David Young Law
Compliance Bulletin

September 2023

The wider impact of Quebec's Law 25

Effective September 22, 2023, key new rules will come into effect under Quebec's *Private Sector Privacy Law*,[1] as amended by Law 25 (formerly Bill 64).

These new rules, while having the most direct impact on organizations that carry on an active business in the province, in fact will impact any organization that collects personal information from Quebec residents, including even if it has no physical presence in the province. Furthermore, the new rules will lead to an alignment more generally with privacy-protective procedures of organizations having a national presence since such organizations are unlikely to adopt procedures that are weaker for non-Quebeckers than for Quebeckers. In any event, to the extent that Quebec residents' data is intermingled with data from outside the province, it will be almost impossible (and in any event illogical) to differentiate processing procedures for Quebec versus non-Quebec data.

Therefore, it can be expected that data collection policies and procedures across organizations will align with the new Quebec standards very quickly if not immediately, recognizing that on an interim basis for certain critical compliance items – such as consent procedures and policies – it will be necessary to ensure that new procedures are in place for Quebec residents effective September 22.

Apart from this wider impact of the new rules across organizations, the Law 25 amendments will influence the privacy norms reflected in the anticipated "second generation" privacy laws, at both the federal and provincial levels. The most prominent instance is Bill C-27, now at the committee stage in Parliament. If passed, Bill C-27 will enact the *Consumer Privacy Protection Act*, which echoes many of the Law 25 rules and, with the hearings expected to take place this fall, may be amended to further align with them.

What are the provisions coming into force September 22, 2023?

It will be remembered that Law 25, enacted on September 21, 2021, comes into force in three annual stages commencing September 22, 2022.[2] The most impactful new rules come into force on September 22, 2023.

---

[1] *Act respecting the protection of personal information in the private sector.*

[2] In force effective September 22, 2022 is a breach reporting requirement (new, similar to PIPEDA and Bill C-27) and the requirement to have a privacy officer (new; in PIPEDA and Bill C-27). Coming into force on September 22, 2024 is a right to data portability (new; not in PIPEDA, in Bill C-27).

David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

These address requirements for comprehensive privacy policies (previously omitted from the *Private Sector Law*), enhanced consent and transparency procedures (again previously not addressed in any detail, but now more in line with PIPEDA[3] and Bill C-27), impact assessments for new information processing projects and cross-border transfers (new, not in PIPEDA or Bill C-27), transparency and disclosure for processing data in automated systems (new; in Bill C-27 but with less rigour), an obligation to destroy information once the purpose has been achieved (new; in PIPEDA and Bill C-27) as well as Privacy by Design rules, minimum stipulations for service provider contracts, and a de-indexing right (all of which are new; not in PIPEDA or Bill C-27). Also of note are rules defining and governing the usage of de-identified and anonymized information (new, not in PIPEDA, but in Bill C-27 with less rigour).

Key compliance item – enhanced data collection transparency and consent procedures

A key element of the Law 25 requirements is contained in the transparency and user friendliness rules related to the collection of personal information. These requirements echo the federal OPC's *Consent Guidelines*[4] under the current PIPEDA rules as well as the proposed codification of elements of those Guidelines under Bill C-27. However they make more explicit certain of the general principles in the Guidelines and in some significant respects go beyond them and the proposed Bill C-27 rules.

Firstly, organizations must provide the following information to individuals upon collection of their personal information: the purposes of the collection; the means of collection; their rights of access and rectification; and their right to withdraw consent. In addition, the following information must also be provided as applicable: the name of any other person on whose behalf the information is being collected; categories of persons to whom the information is provided for processing (i.e. service providers); and whether the information may be exported from Québec.

Consent must be clear, free and informed and be given for specific purposes and must be requested for each such purpose, in clear and simple language and separately from any other information provided to the individual. This "separateness" rule requires both that a request for consent for a specific purpose must be separate from requests for other purposes and that all requests for consent must be presented separately from information regarding other matters, such as a web site's terms and conditions. In particular, the rule means that consent for primary and secondary uses (such as for location data) cannot be bundled together.

A further explicit requirement is that organizations must obtain express consent to use sensitive personal information for secondary purposes, which is consistent with the OPC's *Consent Guidelines* and Bill C-27 which in effect require express consent for collection of any sensitive information. Law 25 defines information as sensitive if, due to its nature, including medical, biometric or otherwise intimate information, or the context of its use or communication, it entails a high reasonable expectation of privacy (consistent with the OPC's Guidelines but not contained in Bill C-27, currently).

[3] *Personal Information Protection and Electronic Documents Act*.
[4] *Guidelines for obtaining meaningful consent;* May 2018, revised August 2021.

All information including consent requests must be provided in clear and simple language, regardless of the means used to collect the personal information.

