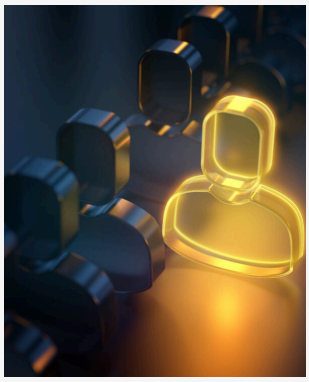
OSLER

Québec's anonymization requirements one year later: lessons and lingering questions for businesses

MAY 8, 2025 13 MIN READ



Related Expertise

- Cybersecurity and Security Incident Response
- Privacy and Data Management

Authors: Éloïse Gratton, Ad. E., Katelyn Smith, Catherine Hart

On May 30, 2024, Québec's *Regulation respecting the anonymization of personal information* [PDF] (the Québec Anonymization Regulation) came into force,[1] setting out specific requirements for the anonymization of personal information under the *Act respecting the protection of personal information in the private sector* (the Québec Privacy Act or the Act).[2] Nearly a year later, key questions remain regarding the scope and application of the Québec Anonymization Regulation and the practical steps organizations seeking to anonymize personal information under the Québec Privacy Act should take to implement applicable requirements.

What is 'anonymization'?

The Québec Privacy Act, like most privacy statutes, regulates "personal information," which means information about an identifiable individual. By implication, any information that falls outside the definition of personal information is not (or is no longer) subject to the Act.

"Anonymization" is a process that involves modifying personal information in order to reduce the risk of an individual being identified, directly or indirectly, from the resulting information, below the applicable statutory threshold (discussed in more detail below). Information that has been effectively anonymized in accordance with this threshold no longer constitutes "personal information" and consequently falls outside the scope of the Act's application.

"Anonymized" information is distinct from "de-identified" (or "pseudonymized") information, which the Québec Privacy Act defines as personal information that "no longer allows the [individual] concerned to be *directly* identified" (emphasis ours). As de-identified information may permit an individual to be indirectly identified, it remains "personal information" that is subject to the Act. This distinction is far from academic and carries significant legal consequences, particularly for organizations seeking to use or disclose anonymized information without consent. If the information is not adequately anonymized, any subsequent use or disclosure without a valid legal basis, such as consent, could constitute unlawful processing of personal information and expose the organization to enforcement action by Québec's privacy regulator, the Commission d'accès à l'information (the CAI).[3]

Notably, the use of these terms across jurisdictions and statutory regimes is not always consistent. For example, while the term "anonymized" is defined in substantially the same

manner under the Québec Privacy Act, the E.U. and U.K.'s *General Data Protection Regulation* (GDPR) and Canada's former federal Bill C-27 (which died on the Order Paper in January 2025), the term "de-identified" is used in Ontario's *Personal Health Information Protection Act, 2004* (PHIPA) to refer to a functionally equivalent concept. To ensure a common understanding, caution should be exercised when using these terms, particularly in commercial arrangements where undefined terms can introduce contractual uncertainty and create regulatory risk for one or both parties (e.g., if the term "anonymize" is used but the anonymization threshold under applicable law is not being met).

The statutory framework for anonymization in Québec

Anonymization features sparingly in the Québec Privacy Act and is only referenced in the following three provisions:

- Section 23 is the operative provision that introduces the concept of anonymized information. In accordance with section 23, information is anonymized where "it is, at all times, reasonably foreseeable in the circumstances that [such information] irreversibly no longer allows the person to be identified directly or indirectly." Section 23 also requires that anonymization be carried out in accordance with "generally accepted best practices" and "the criteria and terms determined by regulation."
    - At its core, section 23 is a data minimization obligation. Where the purposes for which personal information was collected or used are achieved, section 23 requires organizations to "destroy [the] personal information, or anonymize it to use it for serious and legitimate purposes." In other words, section 23 authorizes organizations to anonymize personal information in lieu of destruction; however, it does not speak more generally to anonymization during the lifecycle of personal information before the point at which the organization is required to destroy it. See "Key areas for ongoing consideration" below for further discussion on this point.
- Section 90(3.2) gives the Québec government regulation-making powers *for the purposes of section 23* (i.e., in connection with the destruction or anonymization obligation).
- Section 91(5) makes it an offence to use anonymized information to identify or attempt to identify an individual.

