CAI GUIDE TO DRAFTING WEBSITE PRIVACY NOTICES

Posted on December 20, 2023

Categories: Insights, Publications

With the September 2023 entry into force of significant amendments[1] to the Quebec *Act respecting the protection of personal information in the private sector* (the "**Act**"), the Quebec Commission d'accès à l'information ("**CAI**") has been regularly releasing guidance documents in the recent months.

In its most recent update on December 18, 2023, the CAI has issued a brief reference guide to drafting clear and simple privacy notices (the "**Guide**").[2] The CAI notes that the Guide is the first in a series of several publications to be released over the coming months to assist organizations in understanding and complying with their obligations under the *Act*. The Guide aims to clarify what a privacy notice is and what it should contain, and it provides tips on how to write such a policy in clear and simple terms.

As the Guide is only available in French,[3] we have provided a detailed summary below.

When is a privacy notice required?

Since September 22, 2023, any organization collecting personal information through technological means must publish on its website a confidentiality policy (commonly referred to as a privacy notice). This notice must also be written in clear and simple terms.[4]

While an organization must provide certain information when collecting personal information from an individual, when the collection is done by technological means, it is the privacy notice that provides this information. The privacy notice may include additional information when it would be useful to make an informed decision.

The CAI also defines what is not a privacy notice. While the privacy notice is part of a set of related documents, it must not be confused with:

- **Governance or privacy policies** which provide an internal framework for the organization's activities and notably describe the roles and responsibilities of personnel in the governance of personal information from its collection to its destruction, rules for the keeping and destruction of personal information, as well as the complaint process regarding the protection of personal information;[5]
- **Consent requests** (whether obtained through a written document, a cookie banner or a verbal request),

though the CAI notes that a consent request may contain a link to the privacy notice.

- **Conditions of use / Terms of service** which govern the use of a website, application or services, and define the rights and responsibilities of the users and the organization. The CAI notes that while terms of use or service may contain a reference to a privacy or governance policy or a section on protection of personal information, they must not be combined with the privacy policy.[6]

Contents of a privacy notice

While a regulation sets out the information to be included in the privacy policies by public sector entities subject to the *Act respecting Access to documents held by public bodies and the Protection of personal information* (the "**Public Sector Act**"),[7] the *Act* does not have an equivalent mechanism for private sector entities. The CAI states that its Guide suggests information that must be provided by a private sector organization, with some additions inspired by the regulations for the public sector.

1. Means of collection

Organizations must indicate the technological means used to collect personal information (e.g., emails received by the customer service department, an online appointment request form, an application for customers, cookies, video surveillance, a connected device, etc.).

They must also name any other entities that collect personal information on their behalf, such as a technology service provider, a third-party consultant who provides part of the services to the organization's customers; any agencies tasked with answering questions or handling complaints from customers.

Where an entity collects personal information using a technology that has functions to identify, locate or profile an individual, it must also inform the individuals about the use of this technology as well as how to activate these functions. CAI states that such functions must be disabled by default,[8] and where a technological product or service is offered to the public and has privacy settings, these settings must ensure the highest level of confidentiality by default.[9]

2. The personal information collected and the purposes of collection

Organizations must indicate the personal information collected (such as contact, health, demographic, biometric or financial information, as well as technically generated information such as IP address or actions taken on a website).

Organizations must also state the purposes for the collection such as opening files, processing requests, shipping ordered products, managing invoicing, processing payments, and offering personalized recommendations. The CAI also states that organizations must indicate measures available to refuse the

collection of certain personal information and the possible consequences (e.g., obtaining information in person rather than by e-mail, placing an order without creating an account or earning loyalty points, refusing cookies and using the website without certain functionalities).[10]

3. The categories of persons who have access to personal information (within and outside the organization)

The CAI states that the categories of persons who have access to the personal information within the organization (such as customer service, billing department, etc.) must be named in the privacy notice.[11]

Where, in order to achieve its purposes, the organization transfers or gives access to personal information to other entities, it must also indicate:

- the personal information or categories of personal information concerned;
- the purposes for which the personal information is communicated;
- the names or categories of persons or organizations that receive or have access to this personal information; and
- whether personal information may be transmitted outside Quebec.

4. The rights of the individuals

Organizations must indicate the rights of the individuals to:

- access their personal information held by the organization (which can also include available technological means to access or rectify personal information, if any);
- have their personal information corrected or updated;
- file a complaint in accordance with the process set out in the personal information governance policy and practices.

