UNOFFICIAL GOWLING WLG TRANSLATION

Drafting a privacy policy

Explanatory guide for companies

CAI
Commission d'accès à l'information du Québec

UNOFFICIAL GOWLING WLG TRANSLATION

Since September 22, 2023, you must publish a policy if your company collects personal information by technological means (e.g. e-mail address), website or 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 do you write a policy in clear, simple terms?

1. This obligation is set out in section 8.2 of the *Act respecting the protection of personal information in the private sector*.

UNOFFICIAL GOWLING WLG TRANSLATION

1. What is a privacy policy?

1.1 A way to inform the people whose personal information you collect

A privacy policy informs people whose personal information is collected by technological means, such as visitors to a Web site.

When an organization collects personal information from someone, it must provide that person with certain information[2]. If the collection is done by technological means, no one provides this information on behalf of the organization. The privacy policy therefore aims to provide the same information to the person concerned. It may also include other information useful for making an informed decision.
It must be published on the company's website, if it has one. It should also be distributed in a way that reaches the right people, depending on the context. For example:

- A link to consult before ordering online;
- A message displayed the first time a mobile application is used;
- A booklet included in the packaging of a connected object, designed to be read before first use.

2. This information is listed in section 8 of the *Act respecting the protection of personal information in the private sector*.

UNOFFICIAL GOWLING WLG TRANSLATION

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.

Governance policy or Policy for the protection of personal information	Consent	Conditions of use or terms of service
This policy describes how your organization manages personal information in the course of its activities. In particular, it describes : • The roles and responsibilities of staff in the governance of personal information, from collection to destruction; • Rules for retaining and destroying personal information; • The complaints process for the protection of personal information. This policy is addressed primarily to your organization, since it provides a framework for 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 enables your users to accept your personal information practices. It can take different forms, depending on the context. For example: • A paper or online form to authorize you to obtain a credit file in order to evaluate a financing application; • A verbal request in person or over the phone to send a survey to a customer; • A window for setting *cookies* on a Web site. To be valid, consent must meet the criteria listed in the law[3]. Depending on the case, the request for consent may contain a hyperlink to the privacy policy.	These are the rules that govern the use of your website, application or services. They define what users and you have the right to do, and everyone's responsibilities. For example, they may include: • Permitted and prohibited uses of your services; • When you can terminate a user's access; • Prohibition to reproduce the content of your site or other related rules intellectual property. Terms of use or service are not linked to personal information. They may contain a reference to a privacy or governance policy or protection of personal information, but they must not be merged.

3. These criteria are listed in section 14 of the *Act respecting the protection of personal information in the private sector* (RLRQ, c. P-39.1). Consult the Guidelines on Criteria for Valid Consent for more information.

UNOFFICIAL GOWLING WLG TRANSLATION

2. What should your privacy policy contain?

A regulation describes the information to be included in the privacy policies of public bodies. This regulation mainly sets out the information that public bodies must provide when collecting personal information[4].

There is no equivalent regulation for the private sector. The content suggested here is therefore based on what a company must provide when it collects personal information, plus some additions inspired by the regulations for the public sector.

To get started, you'll need to enter your company's name, the policy's effective date and the date of the last update.

Here are the elements to include or consider.

2.1 How you collect personal information

You must first indicate the technological means you use to collect personal information. For example:

- E-mails received by your customer service department;
- An online appointment request form;
- An application for your customers;
- Certain cookies on your Web site;
- Video surveillance;
- A connected object.

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

UNOFFICIAL GOWLING WLG TRANSLATION

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 ordering platform or newsletter manager;
- A consultant who provides part of the services you offer your customers;
- An agency responsible for answering questions or handling complaints from your customers.

If you collect personal information using a technology that allows you to identify the data subject, to locate or profile him or her[5] (such as an investor or consumer profile), you must indicate :

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

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

2.2 The personal information you collect and why you collect it

You must also include the personal information you collect. For example:

Categories	Examples
Identification information	Last name, first name, postal address, e-mail address, telephone number
Technical or numerical information	IP address, date and time of connection, pages visited, actions taken on a website
Financial information	Salary, payment information, credit report
Health information	Birth weight, sex, health history, lifestyle habits, medication use
Demographic information	Age, ethnic origin, nationality, place of residence
Biometric information[6]	Fingerprints, face, hand or iris shapes, keyboard patterns, voiceprints

5. Section 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 for the purpose of evaluating certain characteristics of an individual, in particular for the purpose of analyzing the individual's work performance, economic situation, health, personal preferences, interests or behaviour.
6. For more information on biometrics, please consult the accompanying guide published by the Commission, titled *Biometrics: principles to be respected and legal obligations of organizations*.

UNOFFICIAL GOWLING WLG TRANSLATION

You must state the purposes for which you are collecting this personal information. For example:

- Open files and process service requests;
- Ship ordered products;
- Manage invoicing and process payments;
- Handle and resolve complaints and dissatisfactions;
- Offer personalized recommendations based on purchasing profile[7].

