David Young Law
Compliance Bulletin

October 2021

Quebec's Bill 64 passed – Canada's first second-generation privacy law

On September 21 the Québec National Assembly passed Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, amending both Quebec's private sector and public sector privacy laws. The amendments to the private sector law,[1] enact provisions that represent what may be characterized as Canada's initial foray into the era of second-generation privacy laws.

It will be recalled that when Quebec enacted the *Private Sector Law* in 1993 it was Canada's first and, until the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into force in 2001, it was the only law protecting individuals' personal information in private sector uses. Quebec was a pioneer with its *Private Sector Law* and now reaffirms that role with the Bill 64 amendments.

Canada's first-generation privacy laws, enacted to respond to the burgeoning personal information databases for commercial uses in the latter part of the last century, included the *Private Sector Law* as well as PIPEDA and the Alberta and BC *Personal Information Protection Acts* (PIPAs). The coming into force of the EU's *General Data Protection Regulation* (GDPR), the successor to the 1995 *Data Protection Directive,* chronicled a new more rigorous and potentially impactful level of mandatory privacy law. The GDPR - the primary example internationally of a "second-generation" privacy law - is providing inspiration for privacy law reform worldwide, including in North America.[2] The law is anchored in a user "rights" framework, addresses transparency in automated data processing and online activity with greater nuance and precision than its predecessor, and provides for significantly increased monetary penalties.

With a view to the GDPR, the federal government is seeking to replace PIPEDA also with a second-generation law, the *Consumer Privacy Protection Act (CPPA)*, proposed to be enacted under the now-defunct Bill C-11. It is anticipated that when Parliament returns in November, a new bill enacting the CPPA, possibly with revisions, will be introduced.

Alignment with existing first-generation laws

The Bill 64 amendments, while clearly drawing inspiration from many of the GDPR's principles, firstly should be understood to bring the *Private Sector Law* into alignment with existing provisions provided for or recognized under most of Canada's other first generation private sector privacy laws – the federal PIPEDA and the BC and Alberta *Personal Information Protection Acts* (PIPAs). So, for example, the amended *Private Sector Law* now includes accountability rules including the requirement to appoint a privacy officer and have policies and procedures addressing an organization's internal privacy compliance, provision for express consent in specified circumstances, an exception for business contact information, a transfer of business exception, and rules regarding outsourcing – most of which are found in in one form or other in the existing private sector privacy

[1] *Act respecting the protection of personal information in the private sector*, RLRQ chap. P-39.1
[2] Including, for example, the *California Consumer Privacy Act* (CCPA).

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

laws. The law also now provides for mandatory breach reporting along the lines included in PIPEDA and Alberta's PIPA.

New, second-generation rules

However in most respects, the Bill 64 amendments take Quebec's *Private Sector Law* to the level of new, more rigorous compliance requirements, consistent with the GDPR. Many of these provisions are expected to be reflected in amendments to the remaining first-generation laws as well, potentially, in a new Ontario private sector privacy law.[3]

The Bill 64 amendments contain, in addition to those noted above, provisions addressing: transparency and disclosure of intended uses of personal information; a requirement for clear and informed consent; requirements to notify individuals regarding use of their information for profiling or targeting or in automated processing; and rights of individuals to deletion and de-indexing, data mobility and to object to automated processing. The amendments also include requirements to conduct privacy impact assessments with respect to new electronic processing and service delivery projects involving personal information and to follow privacy by design principles in any supply of goods or services that involves the collection of personal information.

A significant feature of the amendments is the enhanced rules framework respecting transfers of personal information outside of Quebec, which also is very much inspired by the comparative GDPR rules requiring adequate protection in a foreign jurisdiction.

Bill 64 also includes some important rules facilitating innovation - permitting use of de-identified personal information for internal research and development and streamlined approval of research projects involving personal information. Significantly, the amendments define a category of "de-identified information", which may be used for internal research purposes without consent, and one of "anonymized information" which is outside the scope of the law entirely.

Consistent with the proposals included in the federal government's proposed CPPA, the Bill 64 amendments include provision for substantial administrative monetary penalties and fines for non-compliance. Also included is a private right of action for non-compliance that is more accessible than the right that was proposed in Bill C-11.

A key feature of second-generation privacy laws is the express extension of certain rights to individuals with respect to the uses of their data, specifically: the right to be informed of automated processing, profiling and targeting and the correlative right to object or deactivate such uses; a right to data erasure; and a right of data mobility. The Quebec amendments address all of these rights, again drawing on the GDPR. These rights are also addressed, with some differences, in the proposed CPPA.

[3] See for example, Ontario's White Paper, *Modernizing Privacy in Ontario*, proposing a private sector privacy law, published June 17, 2021.

Right to be informed of and object to automated processing

An organization that uses automated processing of personal information to make a decision about an individual must provide notice to concerned individuals about such processing, and on request provide them with information regarding the elements of personal information used, the reasons and principal factors and parameters leading to the decision, and the right to have their information corrected. In addition, individuals must be given the opportunity "to submit observations" to a member of the organization's staff who is in a position to review the decision. While not an absolute right to object to the automated processing, this provision requires the staff person to "review" these observations and presumably, if they present valid concerns, adjust or eliminate the use of the individual's data.[4]

These rights may be contrasted with the less rigorous comparative CPPA provisions. The CPPA provisions only require an organization pro-actively to provide, as part of the duty to make information available about its policies and practices, a "general account" of its use of any automated processing that makes decisions about individuals "that could have significant impacts on them". While providing the right, on request, to know of the decision, and the provenance of the relevant information, the proposed CPPA provisions do not require disclosure of the relationship between the personal information and the decision, nor the elements of personal information relevant to the decision, as will be required by the Quebec provisions.[5]

In addition to the broad right to know of automated decision systems affecting them, individuals must be notified of any collection of personal information using a technology allowing the individual to be identified, located or profiled, as well as of the means available to de-activate such functions.

