What you need to know about the new Regulation respecting the anonymization of personal information

May 30, 2024

On May 15, 2024, the government of Québec adopted a new *Regulation respecting the anonymization of personal information* (the Regulation). This regulation seeks to specify the criteria and terms for the anonymization of personal information in Québec. It becomes the first regulation to provide a framework for data anonymization in Canada.

Context

Since Law 25 came into force, both the *Act respecting the protection of personal information in the private sector* (ARPPIPS) and the *Act respecting Access to documents held by public bodies and the Protection of personal information* (Access Act) authorize organizations to anonymize personal information when the purposes for which the latter was collected or used have been fulfilled.

Under this provision, organizations must anonymize information in accordance to "generally accepted best practices" and "according to the criteria and terms determined by regulation." Personal information is considered anonymized when it is "at all times, reasonably foreseeable in the circumstances that it irreversibly no longer allows the person to be identified directly or indirectly."

Until the Regulation's recent publication, uncertainties persisted as to the "criteria and terms" with which organizations should comply when they sought to anonymize personal information. In particular, the Commission d'accès à l'information (CAI), Québec's privacy regulator, has indicated on its website that organizations were not authorized to anonymize personal information in the absence of government regulation. Thus, the publication of the Regulation puts an end to several of these uncertainties.[1]

Who must comply with the Regulation?

Both organizations subject to the ARPPIPS and public bodies subject to the Access Act must comply with the Regulation. Professional orders are also required to comply with it

to the extent provided for in the *Professional Code*. The Regulation uses the term “body” to designate all entities required to comply with it.

When does it come into force?

The Regulation will come into force on **May 30, 2024** , save for section 9 on the obligation to record information in a register, which will come into force on Jan. 1, 2025.

Content of the Regulation

Below is a summary of the new requirements introduced by the Regulation to govern the anonymization process. *Italics* identify new elements introduced since the Draft Regulation was submitted in Dec. 2023.

Target period	Requirement	Requirement description
Before an anonymization process	Establishment of the purposes for which the anonymized information will be used (art. 3)	Before beginning a process of anonymization, a body must establish the purposes for which it intends to use the anonymized information. An enterprise must ensure that these purposes are “serious and legitimate,” while a public body must ensure that the anonymized information will be used for “public interest purposes.” The Regulation does not clarify the scope of these terms.
Anonymization process		
At all times during the anonymization process_	Supervision of anonymization process by a person qualified in the field (art. 4)	The body must ensure that the anonymization is carried out under the supervision of a person qualified in the field. To comply with this disposition, a body will have to select a professional qualified in the anonymization and protection of personal information to supervise the process. When the body’s own staff does not have the requisite expertise to supervise such a process, it should call on the services of an external provider who is qualified

		in the field.
At the beginning of the anonymization process	Removal of all personal information allowing the individual to be directly identified (art. 5)	The body must remove all personal information that allows the individual to be directly identified (*e.g.*, name, social insurance number, unique identifier) from the information it intends to anonymize. Information which no longer allows the direct identification of the individual is considered de-identified information as defined by the ARPPIPS and the Access Act.
	Preliminary analysis of re-identification risks (art. 5 par. 2)	The body must then conduct a preliminary analysis of the re-identification risks, with particular regards to: • The individualization criterion, meaning the inability to isolate or distinguish a person within a dataset; • The correlation criterion, meaning the inability to connect datasets concerning the same individual; • The inference criterion, meaning the inability to infer personal information from other available information; • The risks of other *reasonably* available information, in the public space in particular, being used to identify an individual directly or indirectly. *The term "reasonably" was added to section 5 since the publication of the Draft Regulation.*

		The individualization, correlation, and inference criteria are similar to those used by European data protection authorities, notably the CNIL in France. The resources published by these authorities can provide guidance for interpretation in the absence of formal guidelines by the CAI.
	Establishment of the anonymization techniques to be used (art. 6)	On the basis of the re-identification risks identified, a body must establish the anonymization techniques to be used, which must be consistent with generally accepted best practices. **Anonymization techniques**: The European data protection authorities distinguish two main categories of anonymization techniques: randomization and generalization. The Regulation therefore invites bodies to identify appropriate techniques stemming from these two approaches to protect their datasets from the risks of individualization, correlation and inference. **Generally accepted best practices**: To date, the notion of "generally accepted best practices" is not clearly defined. Accordingly, as a precaution, bodies can refer to internationally recognized practices to anonymize personal information. For example, ISO/IEC 27559:2022.
	Establishment of reasonable protection and security measures to reduce re-identification risks (art. 6)	The body must also establish *reasonable* protection and security measures to reduce re-identification risks. *The term "reasonable" was added to section 5*

