OSLER UNOFFICIAL TRANSLATION OF CAI GUIDANCE

Drafting a Confidentiality Policy

Explanatory Guide for Businesses

Comité d'accès à l'information du Québec

Since September 22, 2023, you have been required to publish a confidentiality policy if your business collects personal data by technological means (such as an e-mail address, a website or an application)[1]. This policy must be written in clear and simple language.

This short guide seeks to answer the following questions:

- **What is a confidentiality policy?**
- **What should a confidentiality policy include?**
- **How to write a policy in clear and simple terms?**

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

1. What is a Confidentiality Policy?

1.1 A means of informing people whose personal data you collect

A confidentiality policy is a way of informing people whose personal data is being collected by technological means, such as visitors to a website.

When an organization collects personal data from an individual, it must provide that individual with certain information[2]. If the information is collected by technological means, no one provides this information on behalf of the organization. Thus the confidentiality policy aims to provide the same information to the person in question. Such information may also include other information which is useful for making an informed decision.

This policy must be posted on the business's website, if any. It must also be disseminated so as to reach the people concerned, depending on the context. For example:

- a link to click on before ordering online
- a message that pops up the first time a mobile application is used, or
- a booklet included in the packaging of a related object and intended to be read before first use.

OSLER UNOFFICIAL

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

.2 What is Not a Confidentiality Policy?

The confidentiality policy is part of a set of documents related to your services and your personal data management practices. It is important not to mix up these documents.

Personal Data Governance or Protection Policy	Consent	Terms of Use or Terms of Service
This policy describes how your business manages personal data in the course of its activities. For example, it describes: • The roles and responsibilities of staff in the governance of personal data, from collection to destruction. • Rules for storing and destroying personal data. • Complaints procedures related to personal data protection. This policy is aimed primarily at your business since it encompasses your activities, but it also concerns the people whose personal data you collect. You may make this policy public but you must at least publish detailed information about your practices.	This is the procedure that lets your users accept your practices in relation to personal data. It may take on different forms, depending on the context. For example: • A paper or online form to seek permission to obtain a credit report in order to assess 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 website. To be valid, consent must meet the criteria listed in the Act[3]. A request for consent may, depending on the circumstances, contain a hyperlink to the confidentiality policy.	These are the rules that govern the use of your website, application or services. They define the user's rights and responsibilities and yours as well. These rules may include: • Permitted and prohibited use of your services • Instances where you may terminate a user's access • A ban on reproducing the content of your site or other rules related to intellectual property. Terms of Use or Terms of Service have no bearing on personal data. They may refer to a confidentiality or personal data governance or protection policy, but they may not be merged.

OSLER UNOFFICIAL

[3] These criteria are listed in section 14 of the *Act* respecting *the protection of personal information in the private* sector (CQLR, c P-39.1). For more information, see *Lignes directrices 2023-1 – Consentement: critères de validité*.

2. What Should You Include in Your Confidentiality Policy?

A Regulation describes the information to be included in the confidentiality policies of public bodies. This Regulation essentially sets out the information that must be provided by a public body when collecting personal data[4].

There is no equivalent Regulation for the private sector. The content suggested here is therefore based on what information a business must provide when collecting personal data, including a few additions inspired by the Regulation governing the public sector.

First of all, you must state the name of your business, the date on which the policy came into force and the date on which it was last updated.

The following are elements to be included or to be considered.

2.1 How you collect personal data

You must first describe the technological tools you use to collect personal data. For example:

- emails received by your customer service department
- an online appointment request form
- an application for your customers
- certain cookies on your website
- video surveillance
- a related 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* (CQLR, c A-2.1).

You must also name the persons or other businesses collecting personal data on your behalf, if any. For example:

- a technology services provider, such as an ordering platform or newsletter manager
- a consultant providing part of the services that you offer your customers, or
- an agency hired to answer customer questions or handle customer complaints.

If you collect personal data using technology that makes it possible to identify, locate or profile the data subject[5] (such as an investor or consumer profile), you must reveal:

- that you are using this technology, and
- how to activate these functions, which must be deactivated by default.

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

2.2 Personal data collected by you and why you collect it

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

Categories	Examples
ID information	Surname, first name, postal address, e-mail address, phone number
Technical or numerical information	IP address, connection date and time, pages visited, actions taken on a website
Financial information	Salary, payment information, credit report
Medical information	Weight, gender at birth, medical history, lifestyle habits, medication taken
Demographic information	Age, ethnic origin, nationality, place of residence
Biometric information[6]	Fingerprints, shape of face, hand or iris, keyboard typing pattern, voice print

[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 to evaluate an individual's characteristics, particularly for the purpose of analysing his or her work performance, economic situation, health, personal preferences, interests or behaviour.

[6] As regards biometrics, see the companion guide entitled *Biométrie: principes à respecter et obligations légales des organisations* published by the Commission.

