Regulation respecting the anonymization of personal information in Quebec: Overview and Commentary

The purpose of this flowchart is to present an overview of the personal information anonymization process, as outlined in the Regulation respecting the anonymization of personal information (Gazette no. 20 of 15-05-2024, page 2847) (the "**Regulation**"). Obligations under the Regulation come into force on May 30, 2024. Exceptionally, obligations surrounding the maintenance of an anonymization register (Step 9) will come into force on January 1, 2025.

The purpose of the Regulation is to determine the criteria and terms applicable to the anonymization of personal information as an alternative to destruction pursuant to section 23 of the Act respecting the protection of personal information in the private sector (RLRQ c P-39.1) (the "**Private Sector Act**") and section 73 of the Act respecting Access to documents held by public bodies and the Protection of personal information (RLRQ c A-2.1) (the "**Access Act**").

For an overview of the anonymization process defined by the draft Anonymization Regulation and our comments prepared for the Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité public consultation, please refer to our previous publication here.

Comments typology:

- 💬 Gowling WLG Comments
- 📶 Signals from the the Commission d'accès à l'information ("CAI")

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.**

S. 23, Private Sector Act

📶 In their commentary, the CAI noted that Quebec privacy legislation and the Anonymization Regulation only address anonymization as an alternative to destruction at the end of the personal information lifecycle. This raises the question: What guidelines apply to anonymizing personal information earlier in the data lifecycle (e.g., where identified as a purpose of collection, a compatible purpose, or with individual consent)? The CAI has expressed concern about the uncertainty caused by this lack of guidance. They suggested extending the Anonymization Regulation to cover all instances where organizations anonymize personal information. As a result, the CAI may look favourably upon organizations that follow the Anonymization Regulation's process when anonymizing personal information before the end of its lifecycle.

Step 1: Determine the nature of the organization

Determine the nature of the "organisation", i.e. a person carrying on an enterprise in Quebec (based on physical presence and/or target market), a public body or a professional order under the law.

S. 1 of the Regulation

💬 Section 23 does not apply to political parties, independent Members and independent candidates under section 127.22 of the Election Act; such a disparity remains surprising.

Step 2: Establish anonymization purposes

Establish "serious and legitimate" (for enterprises) or "public interest" (for public bodies) purposes for using anonymized information.

S. 3 of the Regulation

💬 The notion of "serious and legitimate" purposes is not defined in any law or regulation. We must therefore rely on the common meaning of the words and, to a certain extent, on the rules of law (in particular, the requirement to have a serious and legitimate interest in order to establish a file on another person); however, this notion does not mean that we are dealing with another stage in the life cycle of personal information.

📶 In their commentary, the CAI clarified that communicating anonymized information to third parties (except when necessary for lawful mandate or service contract) or selling anonymized information may not be considered "serious and legitimate" or "public interest" purposes.

Step 3: Supervision by a qualified person

Carrying out an anonymization process requires "supervision by a person qualified in the field".

S. 4 of the Regulation

Step 4: Remove personal information

Remove from the information that the organization intends to anonymize all personal information that directly identifies the person concerned by the information.

S. 5 para. 1 of the Regulation

💬 Such a process is equivalent to "de-identifying" personal information so that it can no longer be used to directly identify the person concerned, in accordance with section 12 of the Private Sector Act and section 65.1 of the Access Act.

Step 5: Pre-analyze re-identification risks

Carry out a preliminary analysis of re-identification risks, taking into account the criteria of individualization, correlation and inference, as well as other reasonably available (particularly in the public space).

Ss. 2 and 5 para. 2 of the Regulation

Step 6: Establish anonymization techniques

Establish anonymization techniques, which "must comply with generally accepted best practices", and reasonable protection and security measures to reduce the risk of re-identification, based on the level of risk identified in the preliminary analysis (see step 5).

S. 6 of the Regulation

💬 The notion of "generally accepted best practice" is derived from the law, but should be clarified in the form of guidelines or a code drawn up in close consultation with the industry.

Step 7: Analyze re-identification risks

Analyze the risks of re-identification following the implementation of anonymization techniques (see step 6 above), which must lead to results demonstrating that personal information "irreversibly no longer allows the person to be identified directly or indirectly". In particular, the "residual risk of re-identification must be very low" with regard to several elements including those previously stated (see steps 2 and 5 above) as well as "the measures required to re-identify the persons, taking into account the efforts, resources and expertise required to implement those measures".

S. 7 of the Regulation

💬 The residual risk of re-identification may be low, but not zero or irreversible, giving organizations a salutary degree of flexibility.

📶 The CAI noted in their commentary that the Anonymization Regulation lacks a method for assessing reidentification risk. The CAI insisted that potential consequences of reidentification should be the focus of such assessments.

Step 8: Update the re-identification risk analysis

Periodically update the most recent re-identification risk analysis, particularly in light of "technological advances", to ensure that the results remain unchanged. Should the results change, the information is no longer considered anonymous.

S. 8 of the Regulation

💬 There is no prescribed deadline for this periodic update. The Regulation specifies that an organization's timeline for periodic reviews should be guided by risks identified in the previous re-identification risk analysis.

📶 In their commentary, the CAI suggested conducting these assessments at least annually or whenever an event occurs that could affect reidentification risks.

Step 9: Maintain an anonymization register

Maintain an anonymization register containing the following elements: (i) a description of the personal information that has been anonymized (see step 2 above); (ii) the purposes of use (see step 2 above); (iii) the anonymization techniques and protection and security established (see step 6 above); and (iv) the dates of completetion or update of the analysis.

S. 9 of the Regulation

*Requirements under step 9 are exceptionally coming into force on January 1st 2025

Penalty mechanisms

In addition to the general penalty mechanisms for non-compliance with the Private Sector Act, section 91 specifies that any organization that identifies or attempts to identify a natural person on the basis of anonymized information is liable to a fine of between $15,000 and $25,000,000, or 4% of worldwide sales for the previous fiscal year, whichever is greater.

Antoine Guilmain
Partner and Co-Leader, National Cybersecurity & Data Protection Practice Group
Montréal
+1 514 392 9521 Ext 69521
antoine.guilmain@gowlingwlg.com

Justin Boileau
Associate, National Cybersecurity & Data Protection Practice Group
Montréal
+1 514 877 3988
justin.boileau@gowlingwlg.com

Last Updated June 2024

If you have any questions or require a French version of the documents cited above, please contact the authors or another member of Gowling WLG's National Cybersecurity & Data Protection Group.