		following the publication of the Draft Regulation. Note that this provision echoes the obligation found under the ARPPIPS and the Access Act for bodies that use de-identified information to take reasonable measures to limit the risk of anyone identifying a natural person using this information.
Implementation of anonymization techniques and security measures		
After the implementation of anonymization techniques	Analysis of re-identification risks (art. 7)	After implementing anonymization techniques and security measures, the body must conduct an analysis of the re-identification risks of its dataset. **Elements to consider**: The body must consider the following elements during its analysis: • The circumstances related to the anonymization of personal information, including the purposes for which the body intends to use the anonymized information; • The nature of the information; • The individualization criterion, the correlation criterion, and the inference criterion; • The risks of other *reasonably* available information, in particular in the public space, being used to identify a person directly or indirectly; and *The term "reasonably" has also been added to*

		this paragraph, same as with section 5. • The measures required to re-identify the persons, taking into account the efforts, resources and expertise required to implement those measures. **Results of the analysis**: The results of the analysis 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." The Regulation specifies that this criterion does not require demonstrating that zero risk exists. However, taking into account the above elements, the results of the analysis must show that the residual risks of re-identification are very low. *The notion of residual risks has been pluralized since the publication of the Draft Regulation.* Pending guidelines from the CAI on anonymization, we believe that organizations can draw from the method described by the Information and Privacy Commissioner of Ontario to quantitatively assess re-identification risks.
At the end of the anonymization process and after	Periodic assessment of anonymized information (art. 8)	The body must *periodically* assess the information it has anonymized to ensure that it remains anonymized. *The term "periodically" replaced "regularly," which was used in the Draft*

		Regulation. The third paragraph that was added to section 8 provides useful clarifications on the required assessment intervals. The body must update the *latest re-identification risk analysis* it conducted. The update must take into account any technological advancements that may contribute to the re-identification of a person. The results of the *analysis update* must show that the anonymized information remains anonymized in accordance with the criteria provided at the second paragraph of section 7 of the Regulation. Otherwise, the information is no longer considered to be anonymized. The intervals at which a body must conduct anonymized information assessments are determined according to the residual risks identified in the latest re-identification risk analysis conducted. *This last paragraph has been added to the final version of the Regulation.*
	Maintenance of an anonymization register (art. 9) *This requirement must be met as of Jan. 1, 2025.*	Finally, the body anonymizing personal information must record the following information in a register: • A description of the personal information that *has been anonymized;* • The purposes for which the body intends to use anonymized information; • The anonymization techniques used and the protection and security

		measures established; • The date on which the re-identification risk analysis was completed and the date on which the update was completed. In practice, the body should designate a person responsible for maintaining the register. The register should be kept for as long as is necessary to document the body's compliance.

Compliance tips

The main conclusion that emerges from a careful reading of the Regulation is that the anonymization of personal information in Québec is a rigorous process that requires bodies to devote the necessary time and resources to it. With this in mind, we believe that organizations wishing to anonymize personal information can initiate the following actions as of now:

- Involve your IT, document management, conformity and legal teams in the anonymization project;
- Assess whether your organization would benefit from external expertise in data anonymization;
- Map your existing anonymized data directories to assess compliance with the Regulation; and
- Formalize your anonymization process in an internal document adapted to your teams' operational reality.

Contact us

BLG's Cybersecurity, Privacy & Data Protection Group follows legal developments in order to help organizations navigate the requirements of Canadian data protection laws. Don't hesitate to contact our team if your organization seeks assistance in the implementation of compliance steps to govern a process of anonymization.

Footnote

[1] On Dec. 20, 2023, the government published the Draft Regulation respecting the anonymization of personal information in the Gazette officielle du Québec (155th year, No. 51). Since then, the Draft Regulation has been the object of a public consultation, and amendments to its text have been proposed. Therefore, the Regulation published last May 15 differs slightly from the Draft Regulation.

By

Patrick Laverty-Lavoie, Simon Du Perron

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749