GOWLING WLG

Regulation respecting the anonymization of personal information in Quebec: Modeling and comments

The purpose of this contribution is to comment on the draft Regulation respecting the anonymization of personal information (Gazette no. 51 of 20-12-2023, page 5877) (the "**Regulation**"), particularly in the context of the consultation by the Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité.

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**").

Comments typology:

⚠ Clarification
● Modification
✕ Deletion

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

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 personal 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.

● The expression "anonymized personal information" is misleading, since personal information cannot be anonymous by definition (since it would no longer directly or indirectly identify the person concerned). Instead, it should be referred to as "personal information that the organization intends to anonymize."

Step 3: Supervision by a qualified person

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

S. 4 of the Regulation

✕ This obligation of means should be removed, as it does not provide more guarantees as to the quality of anonymization, and does not respond to the diversity of practices and stakeholders within organizations.

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. In practice, on the sequential level, it is not always necessary to go through de-identification to achieve anonymization.

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 the availability of other information (particularly in the public space).

Ss. 2 and 5 para. 2 of the Regulation

✕ This preliminary step should be removed, as it is redundant with the main analysis (see step 7) and risks overburdening an organizations' existing processes.

● The criteria of individualization, correlation and inference are assessed on the basis of a very high standard, i.e. "the inability to." This wording should be made more flexible, e.g. "the low probability to", to better reflect the spirit of the Regulation and international standards.

● The notion of "public space" is unprecedented and not defined in any way. It would be more appropriate to refer to an existing concept, such as the public nature of information under the law, or to limit the scope of this requirement by making it optional rather than mandatory.

Step 6: Establish anonymization techniques

Establish anonymization techniques, which "must comply with generally accepted best practices," and 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), 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 is 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 protection and security measures outlined above (see step 6) should be added to the elements to be taken into account when assessing the risk of re-identification.

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.

Step 9: Maintain an anonymization register

Maintain an anonymization register containing the following elements: (i) a description of the personal information (see step 2 above); (ii) the purposes of use (see step 2 above); (iii) the anonymization techniques and protection and security measures (see step 6 above); (iv) a summary of the results of the re-identification risk analysis (see steps 7 and 8 above); and (v) the dates of approval or updating of the analyses.

S. 9 of the Regulation

✕ This requirement to maintain a registry should be removed, as it adds a layer of complexity to an already well-documented anonymization process (see all the steps above).

● The retention period for the anonymization register should be specified (e.g. six months) in any case.

Step 8: Update the re-identification risk analysis

Regularly update the re-identification risk a nalysis (see step 7 above), 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 regular update, which must therefore meet a standard of reasonableness based on the organization's internal processes.

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 February 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.