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

- Get information in person, rather than by e-mail;
- Place an order without creating an account or earning loyalty points;
- Refuse *cookies* and use your website without certain functionalities.

2.3 Persons who have access to personal information

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

- Customer service center;
- Billing department;
- People responsible for providing products and services to customers.

If you transmit personal information to other persons or organizations to achieve the purpose, 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 provide this personal information;
- The names or categories of persons or organizations that receive or have access to this personal information;
- If personal information may be transmitted outside Quebec.

7. In this case, since profiling is involved, the conditions of section 8.1 of the *Act respecting the protection of personal information in the private sector* must also be met.

UNOFFICIAL GOWLING WLG TRANSLATION

2.4 Your safety measures

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

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

2.5 The rights of persons concerned by personal information

You must indicate the rights of the individuals whose personal information you hold, i.e. :

- Access the personal information you hold about them;
- Have their personal information corrected or updated;
- File a complaint in accordance with the process set out in your personal information governance policy and practices.

You can also include :

- The technological means available for accessing or rectifying personal information, if any (for example, an online file or access request form);
- The name and contact details of the person responsible for protecting your company's personal information;
- The contact information of the person, organization or administrative unit to be contacted for any question related to the privacy policy.

UNOFFICIAL GOWLING WLG TRANSLATION

3. Tips for drafting a clear and simple policy

By law, policies must be written in clear, simple terms. To achieve this, we recommend that you follow the clear communication rules below.

Remember that clarity is assessed from the point of view of the reader, not the writer. This means listening and adjusting 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 Understanding the needs of your target audience

Identify your readers

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

Identify their reading context

Determine how, when and where your readers will access the policy. 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, such as which messages to prioritize and text format.

3.2 Select messages

Select relevant information

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

Identify key messages

Take into account the needs and specificities of your readers, as well as their reading context. Determine which elements are most important in answering their questions.

Consider the scope and sensitivity of the information collected

For the sake of transparency, identify what might surprise your readers or have a significant impact on their private lives. Evaluate whether certain messages should be specifically brought to readers' attention.

UNOFFICIAL GOWLING WLG TRANSLATION

3.3 Create a clear, visible structure

Use clear, evocative headlines that convey your key messages

Skimming the headlines should give you a good idea of the policy's content. You can try out different types of headlines, such as phrases or questions. Avoid jargon and technical terms.

Create a hierarchy of titles to help you find the information you're looking for

Create clear, easy-to-identify levels of headings and subheadings. Use them consistently throughout the policy.

3.4 Choose your tone

Stay true to your organization's tone

Your privacy policy is part of your communications! Try to keep to your organization's usual tone.

Adopt an inviting tone

Writing in "you" and "we" can help build a relationship of trust and closeness, as well as making it easier to read. Show consideration for your readers. Avoid authoritarian, cold or threatening tones.

3.5 Adopt a clear, precise style

Place the main ideas at the beginning of the paragraph

Give additional information after the main ideas.

Write short sentences with a simple structure

Limit yourself to one idea per sentence. As far as possible, combine subject, verb and complement. Eliminate unnecessary words.

Use everyday words

Avoid formal language and jargon. Choose words your readers are familiar with. If a technical term is necessary, add an explanation or example.

UNOFFICIAL GOWLING WLG TRANSLATION

3.6 Optimizing page layout

Use a legible text format

Choose a font that's easy to read and of a large enough size.

Create an airy layout

Keep sections and paragraphs short. To make reading easier, add subheadings to longer sections and shorten lines.

Use visual elements as needed

Simple techniques such as bulleted lists or tables help break up text length. You can also create visual elements or explanatory diagrams.

3.7 Test your policy

Have your colleagues review the policy

Ask a few people in your organization to read the policy. Can they find their way around the text and understand the main messages? How do they feel about reading the policy?

Test your policy with your target audience

You can do this in a number of ways, such as a survey, individual interviews or group interviews. With the right methodology, it usually only takes a few people to identify problems.

Adapt policy according to test results

Make adjustments and test again, if necessary.

3.8 Reassess your policy regularly

Keep the policy up to date

Reassess your policy regularly to keep it up to date. For example, you'll need to adapt it if your activities evolve and you collect new personal information. Take into account any questions or comments you may receive. When you modify your policy, re-test it with your target audience to assess its clarity and understanding of your practices.

UNOFFICIAL GOWLING WLG TRANSLATION

Montréal
2045 Stanley Street, Suite 900 Montréal (Québec) H3A 2V4 Telephone: 514 873-4196

Quebec
525 René-Lévesque Blvd. René-Lévesque E, bur. 2.36 Québec (Québec) G1R 5S9 Telephone: 418 528-7741

Commission d'accès à l'information du Québec

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

December 2023