Requirements under the Québec Anonymization Regulation

The Québec Anonymization Regulation establishes the following eight requirements that organizations must meet when anonymizing personal information under section 23 of the Québec Privacy Act:

1. Identify the "serious and legitimate" purpose(s) for which the organization intends to use the anonymized information.[4]
2. Involve a "person qualified in the field" to supervise the anonymization process.[5]
3. De-identify the dataset by removing all direct identifiers (i.e., personal information that can be used to directly identify an individual from the dataset, such as name, contact information or social insurance number).[6]
4. Conduct a preliminary analysis of the re-identification risks of the de-identified dataset, taking into account prescribed elements such as

- the correlation, individualization and inference criteria
- the risks of public or other reasonably available information being used to identify the individual[7]

5. Establish appropriate anonymization techniques and security measures that are consistent with generally accepted best practices in order to reduce the re-identification risks.[8]
6. Conduct a subsequent analysis of the re-identification risks to confirm that the residual risk of re-identification is "very low" (zero risk is not necessary), taking into account prescribed elements, such as
   - the purposes and circumstances of anonymization
   - the nature of the information
   - the correlation, individualization and inference criteria
   - the risk of public or other reasonably available information being used to identify the individual
   - the effort, resources and expertise required to re-identify the individual[9]
7. Periodically reassess re-identification risks to ensure the residual risk of re-identification remains "very low" (zero risk is not necessary), taking into account, in particular, technological advancements. Establish an appropriate timeline for conducting such reassessments based on the residual risks identified in the most recent re-identification risk analysis.[10]
8. Maintain an anonymization "register" containing prescribed information, including
   - a description of the personal information anonymized
   - the purposes for which the anonymized information is used
   - the anonymization techniques and measures implemented
   - the date(s) on which the original and any subsequent risk analyses were completed[11]

Key areas for ongoing consideration

For organizations operating in Québec, the Québec Privacy Act provides a useful framework for anonymization and offers several important clarifications — most notably that it is not necessary to demonstrate *zero risk* of re-identification in order to meet the anonymization threshold. However, key areas for ongoing consideration remain, including the following.

Scope and application of the Québec Anonymization Regulation

As set out above, the enabling provisions in the Québec Privacy Act (namely, sections 23 and 90(3.2)), which introduce anonymization and give the Québec government regulation-making powers, are grounded in a data minimization obligation that authorizes reliance on anonymization as an alternative to destruction.

As the Québec Privacy Act is silent on anonymization during the lifecycle of personal information before the point at which the organization is required to destroy it, an open question remains as to whether the Québec Anonymization Regulation applies solely to the anonymization of personal information as a means of satisfying its destruction obligations, or whether the requirements also extend to anonymization that is carried out earlier in the lifecycle (i.e., not in reliance on section 23).

There may be support for the broader interpretation in the language used in paragraphs 2 and 3 of section 23, which refer to anonymization conducted "[f]or the purposes of this Act" and "under this Act." This wording suggests that the Québec Anonymization Regulation could apply more generally to any anonymization of personal information carried out under the Act, and not only to anonymization undertaken at the end of the information lifecycle. This interpretation aligns with how similar language is used elsewhere in the Act to signal broader applicability, whereas the phrase "under this section" is typically used when the intent is to limit a provision's effect to a particular section.

This question of statutory interpretation raises important practical considerations. Notably, the CAI previously stated on its website that effective anonymization under the Act was not possible in the absence of a regulation setting out specific requirements for anonymization. If the Québec Anonymization Regulation were interpreted to apply only at the end of the personal information lifecycle, this could result in uncertainty for organizations as to the CAI's position on whether anonymization is permitted earlier in the information lifecycle (discussed further under "Legal authority to anonymize personal information", immediately below).