The CAI notes that organizations can also include the name and contact as well as the contact information of the person (or department) to be contacted for questions regarding the privacy notice, and/or the name and contact details of the privacy officer.[12]

5. The organization's security measures

The CAI states that organizations may include a brief description of the physical, technological or administrative measures taken to ensure the confidentiality and security of the personal information.

CAI's tips for drafting a clear and simple policy

The CAI reminds at the outset that clarity is assessed from the point of view of the reader and not the writer of

the notice which requires listening to the readers and adjusting when necessary. The CAI also recommends documenting considerations, options, and decisions throughout the drafting process in the event that it may be necessary to demonstrate the seriousness of the approach.

1. **Understanding the needs of the target audience** by identifying the readers (and their needs, special characteristics, language skills, knowledge level based on internal or external data, studies, statistics); and identifying the context (given that how, when, where, and to what end they will access the notice will influence their level of interest and time spent);
2. **Selecting the message** by choosing the relevant information needed to understand the practices required under the law (including by removing what the readers do not need), by identifying key elements in view of the particular characteristics of the readers, and reading context and by considering the scope and sensitivity of the information collected which may require bringing certain messages to their attention if it may surprise them or have a significant impact on their private lives;
3. **Creating a clear, visible structure** by using clear, jargon-free, and meaningful headlines that convey key messages, and by creating a hierarchy of titles used consistently throughout the notice with easy-to-identify levels of headings and subheadings;
4. **Using an authentic and inviting tone** by aligning it with the organization's usual communications, and by fostering a tone that builds trust rather than making it authoritarian or threatening;
5. **Adopting a clear, precise style** by placing the ideas at the beginning of paragraphs, writing short sentences with simple structures, eliminating unnecessary words, using everyday words instead of formal language or jargon, adding explanations or examples to technical words when they are necessary;
6. **Optimizing page layout** by using an easy-to-read, large enough font, keeping sections short, and using visual elements as needed;
7. **Testing the policy** by having others within and outside the organization read the policy, and adjusting the notice accordingly; and
8. **Reassessing the policy regularly** and keeping it up to date as activities and practices evolve.

McMillan's Privacy & Data Protection Group is happy to assist with specific advice on drafting privacy notices or regarding any other obligations under the Quebec privacy regime.

[1] For additional details on the scope of these amendments, we refer to our previous publications Bill 64 Enacted: Québec's Modern Privacy Regime and "Bill 64: A Checklist to Help Businesses Comply with Modern Privacy Requirements in Québec".
[2] Available on CAI's website in original French.
[3] Please note that the CAI has recently indicated in its consent consultation feedback document that, pursuant to Government of Quebec's linguistic policy and the *Charter of the French language* requirements, it

will not be translating its guidance into English.
[4] See section 8.2 of the *Act*.
[5] See section 3.2 of the *Act* on the obligation or organizations to establish and implement such governance policies and practices, as well as to publish detailed information about said policies in simple and clear language on their website.
[6] The CAI takes a similar position in its *Guidelines 2023-1: Criteria on the Validity of Consent*, available online on the CAI website in original French regarding the request for consent which must be presented separately separate from terms of use, privacy notices and signatures.
[7] *Règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique*, online. We note that despite the many similarities between the obligations under the *Act* and the *Public Sector Act*, there are certain nuances regarding the transparency obligations of public and private sector entities. A similar guide for the public sector entities subject to the *Public Sector Act* has been published by the Quebec government's Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité.
[8] See section 8.1 of the *Act*.
[9] See section 9.1 of the *Act*.
[10] We note that this requirement is absent from the wording of the *Act* unlike the Public Sector Act which provides at section 65(5) that the public body must inform the individual of the consequences for refusing to reply to a request or withdrawing consent to the use of personal information collected.
[11] We note that while under Section 8 of the Act, this information is to be provided to the individual "on request", Section 3.2 requires publishing on the organization's website detailed information about governance policies, and in particular, about the roles and responsibilities of the members of its personnel published in simple and clear language.
[12] We note that section 8 of the *Act* refers to informing the individual of the "contact information" of the person in charge of the protection of personal information, while section 3.1 requires publishing their "title and contact information", without requiring the publication of their name.

by Ayse Gauthier

A Cautionary Note


mcmillan