reproduces the information that a public organization must provide when it collects personal information.[4]

There is no equivalent regulation for the private sector. The suggested content here is therefore based on what an organization must provide when it collects personal information, in addition to certain additions inspired by the regulation provided for the public sector.

To start, you must indicate the name of your organization, the effective date of the policy, and the date of the last update. Here are the elements to include or consider.

2.1 The manner in which you collect personal information

First, you must indicate the technological means you use to collect personal information. For example:

- Emails received by your customer service;
- An online appointment request form;
- An application offered to your customers;
- Certain cookies from your website;
- Video surveillance; and
- A connected object.

[4] This information is listed in Article 65 of the *Act respecting access to documents held by public bodies and the Protection of personal information (RLRQ, c. A-2.1)*.

You must also name the people or other organizations that collect personal information for you, if any. For example:

- A technology service provider such as an order platform or a newsletter manager;
- A consultant who provides part of the services you offer to your customers; and
- An agency responsible for answering questions or handling complaints from your customers.

If you collect personal information using technology that can identify, locate, or profile the person concerned[5] (such as an investor or consumer profile), you must indicate:

- The use of this technology;
- How to activate these functions. They must be deactivated by default.

If you offer a product or a technological service that has privacy settings, these settings must ensure the highest level of privacy by default. You may specify this in the privacy policy.

2.2 The personal information that you collect and why

You also need to include the personal information that you collect. For example:

Categories	Examples
Identification information	First name, last name, postal address, email address, phone number
Technical or digital information	IP address, date and time of connection, pages visited, actions taken on a website
Financial information	Salary, payment information, credit report
Health information	Weight, sex at birth, health history, lifestyle habits, medication use
Demographic information	Age, ethnic origin, nationality, place of residence
Biometric information[6]	Fingerprints, shape of the face, hand or iris of the eye, keyboard typing pattern, voice print

[5] Article 8.1 of the *Act respecting the protection of personal information in the private sector* defines profiling as: “the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person’s work performance, economic situation, health, personal preferences, interests or behaviour”).

[6] Regarding biometrics, please consult the accompanying guide published by the Commission – only available in French).

You must mention the purposes for which you collect this personal information. For example:

- Open a file and process service requests;
- Ship ordered products;
- Manage billing and process payments;
- Handle and resolve complaints and dissatisfactions; and
- Offer personalized recommendations based on the purchase profile.

You must indicate the measures offered to refuse the collection of certain personal information and the possible consequences, if any. For example:

- Obtain information in person, rather than by email;
- Place an order without creating an account and without earning loyalty points; or
- Refuse login cookies and use your website without benefiting from certain features.

2.3 Your personnel who have access to personal information

The categories of people who have access to personal information within your organization should also be named in your privacy policy. For example:

- The customer service center;
- The billing department; and
- The people responsible for providing products and services to customers.

If you transmit personal information to other people or organizations to achieve the objective, or if they have access to personal information, you must indicate:

- The personal information or categories of personal information concerned;
- The purposes for which you communicate this personal information;
- The names or categories of people or organizations that receive this personal information or have access to it; and
- If personal information can be transmitted outside of Quebec.

2.4 Your security measures

You can include a brief description of the measures taken to ensure the confidentiality and security of personal information. For example:

- Physical measures, like locked premises;
- Technological measures, like firewalls; and
- Administrative measures, like the adoption of an information security policy.

2.5 The rights of individuals concerned

You must indicate the rights of the individuals whose personal information you hold, namely those:

- To access the personal information you hold about them;
- To correct or update their personal information;
- To file a complaint according to the process set out in your policy and practices for managing personal information.

You may also include:

- The technological means offered to access personal information or to correct it, if any (for example, an accessible online file or an access request form);
- The name of the person responsible for the protection of personal information in your company and their contact information;
- The contact information of the person, organization, or administrative unit to contact for any questions related to the privacy policy.

3. Tips for writing a clear and simple policy

The law requires a policy to be written in clear and simple terms. To achieve this, we recommend following the clear communication rules below.

Remember that clarity is assessed from the reader's perspective, not the writer's. Therefore, you need to listen and adjust when necessary.

Throughout your work, document your thoughts, options, and decisions. This could help you demonstrate the seriousness of your approach, if necessary.

3.1 Understand the needs of your target audience

Identify your readers

Determine their needs and specificities, including their language skills and their level of knowledge of the subject. You can rely on a combination of internal data and public studies or statistics.

Identify their reading context

Determine how your readers will access the policy, the timing, and the process. What is their objective at the time of reading? This influences their level of interest and the time spent reading. You can make decisions accordingly, like the messages to prioritize and the format of the text.

3.2 Chosing the messages

Select pertinent information

Get to the point. Provide the necessary information to understand your practices and comply with the law. Remove what your readers don't need.

Identify key takeaways

Take into account the needs and specificities of your readers as well as their reading context. Determine the most important elements to answer their questions.

Consider the scope and sensitivity of the information collected

In the interest of transparency, identify what may surprise your readers or have a significant impact on their privacy. Evaluate whether certain messages need to be specifically brought to the readers' attention.

3.3 Create a clear and apparent structure

Use clear and evocative titles that reflect your key messages

Browsing the titles should give a good overview of the policy content. You can test several types of titles, such as phrases or questions. Avoid jargon and technical terms.

Create a hierarchy of titles that helps to find information

Create clear and easy-to-identify levels of titles and subtitles. Use them consistently throughout the policy.

3.4 Choose your tone

Stay true to the tone of your organization

The privacy policy is part of your communications! Try to keep the usual tone of your organization.

Adopt a tone that invites reading

Writing in the "you" and "we" can help establish a relationship of trust and proximity, in addition to facilitating reading. Show consideration for your readers. Avoid an authoritative, cold or threatening tone.

3.5 Adopting a clear a precise style

Place the main ideas at the beginning of the paragraph

Provide additional information after the main ideas.

Write short sentences with a simple structure

Limit yourself to one idea per sentence. As much as possible, combine the subject, verb, and object. Remove unnecessary words.

Use common words

Avoid formal language and jargon. Choose usual words that your readers know. If a technical term is necessary, add an explanation or an example.

3.6 Optimize the layout

Use a readable text format

Choose an easy-to-read font and a large enough size.

Create a spacious layout

Write short sections and paragraphs. To facilitate reading, add subheadings to longer sections and shorten lines.

Use visual elements, if necessary

Simple techniques like bullet lists or tables help to break up the length of the text. You can also create visual elements or explanatory diagrams.

3.7 Test your policy

Have your colleagues proofread the policy

Ask a few people in your organization to read the policy. Can they navigate the text and understand the key takeaways? How do they feel when reading the policy?

Test your policy with your target audience

You can do this in several ways, for example through a survey, individual interviews or group interviews. With a good methodology, a few people are usually enough to detect problems.

Adjust the policy following testing

Adjust the policy and test again, if applicable.

3.8 Regularly reassess the policy

Keep your policy up to date

Regularly reassess your policy to update it. For example, you will need to adapt it if your activities evolve and you collect new personal information. Also consider any questions or comments you may receive. When you adjust your policy, re-test it with your target audience to assess its clarity and the understanding it provides of your practices.

Montréal
2045, rue Stanley, bur. 900
Montréal (Québec) H3A 2V4
Téléphone : 514 873-4196

Québec
525, boul. René-Lévesque E,
bur. 2.36
Québec (Québec) G1R 5S9
Téléphone : 418 528-7741

CAI
Commission d'accès
à l'information
du Québec

1 888 528-7741 | cai.gouv.qc.ca

Décembre 2023