An additional new rule provides an express provision for consent by minors: consent of a minor under 14 years of age must be given by the person having parental authority or by their guardian (not provided under PIPEDA or Bill C-27; the OPC's *Consent Guidelines* stipulate under 13 years).

Opt-in consent for online tracking and profiling

In addition to these enhanced transparency requirements, Law 25 goes beyond any other existing or proposed rules by requiring in effect *an express opt-in* consent for collection (i.e. tracking) of identification, location or profiling information using technological means. Section 8.1 of the amended law requires that before collecting such information, an organization must inform the person of the potential use of such technology (e.g. mobile location data collection; use of website cookies) and of the means to activate it. The Quebec regulator, the Commission d'accès à l'information (CAI), interprets this requirement as requiring technologies that identify, track or profile individuals to be *turned off by default* and that organizations must inform individuals of the means to turn them on.[5] In other words, websites and mobile interfaces must be in "do not track" mode unless and until the user opts in to tracking.

A significant impact of the new opt-in requirement will be in effect to mandate the use of cookie banners which, while required under EU law[6] and, in an opt-out form, under the *California Consumer Privacy Act* and similar other US state laws,[7] to date are not mandatory in Canada. Aligning with these other existing rules, many websites directed at Canadians now include cookie banners providing for an opt-in to data tracking. The Law 25 rule will make such an opt-in mandatory for data collected from Quebec residents, with the practical result that such a functionality in effect will be the norm for all websites directed at Canadians generally given the impracticality of differentiating those directed at Quebeckers as distinct from other Canadians.

The CAI currently is undertaking a public consultation regarding its proposed publication of guidelines for the interpretation and application of these new rules. Its *Notice of Consultation* sets out its proposed guidelines, which will be finalized in October 2023. Since these guidelines will only be finalized subsequent to the September 22 in-force date, a review of the *Notice of Consultation* is pertinent for providing insight regarding the CAI's expectations for compliance with the new rules.

Cross-border transfers

A significant new requirement impacting all organizations collecting personal information about Quebec residents is the need to conduct a privacy impact assessment (PIA) regarding any export of data outside Quebec including to other Canadian jurisdictions. In addition to notifying individuals at the time of collection that their

[5] See: Notice of consultation May 16, 2023 *Guidelines 2023-1 on Criteria for Valid Consent*
[6] *E-Commerce Directive*.
[7] Opt-out notice on websites regarding selling user's personal information.

data may be communicated outside Quebec, an organization must conduct a PIA prior to exporting personal information or retaining a service provider located outside Québec to process information about Quebec residents. The assessment must address whether the information will receive "adequate protection" in the hands of the non-Quebec recipient in compliance with "generally accepted data protection principles".[8]

Such "Transfer Risk Assessment" (TRA) must take into account the following privacy-related factors: the sensitivity of the information, the purposes for which it will be used, and the protection measures, including contractual ones, that would apply to it as well as the legal and data protection framework applicable in the jurisdiction to which the information would be communicated. Any such export of data must be subject to a written agreement reflecting the results of the assessment and, if required, providing for actions to mitigate any risks identified.

A TRA template should be developed to document the assessment, reflecting the potential data flows and the jurisdictions to which they are directed. Such flows would be assessed to confirm that the data once exported will receive adequate protection. In particular the privacy-related factors identified in the amended law (as noted above) must be addressed. If the recipient is a service provider for the Quebec data collector, as noted above the law now requires a written agreement and stipulates minimum requirements for such agreement.[9]

If it is contemplated that the data flows are within Canada, the PIPEDA environment will be the most relevant assessment factor since the key requirement is to establish compliance with generally accepted data protection principles. The security procedures of the recipient organization will be the other main information input to the TRA. Additional items will address compliance with Law 25's requirements vis-a-vis individuals (e.g. notification that data will be exported; access rights). An example of other items that potentially should be addressed is mentioned by the CAI in its guidance document for PIAs (not specific to TRAs).

Impact assessments for new information processing projects

A further significant new provision of Law 25 that likely will have impact outside of Quebec is the requirement for organizations to conduct PIAs prior to the adoption of new information technology systems involving the processing of personal information. While not currently required under any other private sector privacy law, to the extent that organizations having operations across Canada collect personal information of both Quebec and non-Quebec residents and potentially intermingle that data, they will need to conduct PIAs in respect of all their new information technology/processing projects. Likewise, service providers for Quebec entities wherever they are located will need to perform PIAs for such new projects undertaken on behalf of their clients.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca *Note:* The foregoing does not constitute legal advice.

[8]The principles adopted by the Organization of Economic Cooperation and Development in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, adopted in 1980 and updated in 2013.
[9] Section 18.3 - security measures; authorized purposes; limiting retention; the right to audit and notification of breaches.