Client Advisory: Québec's New Legal Framework for the Anonymization of Personal Information

Olalekan (Wole) Akinremi, Anna Troshchynsky, and Victoria Di Felice May 24, 2024

Introduction

On May 15, 2024, the Québec government published the final version of the *Regulation respecting the anonymization of personal information* (the "**Anonymization Regulation**").[1] The Anonymization Regulation comes into effect on May 30, 2024, with the exception of Section 9 (which requires organizations to maintain a register), which comes into effect on January 1, 2025.[2] The Anonymization Regulation is significant, as it introduces Canada's first legal framework on the anonymization of personal information.

The Anonymization Regulation sets out the requirements that organizations (both public and private sector) must meet to anonymize personal information in accordance with the *Act respecting the protection of personal information in the private sector* (the "**Québec Private Sector Privacy Act**") and the *Act respecting Access to documents held by public bodies and the Protection of personal information.*[3] The focus of this advisory will be on the Québec Private Sector Privacy Act.[4] All organizations that anonymize personal information from residents of Québec will be required to ensure that its policies and practices regarding anonymization processes comply with the Anonymization Regulation.

Overview

This advisory summarizes the requirements for anonymization introduced by the Anonymization Regulation and discusses some of the best practices regarding the anonymization of personal information.

This advisory is divided into the following parts:

1. Anonymization Framework Defined in the Québec Private Sector Privacy Act
2. The Anonymization Regulation
   - A. Application
   - B. Requirements for Anonymization
     - I. Pre-Anonymization
     - II. Anonymization Process
     - III. Post-Anonymization
3. Anonymization Standards – "Generally Accepted Best Practices"

---

[1] *Regulation respecting the anonymization of personal information* [The Anonymization Regulation].
[2] *Ibid,* at Section 10.
[3] The Anonymization Regulation applies to any person carrying on an enterprise as referred to in the *Act respecting the protection of personal information in the private sector*, CQLR c P-39.1 [Québec Private Sector Privacy Act]. The Anonymization Regulation also applies to: (i) requirements to anonymize personal information set out in Section 73 of the *Act respecting Access to documents held by public bodies and the Protection of personal information*, CQLR c A-2.1 [Québec Public Sector Privacy Act]; and (ii) all "public bodies" referred to in section 3 of the Québec Public Sector Privacy Act.
[4] The Québec Private Sector Privacy Act applies to "any person carrying on an enterprise." Accordingly, the term "organization" referred to throughout this advisory refers to "any person carrying on an enterprise" within the meaning of the Québec Private Sector Privacy Act.

This advisory is not intended to be a complete statement of the law and does not constitute legal advice. This advisory is for information purposes only, no person should act or rely upon the information contained in this advisory without seeking legal advice.

1. Anonymization Framework Defined in the Québec Private Sector Privacy Act

On September 22, 2023, the second stage of amendments to the Québec Private Sector Privacy Act introduced by *The Privacy Legislation Modernization Act* ("**Law 25**")[5] came into effect. These amendments introduced new obligations regarding the retention, destruction, and anonymization of personal information (pursuant to Section 23 of the Québec Private Sector Privacy Act).

Section 23 of the Québec Private Sector Privacy Act states:

> Where the purposes for which personal information was collected or used are achieved, the person carrying on an enterprise must destroy the information or anonymize it to use it for serious and legitimate purposes, subject to any preservation period provided for by an Act.
>
> For the purposes of this Act, information concerning a natural person is anonymized if it is, at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly.
>
> Information anonymized under this Act must be anonymized according to generally accepted best practices and according to the criteria and terms determined by regulation.[6]

Accordingly, Section 23 of the Québec Private Sector Privacy Act sets the following criteria for anonymization, namely, that:

(i) the organization must ensure that anonymized information is used for **"serious and legitimate purposes"**;

(ii) it is, at all times, **"reasonably foreseeable"** in the circumstances that the anonymized information **irreversibly no longer allows the person to be identified directly or indirectly**; and

(iii) the information is anonymized in accordance with **"generally accepted best practices" and the criteria and terms set out by the Anonymization Regulation**.

However, the Québec Private Sector Privacy Act does not provide any guidance on what constitutes a "serious and legitimate purpose", nor does it set out what constitutes "generally accepted best practices". It is possible that the reference to "generally accepted best practices" may refer to internationally recognized practices, such as those published by the U.S. National Institute of Standards and Technology ("NIST"),[7] discussed below in Section 3: Anonymization Standards – "Generally Accepted Best Practices".