Legal authority to anonymize personal information

The CAI's previous comments regarding the ability to effectively anonymize personal information in the absence of regulations also raise questions regarding legal authority to anonymize in the first instance. In other words, while effectively anonymized information falls outside the scope of the Act, some query whether a lawful authority is required to carry out the process of anonymization at the outset.

For example, under Ontario's PHIPA and the E.U./U.K.'s GDPR, the act of anonymizing personal information is considered by privacy regulators to be a "use" or "processing operation" that requires a valid legal basis under the applicable data protection framework.[12] However, unlike the Québec Privacy Act, which is a consent-based regime, Ontario's PHIPA includes an express legal authority to anonymize[13] and the E.U./U.K.'s GDPR recognizes multiple legal bases beyond consent (such as legitimate interests).[14]

Akin to Canada's *Personal Information Protection and Electronic Documents Act,* the Québec Privacy Act does not *expressly* authorize organizations to anonymize personal information outside of section 23 (i.e., as an alternative to destruction). Although neither the Office of the Privacy Commissioner of Canada nor the CAI has taken a clear position on this issue to date, there appears to be consensus among many stakeholders — albeit one generally grounded in practical considerations rather than settled legal interpretation — that a separate legal authority is not required. This position is generally based on the notion that the act of de-identifying or anonymizing personal information is a means of *modifying* that serves to protect both the confidentiality of personal information and individuals' privacy interests and is often used as a safeguarding mechanism (for which consent is clearly not required). Indeed, the Québec Privacy Act includes an exception to consent to use personal information for the production of statistics *if the information is de-identified*.[15] In the view of many, it would lead to an absurd result if the act of de-identifying for purposes of relying on this exception to consent required a separate legal authority.

To mitigate uncertainty on this point, a growing number of organizations in Québec and across Canada are taking proactive steps to enhance transparency around their anonymization practices, including by updating their external-facing privacy policies to inform individuals about such practices.

Requirement to identify 'serious and legitimate' purposes

The obligation to identify the "serious and legitimate" purposes for which anonymized information will be used is unique to the Québec Privacy Act and has no known analogue across Canadian or foreign privacy laws. For the reasons set out under "What is 'anonymization'?" above, typically there are no statutory restrictions on the use of information that has been anonymized, as it is no longer governed by privacy laws.

The term "serious and legitimate" is not defined under the Québec Privacy Act or the Québec Anonymization Regulation. However, in the context of *collecting* personal information under section 4 of the Québec Privacy Act, the CAI has considered a purpose to be "serious and legitimate" when it is "legitimate, significant and real" and where the invasion of privacy is "proportionate to the objectives pursued," taking into account, among other things, the sensitivity of the information, the lawfulness of the purpose and its compliance with law, justice and fairness.[16]

While the CAI could seek to apply a similar standard when assessing the seriousness and legitimacy of an organization's purposes for using the anonymized information, key elements typically used to assess proportionality (e.g., sensitivity of the information and impact on individuals' privacy) would be challenging to apply to anonymized information. When the anonymization threshold is met, the subsequent use of that information would not, practically speaking, have an impact on privacy as the residual risk of re-identification (and, consequently, potential privacy harm) must already be "very low" in order to meet the anonymization threshold in the first instance.

This raises an important question: what, if any, balancing exercise can or should be conducted under the "serious and legitimate" standard when the information in question no longer identifies an individual? Once the risk of re-identification is demonstrably very low, the privacy impact of any subsequent use is, by definition, minimal. In our view, organizations should simply confirm that the purpose is lawful and tied to a real and non-trivial interest.

The form of the anonymization register

Neither the Québec Privacy Act nor the Québec Anonymization Regulation prescribes the form of the anonymization register that organizations must maintain under section 9 of the Québec Anonymization Regulation. Similarly, no retention period is specified. Some organizations have indicated an intention to rely on their existing privacy impact assessment process to satisfy this register requirement.