Right to erasure ("right to be forgotten")

The Quebec amendments introduce express rights for individuals to request that their data cease to be disseminated by an organization and for any website index linking to their data to be deleted if that indexing contravenes the law or if the prejudicial impact to the individual outweighs any public interests (such as the right to freedom of expression) in disseminating the information. These rights may be contrasted with the more limited right proposed under the CPPA which extends only to deletion of any information collected by an organization directly from the individual, and does not extend to de-indexing.

Mobility right

The Quebec amendments introduce an express mobility right for individuals, permitting them to request that personal information collected from them be provided to them, or to another organization designated by them, in a structured, commonly used technological format. The current correlative provision in the CPPA is less explicit, referring only to "data mobility frameworks" to be articulated by regulation. However it is likely that

[4] By contrast the GDPR: which grants individuals an absolute right to object (at Article 22).

[5] As argued by the federal Privacy Commissioner in his Submission to the Parliamentary ETHI Committee, the CPPA provision does not include the right to a meaningful explanation. Furthermore, the CPPA provides no right for individuals to contest any such decision.

both rules will only be put into effect once common standards for such data portability have been developed and, presumably, reflected in regulations under the CPPA.

Of note, neither the Quebec nor the proposed federal mobility rules extend to data inferred from personal information, such as algorithmic financial risk assessments.

Mandatory privacy impact assessments

A further significant feature of the Bill 64 amendments will require organizations to conduct a privacy impact assessment (PIA) with respect to any "information system project" or "electronic service delivery project" involving the processing of personal information. While considered a best practice under privacy law, it does not yet constitute a common practice within private sector organizations although is required for many public sector organizations.[6]

Bill 64 would make PIAs mandatory with respect to new electronic data processing projects involving personal information – which for private sector organizations in effect may mean requiring this assessment process for practically all of their internal business operations.

The new provisions do not spell out the detailed elements of a required PIA. However, they stipulate that any such assessment shall be proportionate to the sensitivity of the information, the purpose for which it is to be used, and the amount, distribution and format of the information. Additionally, the Quebec regulator, the Commission d'accès à l'information (CAI), has published a guidance document, intended to assist organizations of all sizes in understanding what will be required.[7]

Outsourcing and cross-border transfers

The amendments stipulate provisions requiring organizations and their service providers to have outsourcing agreements in place for processing of personal information and for such agreements to include as minimum: provisions stipulating the service provider's security measures; a requirement for the service provider to use the relevant personal information only for purposes of providing the services and to not retain the information at the end of the contract; and a requirement to notify the organization's privacy officer without delay of any actual or attempted breach of confidentiality of the information and to allow the privacy officer to conduct any verification relating to confidentiality requirements.

These "hands on" requirements for outsourcing agreements while taking a lead from the GDPR are not exceptional and are reflected in many such agreements already in place in the private sector. However, they will require a review and potential updating of such agreements.

More likely impactful will be the law's provisions regarding requirements for outsourcing and other data transfers across borders. The new provisions amend the law's previous basic rule requiring that any data communicated outside Quebec be used only for the documented permitted purposes for which was collected. Now, the transferring organization will be required to complete a PIA to ensure that the relevant data will

[6] See, for example, the federal Treasury Board's *Directive on Privacy Impact Assessment*.
[7] *Guide d'accompagnement – Réaliser une évaluation des facteurs relatifs à la vie privé*, March 19, 2021 (currently available only in French).

receive "adequate protection under generally accepted privacy protection principles" in the non-Quebec jurisdiction. If the PIA indicates that such level of protection will not be attained, the data cannot be transferred. The PIA must take into account the sensitivity of the information, the purposes for which it is to be used, the protection measures which would apply to it, and the legal framework of the foreign jurisdiction, including the degree to which it meets the standard of adequate protection under generally accepted privacy protection principles.

All data transferred outside of Quebec also will require an agreement between the transferring and receiving parties that takes into account the results of the PIA and, if applicable, sets out measures to mitigate the risks identified in the PIA.

In contrast to the GDPR, there is no provision for the Quebec authorities to proactively stipulate non-Quebec jurisdictions that meet the required standard, although the publication of such a list had been included in the original version of the Bill. Consequently, the burden will be entirely on organizations to make this determination.

Furthermore, again unlike the GDPR, the Quebec law provides no alternative mechanisms for transferring data to countries that whose privacy laws do not meet the standard.[8] Presumably, there is flexibility within the assessment process and agreement requirement to stipulate contractual protections that may enable the standard to be met.[9]

Conclusions - significant adjustments to organizations' processes will be required

The Bill 64 amendments stipulate a two-year transition period for most of the new provisions.[10] However, it can be appreciated that a number of the new, GDPR-inspired provisions in Bill 64 will entail significant adjustments to organizations' current processes and procedures. Clearly, those that have aligned their practices with the GDPR's requirements will have a significant head start. Furthermore, with the advent of second-generation privacy laws both federally and in other provincial jurisdictions, such adjustments may be seen as anticipating changes that eventually will be required across the country.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca

Field Code Changed

[8] Such are provided within the GDPR regime, for example, through standard contractual clauses.
[9] A further potentially burdensome and consequential aspect for Canadian businesses is that there is no provision for distinction between international and inter-provincial transfers of personal information.
[10] The breach reporting obligations and requirement to have a privacy officer will come into force in one year (September 2022).