[5] Since Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, received formal assent on September 22, 2021, it became *The Privacy Legislation Modernization Act* – also known as Law 25.
[6] Note that these requirements for anonymization are substantially the same under Section 73 of the Québec Public Sector Privacy Act.
[7] See the U.S. National Institute of Standards and Technology (NIST) published guidance on anonymization techniques at Section 4.2.4 "Anonymizing Information" [The NIST Guidance].

2. The Anonymization Regulation

A. *Application*

The Anonymization Regulation applies to "any person carrying on an enterprise".[8]

B. *Requirements for Anonymization*

The Anonymization Regulation specifies the requirements relating to the anonymization of personal information in three stages, namely the:

(i) steps to take prior to anonymization;

(ii) requirements relating to the process of anonymization itself; and

(iii) steps that must be taken after the anonymization process is complete.

The obligations under each stage are summarized below.

I. Pre-Anonymization

(a) Purpose of Anonymization: Prior to anonymization, an organization is required to **identify the intended purposes** for its use of the anonymized information. These purposes must be consistent with Section 23 of the Québec Private Sector Privacy Act,[9] namely, that the anonymized information is used for a **"serious and legitimate"** purpose. Should the purposes change, the organization must re-assess the seriousness and legitimacy of the new purposes.[10]

II. Anonymization Process

(a) Qualified Personnel: The process of anonymization must be carried out under the supervision of a **"person qualified in the field"**.[11]

(b) Removal of Direct-Identifiers: At the beginning of the anonymization process, an organization must **remove all personal information** from the dataset (that it intends to anonymize) **that can lead to the direct identification of an individual**.[12]

(c) Preliminary Re-Identification Risk Analysis: An organization must conduct a preliminary analysis of the re-identification risks in accordance with the following criteria:[13]

(1) **Individualization**: the inability to isolate or distinguish a person within a dataset;

(2) **Correlation**: the inability to connect datasets concerning the same person;

(3) **Inference**: the inability to infer personal information from other available information; and

[8] Québec Private Sector Privacy Act, *supra* note 3, at Section 1. See also *supra* note 4.
[9] Or Section 73 of the Québec Public Sector Privacy Act.
[10] Québec Private Sector Privacy Act, *supra* note 3, at Section 3.
[11] The Anonymization Regulation, *supra* note 1, at Section 4.
[12] *Ibid,* at Section 5.
[13] *Ibid,* at Sections 3 and 5.

(4) **the risks of other reasonably information available, in particular in the public space, being used to identify a person directly or indirectly.**[14]

(d) Anonymization Measures: An organization must **establish appropriate anonymization techniques** to be used, considering the re-identification risks identified through the preliminary risk analysis. The anonymization techniques must be consistent with "generally accepted best practices".[15] The organization must also establish **"reasonable protection and security measures to reduce re-identification risks"**.[16]

III. Post-Anonymization

(a) Re-Identification Risk Analysis: After implementing the appropriate anonymization techniques and protection measures, an organization must **perform another analysis of the re-identification risks**. The results of the assessment must show that it is "at all times, reasonably foreseeable in the circumstances that the information produced further to a process of anonymization irreversibly no longer allows the person to be identified directly or indirectly." Significantly, this does not require an organization to show that the risk of re-identification is zero. It is sufficient to establish, having regard to the following criteria, that "the residual risks of re-identification are very low":[17]

(1) the circumstances related to the anonymization of personal information, in particular the purposes for which the organization intends to use the anonymized information;

(2) the nature of the information;

(3) the individualization criterion,[18] the correlation criterion,[19] and the inference criterion;[20]

(4) the risks of other reasonably available information, in particular in the public space, being used to identify a person directly or indirectly; and

(5) the measures required to re-identify the persons, taking into account the efforts, resources, and expertise required to implement those measures.

