BCLP. Client Intelligent

Insights

QUEBEC LAW NO. 25: A LITTLE-KNOWN PRIVACY LAW WITH A BIG REACH

Jan 22, 2024

In late 2021, the Quebec legislature passed "The Privacy Legislation Modernization Act" or Law No. 25 ("**Law 25**"), which was designed to modernize and make significant changes to Quebec's existing privacy framework. Previously, Quebec's privacy regime was very industry-specific, but Law 25 is far broader and has general application. It grants significant new privacy rights for residents of Quebec and establishes heightened obligations for in-scope public and private organizations.

Of particular note for businesses outside Quebec, Law 25 applies to all organizations "carrying on an enterprise" in Quebec that collect, process, use, or disclose Personal Information of individuals located in Quebec. An "enterprise" is defined as carrying on an "organized economic activity," but that activity does not have to be commercial in nature. Entities deemed "enterprises" under Law 25 include unions and medical practices, whereas spiritual and religious organizations are not considered enterprises, as their main purpose is not "economic." Learning From a Decade of Experience: Quebec's Private Sector Privacy Act, at 1.2.3 and 1.2.4. This means that the law likely applies to both for-profit and nonprofit organizations located abroad that process Personal Information of Quebec residents. There also are no minimum thresholds in terms of number of Quebec residents' Personal Information processed or revenue generated nor broad-brush exemptions under Law 25 for categories of data or entities that are already regulated under different regimes. In short, Law 25 likely is in scope for any organization, either within or outside the borders of Quebec, which processes Personal Information associated with one or more of Quebec's approximately 9 million residents.

Law 25 does not adopt the familiar terminology of "controller" or "processor." However, Law 25 does stipulate that processing of Personal Information by third persons on behalf of an in-scope organization requires a written contract "to protect the confidentiality of the Personal Information communicated, to ensure that the information is used only for carrying out the mandate or performing the contract, and to ensure that the mandatary or person does not keep the information after the expiry of the mandate or contract." *Law 25* at Section III, para. 18.3.

Law 25 will be enforced by the Commission on Access to Information ("**CAI**"), and fines range up to 2% - 4% of worldwide turnover (revenue) or $10 - $25 million CAD, depending on the severity of the

violation. *Id.* at Section VII, paras. 90.12-91. Finally, Law 25 gives rise to a new private right of action, allowing individuals to bring claims against in-scope organizations for recovery of statutory damages. *Id.* Law 25 also allows harmed employees to bring collective actions.

Given the above, Law 25 is comparable to the General Data Protection Regulation ("GDPR") and has a broader reach than any U.S. state omnibus privacy law. When compared to Canada's federal law, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), Law 25 has more onerous requirements and poses a greater potential for liability. For example, PIPEDA does not afford residents expansive data subject rights, whereas Law 25 does offer Quebec residents with a full set of individual rights. Law 25 also has stricter consent requirements than PIPEDA.

LAW 25'S REQUIREMENTS AND STAGGERED COMPLIANCE TIMELINE

Law 25's requirements become effective in phases. Below is a list of Law 25's primary requirements and mandatory compliance dates:

SEPTEMBER 22, 2022

1. **Data Protection Officer ("Privacy Officer") Appointment** – In-scope organizations must appoint a Privacy Officer to oversee the data subject requests, data breach reporting, and Privacy Impact Assessment processes. The Privacy Officer need not be located in Quebec and the role can be delegated to the highest senior employee responsible for overseeing compliance. In-scope organizations must publish the name, title, and contact information for the Privacy Officer on their websites. *Id.* at Section I, para. 3.1.

2. **Breach Reporting** – In-scope organizations must notify the CAI and impacted individuals as soon as possible after discovery of a data breach that poses a "high risk of serious injury." In-scope organizations must also maintain an internal register of all qualifying data breaches, which may be requested by the CAI. *Id.* at Section I, para. 3.5.

3. **Disclosure of Biometric Use** – In-scope organizations must disclose whether they intend to collect and/or use any biometric data within a service, product, or system to the CAI sixty (60) days prior to implementation. *Id.* at Section III.

SEPTEMBER 22, 2023

1. **Privacy Policy** – In-scope organizations must publish a privacy policy on their websites. *Id.* at Section II, para. 8.

2. **Privacy Impact Assessments ("PIA(s)")** – In-scope organizations must conduct a PIA when certain triggering circumstances occur, such as when Personal Information is being transferred outside of Quebec or when risky processing occurs, including the processing of Sensitive Personal Information. The PIA requirement also applies where an in-scope organization entrusts

a service provider, processor, or another third party outside Quebec with the task of collecting, using, communicating, or keeping Personal Information on their behalf. *Id.* at Section I, para. 3.3.

3. **Transparency & Consent** – In-scope organizations must regularly audit their processes for collecting, storing, processing, and sharing Personal Information to ensure they are in compliance with Law 25's requirements. Further, in-scope organizations must obtain explicit opt-in consent prior to collecting, storing, processing, and sharing Personal Information, subject to certain exceptions. *Id.* at Section II, para. 12. Law 25 also requires in-scope organizations to take an opt-in approach with respect to cookies and other tracking technologies, meaning that certain cookies cannot deploy on an in-scope organization's website without the user's affirmative consent to the deployment of such cookies. *Id.* at Section II, paras. 8.1 and 9.1. Law 25 does not specify the types of cookies that will require opt-in consent but rather states that the cookies and similar tracking mechanisms whose function allows a user to be "identified, located, or profiled" are subject to the opt-in requirement. Without further guidance from the CAI on this subject, in-scope organizations should consider obtaining opt-in consent for the deployment of all non-essential cookies.

4. **Data Minimization** – In-scope organizations must ensure Personal Information is destroyed and/or anonymized when retention is no longer reasonably necessary. *Id.* at Section 3, para. 23.

5. **Data Subject Rights** – In-scope organizations are required to permit individuals to submit, and must respond to, certain privacy rights requests, such as the right to be informed, access, rectification, withdrawal of consent, and restriction of processing. *Id.* at Section I, para. 8.

SEPTEMBER 22, 2024

1. **Right to Portability** – In-scope organizations must be able to produce a portable record of Personal Information stored about an individual upon request by the individual. *Id.*

With the majority of Law 25's requirements currently in effect, and the law becoming fully effective by the end of 2024, we can expect aggressive enforcement by the CAI.

CONSIDERATIONS FOR IN-SCOPE ORGANIZATIONS

While Law 25 went into force without much fanfare, organizations should waste no time in considering Law 25's applicability. The following measures should be considered when assessing the applicability of Law 25 to business operations and preparing to comply:

1. Understand whether Personal Information belonging to a Quebec resident has been or will be collected or processed through any offered service, product, or system;

2. Ensure that when Personal Information is transferred outside of Quebec, a PIA is conducted;

3. Ensure privacy notices are updated to accurately describe Personal Information collection, processing, and use;

4. Determine whether appointing a Privacy Officer is necessary, if one is not already appointed in Canada and/or Quebec;

5. Ensure that certain cookies or other similar tracking technologies are deployed on a website only upon affirmative opt-in by a user; and

6. Develop a clear and actionable strategy for obtaining consent for processing Personal Information of Quebec residents or assess whether a consent exception can be relied upon.

If you have any questions relating to Quebec Law 25 and its reach and requirements, please contact a member of our Data Privacy & Security team.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448
