CLIENT ALERTS & INSIGHTS

Quebec Adopts New Law to Modernize Personal Information Protection

SEPTEMBER 30, 2021

Authors: Ryan T. Sulkin

Bill 64 largely tracks with already existing privacy regulations in other jurisdictions and will take effect over the course of the next three years, with some provisions taking effect in September 2022.

On September 21 Quebec's National Assembly passed Bill 64, *An Act to Modernize Legislative Provisions as regards the Protection of Personal Information* ("**Bill 64**"), and on September 22 it received royal assent to become law. Bill 64 does not create a new privacy law in Quebec, but instead amends already existing law.

Quebec is now home to Canada's most onerous privacy law as the new law brings its privacy law up to speed with other omnibus privacy laws such as the General Data Protection Regulation ("**GDPR**") in the European Union. Like the GDPR, Bill 64 represents Quebec's attempt to create a legal framework requiring data protection by design and default.

While Bill 64 amends already existing law, it drastically expands the depths of privacy law in Quebec. The law largely focuses on increasing the number of individual privacy rights, creating a private right of action, clarifying what consent is required under what circumstances, requiring data security assessments under variance circumstances, and requiring the appointment of a privacy officer.

The new provisions also create new breach notice requirements, create new exceptions, and add to the obligations an entity must undertake to protect an individual's privacy. Most of the law will gradually come into effect over the course of the next three years.

Below is a brief explanation of the scope of Quebec privacy law and key changes Bill 64 makes to Quebec's privacy law.

Scope

While Bill 64 itself does not specify the territorial scope of Quebec privacy law, it is safe to assume that any entity collecting, using, or processing the personal information ("**PI**") of individuals based in Quebec will likely fall within the law's scope.

The law applies to those "carrying on an enterprise" within Quebec and the Commission d'accès à l'information ("**CAI**"), which is Quebec's privacy regulator, regularly exerts jurisdiction (under the old privacy law and other privacy laws) over entities that operate completely outside of Quebec.

So long as an entity has a real and substantial connection to Quebec, they could be subject to the law. Key factors used to determine if a real and substantial connection exists are whether (1) the entity targeted Quebec in any way; (2) whether it has any actual customer located in Quebec; and (3)

whether the entity collects personal information from data subjects located in Quebec. These factors were used in CAI's recent joint investigation of Clearview AI.

Because the CAI pushes its jurisdiction to the maximum and the CAI is the chief privacy law enforcer in Quebec, this law may apply to a large swatch of entities that are not physically located in Quebec.

Additionally, Canada has the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") that governs privacy law at the federal level. At the federal level, the Office of the Privacy Commissioner of Canada ("**OPCC**") are the lead privacy regulators. However, at the provincial level, privacy law is regulated and enforced by the separate provinces' privacy regulators.

Therefore, entities cannot rely on PIPEDA compliance to comply with Bill 64 because Bill 64 created new obligations and privacy rights at the provincial level in Quebec. Therefore, any entity subject to Quebec privacy law must not only comply with Canadian law, but also Quebec law.

It is also important to note that both Quebec and Canadian privacy laws do not provide broad exceptions for the collection, use, and disclosure of an employee's information.

Data Protection Policies and Procedures

Two of the new requirements under Bill 64 that must be implemented by September 2022 relate to the policies and procedures an entity must have in place.

First, an entity subject to Quebec's privacy laws and regulations must appoint a privacy officer who will be in charge of creating, implementing, and maintaining policies and procedures that ensure the entity's compliance with the law. The CEO of an entity will become the default privacy officer unless someone else is appointed or the authority is delegated in writing.

The new requirements also state that an entity's policies and procedures must be published on their website.

Under Bill 64, those policies and procedures must (1) provide for the keeping and destruction of PI; (2) define roles and responsibilities of employees throughout the PI's life cycle; and (3) define a process for handling individual requests and complaints. The privacy officer is charged with protecting all personal information but may delegate their duties and responsibilities in writing, to any person.

Second, Bill 64's new breach reporting provisions will come into effect within the next year. Under the new breach reporting provisions, any time a "confidentiality incident" creates a risk of serious injury, the CAI and any affected individuals must be notified. Confidentiality incidents include any (1) unauthorized access to PI; (2) unauthorized use of PI; (3) unauthorized disclosures or communications of PI; or (4) any other loss or breach of PI.

Further, to determine if a confidentiality incident creates a risk of serious injury, an entity must weigh the sensitivity of the information, the anticipated consequences of its use, and the likelihood that it will be used to injure the individual.

Finally, entities must keep a log or register of all breaches that can then be requested by the CAI.

Privacy Impact Assessments

Bill 64 will now require entities to conduct mandatory Privacy Impact Assessments ("**PIA**") in three scenarios: (1) acquisition, development, and redesign of any information systems or electronic services involving PI; (2) transfers of PI to somewhere outside of Quebec; and (3) communications of PI without consent for study, research, or statistical purposes.

PIAs must assess "privacy-related factors," under Bill 64. However, the new law does not expand on what specific privacy-related factors must be consulted, so, entities are left waiting for regulation that will hopefully expand on these requirements.

Notice and Consent Requirements

The new law also amends existing consent requirements and strengthens an individual's control over the collection and processing of their PI. Consent is required for each specific purpose an entity is collecting, using, processing, or disclosing PI and it must be clear, free, and informed. Additionally, the notice and consent must disclose the specific purposes.

Due to the new data minimization principle explained below, consent is only valid for as long as the PI is necessary for the stated specific purposes.