(b) Periodic Re-Identification Risk Assessments: An organization must periodically re-assess the information it has anonymized to ensure that the information remains anonymized, **taking into consideration any technological advancements that may contribute to re-identification**.[21] This assessment requires an organization to update the results of its re-identification risk analysis to ensure that it is still reasonably foreseeable in the circumstances that the information produced further to a process of

[14] The Anonymization Regulation, *supra* note 1, at Section 5.
[15] Currently, no official guidance is provided by the Québec government on what constitutes "generally accepted best practices".
[16] The Anonymization Regulation, *supra* note 1, at Section 6.
[17] *Ibid,* at Section 7.
[18] "individualization criterion" means the inability to isolate or distinguish a person within a dataset.
[19] "correlation criterion" means the inability to connect datasets concerning the same person.
[20] "inference criterion" means the inability to infer personal information from other available information.
[21] The Anonymization Regulation, *supra* note 1, at Section 8.

anonymization irreversibly no longer allows the person to be identified directly or indirectly. If the updated results of the re-identification risk analysis demonstrate that it is reasonably foreseeable in the circumstances for the person to be identified directly or indirectly, the information is no longer consider anonymized.[22]

The intervals at which an organization must conduct these assessments are determined according to the residual risks identified in the latest re-identification risk analysis conducted by the organization and the five elements referred to above.

(c) Record-Keeping: An organization must record the following information in a register:[23]

(1) a description of the personal information that has been anonymized;

(2) the purposes for which the it intends to use anonymized information;

(3) the anonymization techniques used and the protection and security measures established; and

(4) the dates on which the re-identification risk assessments conducted post-anonymization were completed.

The record-keeping requirements referred to in this paragraph are effective as of January 1, 2025.

3. Anonymization Standards – "Generally Accepted Best Practices"

No guidance is provided in the Anonymization Regulation on what constitutes "generally accepted best practices". However, in response to the requirements under the Anonymization Regulation, organizations may consider implementing anonymization practices recommended by standards-setting bodies, e.g., the anonymization techniques recommended by NIST.[24]

NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST has published a guidance document that explains the types of anonymization techniques organizations should use to protect the confidentiality of personal information.[25]

NIST suggests employing **statistical disclosure limitation techniques**[26] to ensure that data cannot be re-identified. These techniques include:

(i) Generalizing Data: making the information within the dataset less precise such as by grouping continuous values;

[22] The Anonymization Regulation, *supra* note 1, at Section 8.
[23] *Ibid,* at Section 9.
[24] The NIST Guidance, *supra* note 7. The NIST Guidance is only one example of recommended anonymization practices by a standards-setting body, other independent bodies, such as the International Organization for Standardization (ISO), also provide anonymization guidance. For example, see: ISO/IEC 27559:2022.
[25] *Supra* note 7.
[26] For additional information on statistical disclosure limitation techniques, see OMB's Statistical Policy Working Paper #22. See also Census Bureau, Report on Confidentiality and Privacy 1790-2002.

(ii) Suppressing Data: deleting parts of the dataset, such as removing direct identifiers or quasi-identifiers;[27]

(iii) Introducing Noise into the Data: adding variations or small changes to parts of the dataset;

(iv) Swapping the Data: exchanging certain data fields of one record with the same data fields of another similar record (e.g., swapping the postal codes of two records); and

(v) Replacing Data with the Average Value: replacing a selected value of data with the average value for the entire group of data.

NIST also offers anonymization tools to assist organizations in their anonymization processes. This includes the **"ARX Data Anonymization Tool"**, which is an open-source software for anonymizing sensitive personal data.[28] This specific software can be used to anonymize data in a variety of contexts, including commercial big data analytics platforms, research projects, clinical data sharing, and for training purposes.[29]

Conclusion

If your organization is subject to Québec privacy laws and intends to anonymize personal information, it should, as soon as possible, update (or develop) policies and practices regarding its anonymization processes to ensure compliance with the Anonymization Regulation. Organizations may wish to consider the recommendations provided by NIST or other standards-setting bodies when updating (or developing) their anonymization policies and practices.

Organizations should monitor their compliance with these new requirements, as non-compliance could result in steep fines and penalties. Organizations found in contravention of the Québec Private Sector Privacy Act may be subject to: (i) penal fines as high as the greater of $25 million or 4% of worldwide turnover for the preceding fiscal year (amounts can be doubled for repeat offences); and (ii) administrative monetary penalties of up to the greater of $10 million or 2% of worldwide turnover for the preceding fiscal year.[30]

If you have any questions, please contact a member of our Technology Law Practice Group.

[27] Quasi-identifiers are identifiers that by themselves do not identify a specific individual but can be aggregated and linked with other information to identify data subjects.
[28] See the National Institute of Standards and Technology (NIST) Disassociability Tools.
[29] See further information on the ARX Data Anonymization Tool.
[30] Québec Private Sector Privacy Act, *supra* note 3, at Sections 91, 92.1, and 90.12.