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

- Opening a file and processing service requests
- Shipping products ordered
- Managing invoicing and processing payments
- Handling and resolving complaints and dissatisfaction, or
- Offering personalized recommendations based on purchasing profile[7].

You must describe the alternatives offered to someone who refuses to provide certain personal data, and the possible consequences, if any. For example:

- Obtaining information in person rather than by e-mail
- Placing an order without creating an account or earning loyalty points, or
- Refusing cookies and using your website without the benefit of certain features.

2.3 Persons with access to personal data

The categories of people having access to personal data within your business must also be named in your confidentiality policy. For example:

- customer service department
- billing department, and
- persons in charge of providing products and services to customers.

If you disclose personal data to other persons or businesses to reach your objective, or if they have access to personal data, you must state:

- which personal data or categories of personal data are concerned
- reasons for disclosing the personal data
- the names or categories of persons or businesses receiving or having access to the personal data, and
- whether personal data may be forwarded outside Quebec.

[7] Since this is profiling, the conditions set forth in section 8.1 of the *Act* respecting *the protection of personal information in the private sector* must also be met.

2.4 Your safety measures

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

- physical measures, such as locked premises
- technological measures, such as firewalls, and
- administrative measures, such as the adoption of a data security policy.

2.5 Rights of personal data owners

You must describe the rights of the owners of the personal data in your possession, namely the right to:

- access their personal data in your possession
- have their personal data corrected or updated, and
- file a complaint in accordance with the procedure set out in your personal data governance policy and in your practices.

You may also include:

- the technological tools available for accessing or correcting personal data, if any (e.g., an accessible online file or an access request form)
- the name and contact information of the person in charge of protecting personal data in your company, and
- the contact information of the person, business or administrative unit to contact for any question relating to the confidentiality policy.

OSLER UNOFFICIAL

3. Tips on How to Draft a Clear and Simple Policy

The law requires a policy to be written in clear and simple language. To achieve this, we recommend that you follow the rules of clear communication set out below.

Remember that clarity is in the eye of the reader, not the writer. So you need to be attentive and make adjustments where necessary.

Throughout your work, you should keep track of your thoughts, your options and your decisions. This could help you demonstrate the seriousness of your approach, if required.

3.1 Understanding the needs of your target audience

Identify your readers

Determine what their needs and distinctive characteristics are, particularly their language skills and how much they know about the subject. You can draw on a combination of internal data and studies or statistics in the public domain.

Identify the context of the readers

Determine how, when and in what circumstances your readers will access the policy. What is their objective at the time of reading? This will have a bearing on their interest level and the time spent reading. You can make decisions accordingly, such as which messages to prioritize and what text format to choose.

3.2 Choosing the message

Selecting relevant information

Get straight to the point. Provide the information needed to understand your practices and comply with the law. Eliminate whatever your readers do not need.

Identify key messages

Bear in mind what your readers' needs and specific characteristics are, as well as the context in which they are reading. Pinpoint the most important elements for 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. Assess whether certain messages should be specifically brought to their attention.

3.3 Create a clear, visible structure

Use clear, evocative headings that reflect your key messages

Skimming the headings should give you a good idea of the content of the policy. You may try out different types of heading, such as sentences or questions. Avoid jargon and technical terms.

Create a hierarchy of headings to help you find the information

Create clear and easily identifiable levels of headings and sub-headings. Use them consistently throughout the policy.

3.4 Choose your tone

Stay true to the tone of your company

The confidentiality policy is part of your communications! Try to keep to your company's usual tone.

Adopt a tone that draws in the reader

Using "we" and "you" can help to establish a relationship of trust and intimacy, as well as making the text more reader-friendly. Show consideration for your readers. Avoid a cold, authoritarian or threatening tone.

3.5 Adopt a clear, precise style

Place main ideas at the beginning of the paragraph

Provide additional information after the main ideas.

Write short sentences with a simple structure

Stick to one idea per sentence. To the extent possible, keep the subject, verb and complement together. Eliminate unnecessary words.

Use everyday words

Avoid formal language and jargon. Choose everyday words that are familiar to your readers. If you are required to use a technical term, add an explanation or an example.

3.6 Optimize page layout

Use a legible text format

Choose a font that is easy to read and sufficiently large.

Create an uncluttered layout

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

Use visual aids where necessary

Simple techniques such as bulleted lists or tables help to break up a lengthy text. You can also create visual aids or explanatory diagrams.

3.7 Put your policy to the test

Have your colleagues read over the policy

Ask a few people in your company to read the policy. Can they find their way through the text and grasp the main points? What do they feel when they read the policy?

Test your policy on your target audience

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

Adapt the policy according to test results

Make adjustments and test again, if necessary.

3.8 Reassess your policy regularly

Keep your policy up to date

Reassess your policy regularly to keep it up to date. For example, you will need to adapt it if your business activities change and you collect new personal data. Also take into account any questions or comments you may receive. When you amend your policy, test it again on your target audience to see whether it is clear and makes your practices understandable.