Oversight of the anonymization process by a 'person qualified in the field'

The Québec Anonymization Regulation specifically requires that a "person qualified in the field" supervise the anonymization process; however, it does not specify what qualifications, expertise or certifications this individual must possess, nor does it define the scope of their responsibilities or level of involvement. As a result, organizations retain a degree of discretion in determining which stakeholders to involve, at what stages and to what extent.

Depending on the context, organizations may need to involve a range of stakeholders in the anonymization process, from privacy officers and IT specialists to business unit leaders and external experts. These decisions should be guided by factors such as the nature, sensitivity and volume of the personal information being anonymized; the complexity of the anonymization techniques and safeguards being applied; and the intended use of the anonymized information. In practice, organizations should carefully assess their internal resources and, where necessary, seek external expertise to ensure that the anonymization process is adequately supervised and meets regulatory expectations.

Next steps for businesses

Many organizations will find that their pre-existing anonymization practices meet several of the requirements in the Québec Anonymization Regulation, particularly those that generally align with core elements of other well established standards, including the Information and Privacy Commissioner of Ontario's De-identification Guidelines for Structured Data [PDF] and the ISO De-identification Framework. Certain other requirements — most notably the requirement to identify and document the purpose(s) for using anonymized information and to ensure that such purposes are "serious and legitimate" — are unique to the Québec Privacy Act and may require certain updates or enhancements to existing practices.

Organizations seeking to anonymize personal information under the Québec Privacy Act should familiarize themselves with the requirements under the Québec Anonymization Regulation and review their anonymization processes to ensure alignment. This may include

- updating internal policies and procedures to reflect the organization's approach to anonymization
- assigning clear roles and responsibilities for when, how and under what conditions personal information is anonymized
- developing a workable method for documenting anonymization practices, including the anonymization register
- training employees on relevant privacy and data security requirements, including restrictions on re-identification of anonymized information
- reviewing agreements to ensure that any rights granted to third parties (e.g., service providers) to anonymize personal information are consistent with the requirements under the Québec Anonymization Regulation and that such third parties are subject to robust contractual safeguards, including a prohibition on re-identifying anonymized information and audit rights to support oversight and enforcement
- updating external-facing privacy notices or policies to contemplate the anonymization of personal information, where relevant and appropriate

More broadly, organizations should carefully document their anonymization processes, seek input from external experts where appropriate and establish clear retention periods and procedures for periodically reassessing risk of re-identification. These measures, among others, should be reviewed regularly to ensure they remain aligned with evolving legal and regulatory standards for anonymization and rapid technological advancements, particularly in the age of AI and quantum computing.

---

[1] With the exception of the section 9 obligation to record certain information regarding anonymization activities in a register, which came into force on January 1, 2025.

[2] The Québec Anonymization Regulation also applies to public bodies under the *Act respecting Access to documents held by public bodies and the Protection of personal information*; however, this Osler Update focuses on implications for private sector organizations under the Québec Privacy Act.

[3] Under the Québec Privacy Act, the CAI has the authority to impose significant administrative monetary penalties of up to the greater of $10 million or 2% of worldwide turnover for a broad range of violations. For statutory offences, penal fines may reach the greater of $25 million or 4% of worldwide turnover.

[4] Section 23 of the Québec Privacy Act and section 3 of the Québec Anonymization Regulation.

[5] Section 4 of the Québec Anonymization Regulation.

[6] Section 5 of the Québec Anonymization Regulation.

[7] Section 5 of the Québec Anonymization Regulation.

[8] Section 6 of the Québec Anonymization Regulation.

[9] Section 7 of the Québec Anonymization Regulation.

[10] Section 8 of the Québec Anonymization Regulation.

[11] Section 9 of the Québec Anonymization Regulation.

[12] See Information and Privacy Commissioner of Ontario, PHIPA Decision 175, March 25, 2022; Information Commissioner's Office (ICO), *Anonymisation* (accessed May 3, 2025).

[13] Section 37(1)(f) of PHIPA.

[14] Article 6(1) of the GDPR.

[15] Section 12(5) of the Québec Privacy Act.

[16] See PIPEDA Findings #2021-001, paras. 71–73; 1023158-S, paras. 96–107.