Despite the strong language in Bill 64, however, something less than express consent is likely required. The new law explicitly requires express consent where sensitive personal information is concerned, while it is silent on the exact type of consent (implied or express) is required where PI is concerned. PI is considered sensitive PI if its nature creates a high level of a reasonable expectation of privacy.

Further, Bill 64 amends existing law to allow entities to use collected PI, without *additional* consent, for other purposes that were not originally disclosed if the further purpose is (1) used for purposes consistent with the original purpose; (2) used for clear the benefit of the individual concerned; (3) necessary for study, research, or statistical purposes (and the information is deidentified); and (4) necessary for the purpose of an entity's standard administrative practices.

Administrative practices include (1) providing requested goods or services; (2) preventing and detecting fraud; (3) detecting and preventing fraud; (4) management and assessment of an entity's resources; and (5) establishing or managing an employment relationship.

Consent Exceptions

As stated above, consent is generally required prior to disclosing any PI to third parties. However, Bill 64 introduces some exceptions.

An entity can disclose PI without consent when such disclosure is needed to conclude a commercial transaction and the third party must enter into an agreement with the entity. That agreement must ensure (1) the PI is used only for concluding a commercial transaction; (2) PI is not further disclosed without consent; (3) the third party takes measures needed to protect the confidentiality of the PI; and (4) to destroy the PI if the transaction falls through or its use becomes no longer necessary.

Additionally, PI can be used without consent for study, research, or statistical purposes if a PIA makes certain findings related to confidentiality and proportionality.

It is important to note that deidentified data and anonymized data are two different categories of data under Bill 64. Deidentified data includes any information that "no longer allows the person concerned to be directly identified" while anonymized data includes any information that is "irreversibly no longer allows the person to be identified directly or indirectly."

Data Minimization

Similar to the GDPR and other omnibus privacy laws and regulations, Bill 64 implements new requirements for data minimization.

Entities are required to destroy (or alternatively anonymize) PI when it is no longer needed to serve the specific purpose it was collected for. Like other laws and regulations, the retention periods for PI under Bill 64 are tied to what the disclosed specific purpose is and the lifetime of the need to use the PI for that purpose.

Third Parties

Prior to Bill 64, the language of Quebec privacy law focused on an entity's protection of PI in their own possession.

Bill 64, however, vastly expands the universe of policies and procedures an entity must implement and maintain by broadening the reach of Quebec privacy law.

The new law requires an entity to be responsible for PI security and protection regardless of whether the information is collected, maintained, or processed by the entity itself or a third-party on the entity's behalf (i.e., contractors, vendors, etc.). Agreements akin to standard contractual clauses are likely going to be required, however regulators have not formulated them yet.

Data Localization and Cross-Border Transfer

Bill 64 also amends Quebec privacy law to require certain conditions on the transfer of PI to a location outside of Quebec.

A PIA is required when an entity transfers PI outside of Quebec must contemplate (1) the security laws in the location where the PI is being transferred to; (2) the sensitivity of the PI being transferred; (3) the specific purpose of the PI; and (4) the contractual measures in place.

Importantly, the PIA must find that the PI is being transferred to a state that offers adequate levels of protection. Written agreements related to the transfer of PI to a location outside of Quebec must incorporate the PIA and address any concerns by implementing mitigation policies and procedures. This is a slight twist on cross-border transfer adequacy determinations required under other laws because the determination is in the hands of the entity conducting the PIA, not in the hands of regulators.

Beyond the PIA, consent is not required, but the entity must inform the individual concerned of the possibility of cross-border transfer.

Individual Privacy Rights

Canadian and Quebec privacy laws already grant a litany of privacy rights. Bill 64 brings Quebec to the forefront of Canadian privacy law, tracking closely with rights granted to individuals under the

GDPR. Rights of access, correction, data portability, to object to automated decision-making, and to be forgotten are now Quebec law under Bill 64.

First, the rights of access and correction grant individuals the ability to require an entity to inform them of what PI an entity possesses about them; and if that PI is inaccurate, request that it be corrected.

Second, the right to data portability requires an entity to respond to requests for access to PI and provide them a readable copy of the PI. The right only applies to computerized data collected from the individual. Entities must also develop and install the necessary procedures and systems designed to transfer PI in commonly used technological formats in order to comply.

Third, individuals now have a right to object to automated decision-making. An entity must fully inform the individual prior to using PI to render any decision that is based solely on automated processing. Notice to the individual is required at or before the time automated decision is rendered and must include information describing (1) the PI being used; (2) the reasons and principal factors that lead to a decision; and (3) the individual's right to have such PI corrected.

Finally, Bill 64 adds the right to be forgotten to the list of privacy rights in Quebec. An individual can require an entity to "forget" them if (1) disseminating the PI causes the individual serious injury in relation to his reputation or privacy; (2) the injury is greater than the public interest; and (3) the cost of forgetting someone does not exceed the possible injury.

Enforcement

Moving towards stricter enforcement mechanisms, the new law gives the CAI the ability to fine entities that violate Quebec privacy law. Administrative penalties can run up to CA$10 million or 2% of an entity's previous year's worldwide turnover (whichever is a higher total). Penal penalties can run up to CA$25 million or 4% of an entity's previous year's worldwide turnover (whichever is a higher total). Additionally, there is a minimum penalty of CA$15,000.

There is also a new private right of action in Bill 64 that allows individuals to bring suit based on violations of the law. The private right of action is meant to give individuals greater control over their PI privacy and rights granted under Quebec law. If any violation is intentional or caused by gross negligence, individuals can obtain at least CA$1,000 in punitive damages.

As the Canadian privacy regulatory structure continues to develop and the obligations your business is required to take on grow, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.